



User Guide

AWS Transfer Family



AWS Transfer Family: User Guide

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

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

Table of Contents

Was ist AWS Transfer Family?	1
Wie AWS Transfer Family funktioniert	4
Blogbeiträge relevant für Transfer Family	5
Voraussetzungen	9
Regionen, Endpunkte und Kontingente	9
Melde dich an für AWS	10
Speicher konfigurieren	10
Einen Amazon S3 S3-Bucket konfigurieren	11
Ein Amazon EFS-Dateisystem konfigurieren	16
Erstellen Sie eine IAM-Rolle und -Richtlinie	20
Eine Benutzerrolle erstellen	21
So funktionieren Sitzungsrichtlinien	25
Beispiel für eine read/write Zugriffsrichtlinie	28
Familientutorials übertragen	32
Erste Schritte mit Serverendpunkten	33
Voraussetzungen	33
Schritt 1: Melden Sie sich bei der AWS Transfer Family Konsole an	34
Schritt 2: Einen SFTP-enabled Server erstellen	35
Schritt 3: Fügen Sie einen vom Service verwalteten Benutzer hinzu	36
Schritt 4: Eine Datei mit einem Client übertragen	37
Erstellen Sie einen Entschlüsselungs-Workflow	39
Schritt 1: Konfigurieren Sie eine Ausführungsrolle	40
Schritt 2: Erstellen Sie einen verwalteten Workflow	41
Schritt 3: Fügen Sie den Workflow einem Server hinzu und erstellen Sie einen Benutzer	43
Schritt 4: Erstellen Sie ein PGP-Schlüsselpaar	44
Schritt 5: Speichern Sie den privaten PGP-Schlüssel in AWS Secrets Manager	45
Schritt 6: Verschlüsseln Sie eine Datei	46
Schritt 7: Führen Sie den Workflow aus und sehen Sie sich die Ergebnisse an	47
SFTP-Konnektoren erstellen und verwenden	48
Ausgangstypen für Konnektoren	49
Schritt 1: Erstellen Sie die erforderlichen unterstützenden Ressourcen	50
Schritt 2: Erstellen und testen Sie einen SFTP-Connector	57
Schritt 3: Senden und Abrufen von Dateien mithilfe des SFTP-Connectors	62

Verfahren zum Erstellen eines Transfer Family Family-Servers, der als Remote-SFTP-Server verwendet werden kann	67
Verwenden Sie einen benutzerdefinierten Identitätsanbieter	70
Voraussetzungen	70
Schritt 1: Erstellen Sie einen CloudFormation Stack	71
Schritt 2: Überprüfen Sie die Konfiguration der API Gateway Gateway-Methode für Ihren Server	72
Schritt 3: Die Transfer Family Family-Serverdetails anzeigen	73
Schritt 4: Testen Sie, ob Ihr Benutzer eine Verbindung zum Server herstellen kann	75
Schritt 5: Testen Sie die SFTP-Verbindung und die Dateiübertragung	75
Schritt 6: Beschränken Sie den Zugriff auf den Bucket	76
Aktualisieren Sie Lambda, wenn Sie Amazon EFS verwenden	78
Richten Sie eine AS2-Konfiguration ein	79
Schritt 1: Zertifikate für AS2 erstellen	81
Schritt 2: Zertifikate als Transfer Family Family-Zertifikatsressourcen importieren	85
Schritt 3: Erstellen Sie Profile für Sie und Ihren Handelspartner	87
Schritt 4: Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet	88
Schritt 5: Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Partner	91
Schritt 6: Stellen Sie eine Verbindung zwischen Ihnen und Ihrem Partner her	93
Schritt 7: Testen Sie den Austausch von Dateien über AS2 mithilfe von Transfer Family	94
Richten Sie eine einfache Web-App ein	96
Voraussetzungen	97
Schritt 1: Erstellen Sie die erforderlichen unterstützenden Ressourcen	97
Schritt 2: Erstellen Sie eine Transfer Family Family-Web-App	98
Schritt 3: Konfigurieren Sie Cross-origin Resource Sharing (CORS) für Ihren Bucket	99
Schritt 4: Fügen Sie Ihrer Transfer Family Family-Web-App einen Benutzer hinzu	101
Schritt 5: Registrieren Sie einen Standort in Amazon S3 und erstellen Sie eine Zugriffsberechtigung	102
Schritt 6: Greifen Sie als Benutzer auf Ihre Transfer Family Family-Web-App zu	105
Nächste Schritte	106
Integrieren Sie Okta als Ihren Identitätsanbieter für Web-Apps	107
Richten Sie eine Web-App mit selektivem Multi-Bucket-Zugriff ein	109
Voraussetzungen	109
Schritt 1: Erstellen Sie eine Transfer Family Family-Web-App	110
Schritt 2: Konfigurieren Sie IAM-Rollen für den S3-Zugriff	111

Schritt 3: Richten Sie S3 Access Grants ein	113
Schritt 4: Registrieren Sie S3-Bucket-Standorte	114
Schritt 5: Zugriffsberechtigungen erstellen	114
Schritt 6: Konfigurieren Sie die CORS-Richtlinie für S3-Buckets	115
Schritt 7: Testen Sie die Konfiguration	116
Schlussfolgerung	116
Transfer Family für SFTP, FTPS, FTP	118
Optionen für den Identitätsanbieter	118
AWS Transfer Family Endpunkt-Typmatrix	120
Konfiguration eines Transfer Family Family-Serverendpunkts	124
Erstellen Sie einen SFTP-enabled Server	126
Erstellen Sie einen FTPS-enabled Server	135
Erstellen Sie einen FTP-enabled Server	144
Einen Server in einer VPC erstellen	153
Arbeiten mit benutzerdefinierten Hostnamen	180
FTP/FTPS Überlegungen zum NLB	184
Dateien über den Serverendpunkt übertragen	184
Verfügbare SFTP/FTPS/FTP Befehle	187
Finden Sie Ihren Amazon VPC-Endpunkt	189
Vermeiden Sie Fehler setstat	191
OpenSSH verwenden	38
Verwenden Sie WinSCP	193
Benutze Cyberduck	37
Benutzen FileZilla	197
Verwenden Sie einen Perl-Client	198
Verwenden Sie LFTP	198
Verarbeitung nach dem Upload	198
SFTP-Nachrichten	200
Benutzer verwalten	202
Amazon EFS im Vergleich zu Amazon S3	203
Logische Verzeichnisse	204
Active Directory-Gruppenkontingente	205
Service-managed Benutzer	206
Benutzerdefinierter Identitätsanbieter	217
Verzeichnisdienst für MS AD	259
Verzeichnisdienst für Entra ID	270

Verwenden Sie logische Verzeichnisse	277
Grundlegendes zur Chroot- und Verzeichnisstruktur	278
Regeln für die Verwendung logischer Verzeichnisse	279
Implementierung logischer Verzeichnisse	281
Beispiele für die Konfiguration logischer Verzeichnisse	284
Logische Verzeichnisse für Amazon EFS konfigurieren	286
Benutzerdefinierte AWS Lambda Antwort	286
Access FSx für NetApp ONTAP-Dateisysteme	287
-Übersicht	288
Voraussetzungen	289
So funktioniert FSx-Speicher mit Transfer Family	290
Einen S3-Zugangspunkt für FSx erstellen	291
Verwendung von S3-Zugangspunkt-Aliasen mit FSx	293
Konfiguration der Transfer Family für FSx-Speicher	295
Benutzer für FSx-Speicher verwalten	297
Konfiguration von Dateiübertragungsclients	299
Problembehandlung bei FSx-Speicher	300
Familien-Web-Apps übertragen	302
AWS-Regionen für Transfer Family Family-Web-Apps	303
Browserkompatibilität für AWS Transfer Family Web-Apps	303
So erstellen Sie eine Transfer Family Family-Web-App	303
Konfigurieren Sie Ihren Identitätsanbieter	306
Konfigurieren Sie IAM-Rollen	308
Eine Transfer Family Family-Web-App konfigurieren	311
Eine Transfer Family Family-Web-App erstellen	311
IP-Adressierung	313
Eine Transfer Family Family-Web-App in einer VPC erstellen	314
Eine Transfer Family Family-Web-App erstellen	315
Post-creation Schritte	317
Cross-origin Richtlinie zur gemeinsamen Nutzung von Ressourcen (CORS)	317
Beschränken des Zugriffs auf einen bestimmten VPC-Endpunkt	318
Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu	319
Richten Sie Cross-origin Resource Sharing (CORS) für Ihren Bucket ein	323
Amazon S3 S3-Zugriffsberechtigungen konfigurieren	325
Verwenden Sie eine benutzerdefinierte URL	331

Protokollierung für Transfer Family Family-Web-Apps	334
Amazon S3 S3-Datenereignisse aktivieren	335
Beispiele für Authentifizierungsprotokolle	337
Protokolleinträge anzeigen	345
Fehlerbehebung bei Ihren Web-Apps	346
Beheben Sie Netzwerkfehler	346
Fehlerbehebung: Der konfigurierte Bucket wird nicht angezeigt	347
Beheben Sie Fehler mit benutzerdefinierten URLs	347
Beheben Sie verschiedene Fehler	348
Doppelte S3-Buckets werden in der Web-App angezeigt	349
Anweisungen für Endbenutzer	349
Kontingente für Web-Apps	350
Benutzer von IAM Identity Center	350
Third-party Endbenutzer	351
Endbenutzeroberfläche von Transfer Family	352
Verfügbare Aktionen	353
SFTP-Anschlüsse	356
SFTP-Konnektoren erstellen	356
Wählen Sie den Ausgangstyp des SFTP-Connectors	357
Wählen Sie den IP-Adressierungsmodus	359
Anmeldeinformationen im Secrets Manager speichern	359
Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang	361
Erstellen Sie einen SFTP-Connector mit Egress VPC-based	372
Testen Sie einen SFTP-Connector	384
VPC-Konnektivität	386
Verwendung von SFTP-Anschlüssen	387
Übertragen von Dateien	388
Listet den Inhalt von Remote-Verzeichnissen auf	389
Dateien auf dem Remoteserver verschieben und löschen	391
Überwachung von SFTP-Anschlüssen	394
Verwenden Sie die Connector-API, um den Status von Dateiübertragungsanfragen abzufragen	394
SFTP-Connector-Ereignisse in Amazon anzeigen EventBridge	394
SFTP-Connector-Protokolle in Amazon anzeigen CloudWatch	395
Überwachung VPC VPC-Ausgangsanschlüssen	395
Verwaltung von SFTP-Konnektoren	397

Aktualisieren Sie die SFTP-Konnektoren	397
Details zum SFTP-Connector anzeigen	398
Kontingente für SFTP-Konnektoren	399
Kontingente für SFTP-Anschlüsse	400
Skalierung Ihrer SFTP-Konnektoren	401
Referenzarchitekturen	403
Blog-Posts	403
Workshops	403
Lösungen	403
VPC-Referenzarchitekturen	404
Familie für AS2 übertragen	406
AS2-Anwendungsfälle	407
AS2-Vorlagen CloudFormation	412
AS2-Vorlagen anpassen	412
Testen Sie Ihre AS2-Bereitstellung	413
Bewährte Methoden für die Bereitstellung von AS2-Vorlagen	413
AS2 konfigurieren	414
AS2-Konfigurationen	415
AS2-Kontingente	417
Merkmale und Fähigkeiten von AS2	420
AS2-Zertifikate verwalten	422
AS2-Zertifikate importieren	423
Rotation der AS2-Zertifikate	425
Erstellen Sie AS2-Profile	427
Erstellen Sie einen AS2-Server	428
Erstellen Sie einen AS2-Server mit der Transfer Family Family-Konsole	429
Erstellen Sie einen AS2-Server mithilfe einer Vorlage	432
Erstellen Sie eine AS2-Vereinbarung	436
Konfigurieren Sie AS2-Konnektoren	438
Erstellen Sie einen AS2-Konnektor	438
Algorithmen für AS2-Konnektoren	442
Standardauthentifizierung für AS2-Konnektoren	443
Aktivieren Sie die Standardauthentifizierung für AS2-Konnektoren	444
Konnektordetails anzeigen	448
AS2-Nachrichten übertragen	450
Empfangen Sie AS2-Nachrichten	451

Konfigurieren Sie HTTPS für AS2	452
Dateien mit AS2-Anschlüssen übertragen	459
Dateinamen und Speicherorte	461
Statuscodes	464
JSON-Beispieldateien	465
Benutzerdefinierte HTTP-Header für AS2	467
Vorlagen – Übersicht	468
So funktioniert's	468
Wichtigste Funktionen	468
Implementierungsinformationen	469
Bereitstellung und Verwendung	470
Überwachen Sie AS2	471
AS2-Statuscodes	473
AS2-Fehlercodes	474
Überwachung des Ablaufs von Zertifikaten	488
DaysUntilExpiry Metrik	489
Bewährte Methoden für die Zertifikatsüberwachung	489
Beispiele für Alarmkonfigurationen	490
Verwaltung von Workflows zur Dateiverarbeitung	492
Erstellen Sie einen Workflow	494
Konfigurieren Sie einen Workflow und führen Sie ihn aus	496
Workflow-Details anzeigen	498
Verwenden Sie vordefinierte Schritte	501
Datei kopieren	501
Datei entschlüsseln	506
Datei kennzeichnen	513
Datei löschen	514
Benannte Variablen für Workflows	515
Beispiel für einen Workflow zum Markieren und Löschen	515
Verwenden Sie benutzerdefinierte Schritte zur Dateiverarbeitung	520
Mehrere Lambda-Funktionen nacheinander verwenden	522
Zugreifen auf eine Datei nach der benutzerdefinierten Verarbeitung	522
Beispiele für Ereignisse, an die AWS Lambda beim Hochladen einer Datei gesendet werden	523
Beispiel für eine Lambda-Funktion für einen benutzerdefinierten Workflow-Schritt	525
IAM-Berechtigungen für einen benutzerdefinierten Schritt	525

IAM-Richtlinien für Workflows	526
Vertrauensbeziehungen im Arbeitsablauf	528
Beispiel für eine Ausführungsrolle: Entschlüsseln, Kopieren und Markieren	528
Beispiel für eine Ausführungsrolle: Funktion ausführen und löschen	530
Ausnahmebehandlung für einen Workflow	531
Überwachen Sie die Workflow-Ausführung	532
CloudWatch Protokollierung für einen Workflow	532
CloudWatch Metriken für Workflows	535
Erstellen Sie einen Workflow aus einer Vorlage	535
Einen Workflow von einem Transfer Family Family-Server entfernen	539
Einschränkungen und Beschränkungen	541
Server verwalten	543
Eine Liste von Servern anzeigen	543
Löschen Sie einen Server	544
SFTP-Serverdetails anzeigen	545
AS2-Serverdetails anzeigen	547
IPv6-Support	548
IPv6-Einschränkungen	549
Konfiguration von IPv6 für Server	549
Verwenden Sie ALB für öffentliche Dual-Stack-AS2-Server	550
Serverdetails bearbeiten	552
Bearbeiten Sie die Dateiübertragungsprotokolle	555
Bearbeiten Sie den Serverendpunkt	557
Bearbeiten Sie die Protokollierung	558
Bearbeiten Sie die Sicherheitsrichtlinie	559
Ändern Sie den verwalteten Workflow	561
Ändern Sie die Display-Banner für Ihren Server	562
Stellen Sie Ihren Server online oder offline	562
Konfiguration des Identitätsanbieters bearbeiten	563
Umstellung auf einen vom Service verwalteten Identitätsanbieter	564
Wechsel zum AWS Directory Service	564
Wechseln Sie zum benutzerdefinierten Identitätsanbieter	565
Benutzererhaltung bei Übergängen zum Identitätsanbieter	570
Wichtige Überlegungen beim Wechsel des Identitätsanbieters	570
Server-Hostschlüssel verwalten	570
Wann müssen Hostschlüssel importiert werden	572

Fügen Sie einen zusätzlichen Server-Hostschlüssel hinzu	572
Löscht einen Server-Hostschlüssel	574
Rotiert die Server-Hostschlüssel	575
Zusätzliche Schlüsselinformationen zum Server-Host	577
Überwachen Sie die Nutzung innerhalb der Konsole	578
Verwaltung von Zugriffssteuerungen	584
Eine S3-Bucket-Zugriffsrichtlinie erstellen	585
Eine Sitzungsrichtlinie erstellen	586
Beispiel für eine Sitzungsrichtlinie	587
Verschachtelte Ersetzungen für Sitzungsrichtlinien	590
Dynamisches Berechtigungsmanagement	591
Grundlegendes zur Berechtigungsarchitektur von Transfer Family	591
Zwei Ansätze für die Rechteverwaltung	591
Implementieren von Sitzungsrichtlinien	592
Implementierung nach Benutzertyp	593
Beispiel: Vereinfachung der Rollenverwaltung mit Sitzungsrichtlinien	594
CloudTrail Protokollierung	597
CloudTrail Protokollierung aktivieren	599
Amazon S3 S3-Datenereignisse aktivieren	599
Beispiel für einen Protokolleintrag zum Erstellen eines Servers	600
Datenzugriffsprotokolle	601
Beispiel für einen Protokolleintrag für einen erfolgreichen Datenzugriff	601
Allgemeine Datenzugriffsvorgänge	604
CloudWatch Protokollierung	605
Arten der CloudWatch Protokollierung für Transfer Family	606
Protokollierung für Server erstellen	608
Protokollierung für Server erstellen	611
Die Protokollierung für einen Server aktualisieren	611
Serverkonfiguration anzeigen	614
Verwaltung der Protokollierung für Workflows	616
Konfiguration einer Rolle für CloudWatch	619
Protokollstreams von Transfer Family anzeigen	621
CloudWatch Amazon-Alarme erstellen	625
Protokollierung von S3-API-Aufrufen in S3-Zugriffsprotokollen	626
Beispiele zur Begrenzung des Problems mit verwirrtem Stellvertreter	626
CloudWatch Protokollstruktur für Transfer Family	628

Strukturierte JSON-Logs für Transfer Family	628
Legacy-Protokolle für Transfer Family	632
Beispiel für CloudWatch Protokolleinträge	635
Beispiele für Protokolleinträge für Übertragungssitzungen	636
Beispielprotokolleinträge für SFTP-Konnektoren	637
Beispielprotokolleinträge für VPC-Lattice-Konnektoren	639
Beispiel für Protokolleinträge für Fehler beim Schlüsselaustausch-Algorithmus	640
CloudWatch Metriken verwenden	641
Familiendimensionen übertragen	647
Benutzerbenachrichtigungen	647
CloudWatch Abfragen	647
Ereignisse verwalten mit EventBridge	650
Transfer Family Ereignisse	651
SFTP-, FTPS- und FTP-Serverereignisse	651
Ereignisse des SFTP-Connectors	655
AS2-Ereignisse	656
Senden von Transfer Family Ereignissen	657
Erstellen von Ereignismustern	659
Testen von Ereignismustern für Transfer Family Ereignisse	660
Berechtigungen	660
Weitere Ressourcen	660
Detailreferenz zu Ereignissen	661
Serverereignisse	662
Connector-Ereignisse	669
AS2-Ereignisse	677
Sicherheit	683
Sicherheitsvorteile der VPC-Konnektivität	684
VPC Lattice-Sicherheitsmodell	684
Bewährte Sicherheitsmethoden für VPC-Konnektivität	685
Sicherheitsrichtlinien für Server	686
Kryptografische Algorithmen	687
Einzelheiten zur Sicherheitsrichtlinie	699
Sicherheitsrichtlinien für SFTP-Konnektoren	717
Kryptografische Algorithmen	717
Einzelheiten zur Sicherheitsrichtlinie für den SFTP-Connector	718
Post-Quantum Sicherheitsrichtlinien	720

Informationen zum hybriden Schlüsselaustausch in SSH nach der Quantenphase	722
Verwendung	722
Testen	724
Datenschutz	727
Datenverschlüsselung in Transfer Family	729
Verschlüsselung im Ruhezustand	730
Schlüsselverwaltung	731
Überblick über den Algorithmus	732
SSH-Authentifizierung	732
PGP-Algorithmen	733
Generieren Sie SSH-Schlüssel	735
SSH-Schlüssel rotieren	741
Generieren Sie PGP-Schlüssel	743
PGP-Schlüssel verwalten	745
Unterstützte PGP-Clients	750
Identity and Access Management	751
Zielgruppe	751
Authentifizierung mit Identitäten	752
Verwalten des Zugriffs mit Richtlinien	753
Wie AWS Transfer Family funktioniert mit IAM	755
Identity-based politische Beispiele	760
Tag-based Beispiele für politische Maßnahmen	763
Fehlerbehebung für -Identität und -Zugriff	767
IAM-Bedingungsschlüssel	769
Compliance-Validierung	771
Ausfallsicherheit	772
VPC-Endpunkte für APIs	773
Steuern des Zugriffs mithilfe von VPC-Endpunktrichtlinien	773
VPC-Endpunkt erstellen	774
Sicherheit der Infrastruktur	775
Überlegungen zu NLB und NAT	775
Sicherheit der VPC-Konnektivität und der Infrastruktur	777
Firewall für Webanwendungen	778
Cross-service Prävention von verwirrten Stellvertretern	779
Familien-Benutzerrollen übertragen	781
Workflow-Rollen für Transfer Family	783

Family Connector-Rollen übertragen	784
logging/invocationFamilienrollen übertragen	786
AWS verwaltete Richtlinien	787
AWSTransferConsoleFullAccess	788
AWSTransferFullAccess	788
AWSTransferLoggingAccess	788
AWSTransferReadOnlyAccess	788
Richtlinienaktualisierungen	789
Terraform-Module der Transfer Family	790
SFTP-Server	790
SFTP-Anschlüsse	790
AS2	791
B2B-Datenaustausch	791
Problembehebung bei Transfer Family	792
Probleme bei der Authentifizierung	792
Authentifizierungsfehler— SSH/SFTP	793
Problem mit nicht übereinstimmenden verwalteten AD-Bereichen	794
Die Active Directory-Gruppenlimits wurden überschritten	794
Verschiedene Probleme bei der Authentifizierung	795
Probleme mit Amazon API Gateway beheben	795
Beheben Sie Fehler beim Testen Ihres Identitätsanbieters	797
Doppelte Amazon S3 S3-Buckets in der Web-App	349
Probleme mit dem SFTP-Anschluss	798
Beheben Sie Probleme beim Hinzufügen vertrauenswürdiger Hostschlüssel für Ihren SFTP-Connector	799
Die Schlüsselerhandlung schlägt fehl	799
Drosselung des SFTP-Anschlusses	800
Optimierung der Leistung des SFTP-Connectors	801
Behebung von VPC-Verbindungsproblemen	802
Verschiedene Probleme mit dem SFTP-Connector	805
Probleme mit der SFTP-Konnektivität	805
Beheben Sie Probleme mit der SFTP-Konnektivität	806
Beheben Sie Probleme mit dem SFTP-Client	806
Beheben Sie Probleme beim Hochladen von Dateien	806
Behebung von Problemen mit dem SFTP-Connector vom VPC-Ausgangstyp	808
Probleme mit dem benutzerdefinierten Identitätsanbieter	810

Beheben Sie Fehler bei der API Gateway Gateway-Integration	810
Behebung von Timeouts bei Lambda-Funktionen	812
Behebung konsistenter Lambda-Timeout-Probleme	813
Beheben Sie Ausnahmen <code>KeyError</code>	813
Workflow-Probleme	813
Beheben Sie Probleme mit verwalteten Workflows	814
Beheben Sie Probleme mit der Workflow-Entschlüsselung	816
EFS-Probleme	821
Probleme mit Amazon EFS beheben	821
Speicher- und Verschlüsselungsprobleme	823
Richtlinien zur Fehlerbehebung für verschlüsselte Amazon S3 S3-Buckets	824
Beheben Sie die <code>ResourceNotFound</code> Ausnahme	824
Probleme mit der Überwachung und Warnung	825
Beheben Sie Fehler bei fehlenden oder unvollständigen Metriken CloudWatch	825
Beheben Sie fehlende EventBridge Ereignisse	826
Cross-region Probleme mit der Übertragung	827
Beheben Sie Probleme mit regionsübergreifenden Übertragungsberechtigungen	828
Beheben Sie Leistungsprobleme bei regionsübergreifenden Übertragungen	829
Probleme bei der Terraform-Bereitstellung	830
Beheben Sie Fehler bei der Erstellung von Terraform-Ressourcen	831
Beheben Sie Probleme mit der Terraform-Statusverwaltung	832
Probleme mit der WAF-Integration	833
Beheben Sie Fehler beim Blockieren von legitimem Datenverkehr durch WAF	833
Beheben Sie Probleme bei der WAF-Integration mit benutzerdefinierten Identitätsanbietern	834
Service-managed Benutzerprobleme	835
Beheben Sie Probleme mit Benutzern, die vom Service	835
AS2-Probleme	836
Beheben Sie AS2-Probleme	837
Probleme mit dem AS2-Zertifikat	837
Probleme mit dem AS2 MDN-Empfang	837
Probleme bei der Überwachung des Ablaufs von Zertifik	838
API-Referenz	840
Dokumentverlauf	842
.....	dcclix

Was ist AWS Transfer Family?

AWS Transfer Family ist ein sicherer Übertragungsdienst, mit dem Sie Dateien in und aus AWS Speicherdiensten übertragen können. Transfer Family ist Teil der AWS Cloud Plattform. AWS Transfer Family bietet vollständig verwaltete Unterstützung für die Übertragung von Dateien über SFTP, AS2, FTPS, FTP und webbrowserbasierte Übertragungen direkt in und aus Speicherdiensten. AWS Sie können Ihre Workflows für die Dateiübertragung nahtlos migrieren, automatisieren und überwachen, indem Sie bestehende clientseitige Konfigurationen für Authentifizierung, Zugriff und Firewalls beibehalten. Somit ändert sich nichts für Ihre Kunden, Partner und internen Teams oder deren Anwendungen. Weitere Informationen und Informationen AWS zum Erstellen von Cloud-Anwendungen [mit Amazon Web Services finden Sie unter Erste Schritte](#) mit.

AWS Transfer Family unterstützt die Übertragung von Daten von oder zu den folgenden AWS Speicherdiensten.

- Speicher im Amazon Simple Storage Service (Amazon S3). Informationen zu Amazon S3 finden Sie unter [Erste Schritte mit Amazon Simple Storage Service](#).
- Dateisysteme des Amazon Elastic File System (Amazon EFS) Network File System (NFS). Informationen zu Amazon EFS finden Sie unter [Was ist Amazon Elastic File System?](#)

AWS Transfer Family unterstützt die Übertragung von Daten über die folgenden Protokolle:

- Secure File Transfer Protocol (SFTP): Version 3

Das offizielle IETF-Dokument ist hier: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Sicheres Dateiübertragungsprotokoll (FTPS)
- Dateiübertragungsprotokoll (FTP)
- Erklärung zur Anwendbarkeit 2 (AS2)
- Browser-based Übertragungen

Note

Für FTP- und FTPS-Datenverbindungen liegt der Portbereich, den Transfer Family zum Einrichten des Datenkanals verwendet, zwischen 8192 und 8200.

Dateiübertragungsprotokolle werden in Datenaustausch-Workflows in verschiedenen Branchen wie Finanzdienstleistungen, Gesundheitswesen, Werbung und Einzelhandel verwendet. Transfer Family vereinfacht die Migration von Dateiübertragungsworkflows zu AWS.

Im Folgenden sind einige häufige Anwendungsfälle für die Verwendung von Transfer Family mit Amazon S3 aufgeführt:

- Daten werden AWS für Uploads von Drittanbietern wie Anbietern und Partnern genutzt.
- Subscription-based Datenverteilung mit Ihren Kunden.
- Unternehmensinterne Übertragungen

Im Folgenden sind einige häufige Anwendungsfälle für die Verwendung von Transfer Family mit Amazon EFS aufgeführt:

- Datenverteilung
- Lieferkette
- Verwaltung von Inhalten
- Web-Server-Anwendungen

Im Folgenden sind einige häufige Anwendungsfälle für die Verwendung von Transfer Family mit AS2 aufgeführt:

- Workflows mit Compliance-Anforderungen, die darauf beruhen, dass Datenschutz- und Sicherheitsfunktionen in das Protokoll integriert sind
- Logistik in der Lieferkette
- Workflows für Zahlungen
- Business-to-business (B2B-) Transaktionen
- Integrationen mit Systemen für Unternehmensressourcenplanung (ERP) und Kundenbeziehungsmanagement (CRM)

Im Folgenden sind einige häufige Anwendungsfälle für die Verwendung von Transfer Family Family-Web-Apps aufgeführt:

- Vereinfachter Zugriff auf Daten in Amazon S3 für ein breiteres und vielfältigeres Spektrum von Geschäftsanwendern

- Zentralisiertes Datenzugriffsmanagement für Ihre Belegschaft
- Visualisierung von Amazon S3 Access Grants über eine verwaltete Oberfläche

Mit Transfer Family erhalten Sie Zugriff auf einen Server mit aktiviertem Dateiübertragungsprotokoll AWS (oder eine Webschnittstelle für verwaltete Dateiübertragung), ohne eine Serverinfrastruktur betreiben zu müssen. Sie können diesen Service verwenden, um Ihre auf Dateiübertragung basierenden Workflows zu migrieren und AWS gleichzeitig die Clients und Konfigurationen Ihrer Endbenutzer unverändert beizubehalten. Bei Servern verknüpfen Sie zuerst Ihren Hostnamen mit dem Serverendpunkt, fügen dann Ihre Benutzer hinzu und gewähren ihnen die richtige Zugriffsebene. Nachdem Sie dies getan haben, werden die Übertragungsanfragen Ihrer Benutzer direkt von Ihrem Transfer Family Family-Serverendpunkt aus bearbeitet.

Ermitteln Sie für Transfer Family-Web-Apps Ihre Konfigurationseinstellungen und nehmen Sie optionale Anpassungen vor. Danach können sich Ihre Benutzer anmelden und Daten direkt zu und von Amazon S3 übertragen.

Transfer Family bietet die folgenden Vorteile:

- Ein vollständig verwalteter Service, der sich in Echtzeit an die Anforderungen anpasst.
- Sie müssen Ihre Anwendungen nicht ändern oder eine Infrastruktur für Dateiübertragungsprotokolle ausführen.
- Da sich Ihre Daten im dauerhaften Amazon S3 S3-Speicher befinden, können Sie native Funktionen AWS-Services für Verarbeitung, Analyse, Berichterstattung, Prüfung und Archivierung verwenden.
- Mit Amazon EFS als Datenspeicher erhalten Sie ein vollständig verwaltetes elastisches Dateisystem zur Verwendung mit AWS Cloud Services und lokalen Ressourcen. Amazon EFS ist so konzipiert, dass es bei Bedarf auf Petabytes skaliert werden kann, ohne Anwendungen zu unterbrechen. Es wächst und schrumpft automatisch, wenn Sie Dateien hinzufügen oder entfernen. Dadurch entfällt die Notwendigkeit, Kapazitäten bereitzustellen und zu verwalten, um dem Wachstum Rechnung zu tragen.
- Ein vollständig verwalteter, serverloser File Transfer Workflow-Dienst, der die Einrichtung, Ausführung, Automatisierung und Überwachung der Verarbeitung von Dateien, die mit AWS Transfer Family hochgeladen wurden, vereinfacht.
- Es sind keine Investitionen erforderlich und die Kosten für den Service sind nutzungsbezogen.

In den folgenden Abschnitten finden Sie eine Beschreibung der verschiedenen Funktionen von Transfer Family, ein Tutorial für die ersten Schritte, detaillierte Anweisungen zur Einrichtung der verschiedenen protokollfähigen Server, zur Verwendung verschiedener Arten von Identitätsanbietern und die API-Referenz des Dienstes.

Informationen zu den ersten Schritten mit Transfer Family finden Sie im Folgenden:

- [Wie AWS Transfer Family funktioniert](#)
- [Voraussetzungen](#)
- [Erste Schritte mit AWS Transfer Family Server-Endpunkten](#)
- [Familien-Web-Apps übertragen](#)

Wie AWS Transfer Family funktioniert

AWS Transfer Family ist ein vollständig verwalteter AWS Service, mit dem Sie Dateien über die folgenden Protokolle oder Webbrowser in und aus dem Amazon Simple Storage Service (Amazon S3) -Speicher oder Amazon Elastic File System (Amazon EFS) -Dateisysteme übertragen können:

- Secure File Transfer Protocol (SFTP): Version 3

Das offizielle IETF-Dokument ist hier: [SSH File Transfer Protocol draft-ietf-secsh-filexfer-02.txt](#).

- Sicheres Dateiübertragungsprotokoll (FTPS)
- Dateiübertragungsprotokoll (FTP)
- Erklärung zur Anwendbarkeit 2 (AS2)
- Browser-based Übertragungen

AWS Transfer Family unterstützt bis zu 3 Availability Zones und wird durch eine automatisch skalierbare, redundante Flotte für Ihre Verbindungs- und Übertragungsanfragen unterstützt. Ein Beispiel dafür, wie Sie mithilfe von Latency-based Routing eine höhere Redundanz erreichen und die Netzwerklatenz minimieren können, finden Sie im Blogbeitrag [Minimiere die Netzwerklatenz bei der AWS Übertragung für SFTP-Server](#).

Transfer Family Managed File Transfer Workflows (MFTW) ist ein vollständig verwalteter, serverloser File Transfer Workflow-Dienst, mit dem die Verarbeitung von Dateien, die mit hochgeladen wurden, einfach eingerichtet, ausgeführt, automatisiert und überwacht werden kann. AWS Transfer Family Kunden können MFTW verwenden, um verschiedene Verarbeitungsschritte wie Kopieren, Markieren,

Scannen compressing/decompressing, Filtern und encrypting/decrypting die Übertragung von Daten mit Transfer Family zu automatisieren. Dies bietet umfassende Transparenz für Nachverfolgung und Überprüfbarkeit. Weitere Details finden Sie unter [AWS Transfer Family verwaltete Workflows](#).

AWS Transfer Family unterstützt jeden Standard-Client für das Dateiübertragungsprotokoll. Einige häufig verwendete Clients sind die folgenden:

- [OpenSSH](#) — Ein Befehlszeilenprogramm für Macintosh und Linux.
- [WinSCP](#) — Ein Windows-only grafischer Client.
- [Cyberduck](#) — Ein grafischer Linux-, Macintosh- und Microsoft Windows-Client.
- [FileZilla](#) — Ein grafischer Linux-, Macintosh- und Windows-Client.

AWS bietet die folgenden Transfer Family Family-Workshops an.

- Entwickeln Sie eine Dateiübertragungslösung, die AWS Transfer Family für verwaltete SFTP/FTPS Endgeräte und Amazon Cognito und DynamoDB für die Benutzerverwaltung nutzt. [Die Details zu diesem Workshop finden Sie hier.](#)
- [Erstellen Sie einen Transfer Family-Endpunkt mit aktiviertem AS2 und einen Transfer Family AS2-Connector. Die Details für diesen Workshop finden Sie hier.](#)
- Entwickeln Sie eine Lösung, die präskriptive Anleitungen und ein praktisches Lab bietet, auf der Sie erfahren, wie Sie eine skalierbare und sichere Dateiübertragungsarchitektur aufbauen können, AWS ohne bestehende Anwendungen ändern oder die Serverinfrastruktur verwalten zu müssen. [Die Einzelheiten zu diesem Workshop finden Sie hier.](#)

Blogbeiträge relevant für Transfer Family

In der folgenden Tabelle sind die Blogbeiträge aufgeführt, die nützliche Informationen für Kunden von Transfer Family enthalten. Die Tabelle ist in umgekehrter chronologischer Reihenfolge angeordnet, sodass die neuesten Beiträge am Anfang der Tabelle stehen.

Titel und Link des Blogbeitrags	Date
Stellen Sie Okta als benutzerdefinierten Identitätsanbieter bereit für AWS Transfer Family	11. August 2025

Titel und Link des Blogbeitrags	Date
Automatisierung der Bearbeitung von Leistungsansprüchen im Gesundheitswesen von Papier bis in elektronische Form mit AWS	29. Mai 2025
Wie verwendet AWS Transfer Family man und zum Schutz vor Malware GuardDuty	30. April 2025
Wie FICO Dateiübertragungen mithilfe von ETL-Automatisierung modernisiert AWS Transfer Family	24. April 2025
Ankündigung von AWS Transfer Family Web-Apps für vollständig verwaltete Amazon S3 S3-Dateiübertragungen	01. Dezember 2024
Sechs Tipps zur Verbesserung der Sicherheit Ihres Servers AWS Transfer Family	24. September 2024
Vereinfachen Sie die Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für AWS Transfer Family	12. August 2024
Architektur sicherer und richtlinienkonformer verwalteter Dateiübertragungen mit AWS Transfer Family SFTP-Konnektoren und PGP-Verschlüsselung	16. Mai 2024
Verwenden von Amazon Cognito als Identitätsanbieter mit AWS Transfer Family Amazon S3	14. Mai 2024
Wie Transfer Family Ihnen helfen kann, eine sichere, konforme verwaltete Dateiübertragungslösung aufzubauen	3. Januar 2024
Erkennen Sie Malware-Bedrohungen mit AWS Transfer Family	20. Juli 2023

Titel und Link des Blogbeitrags	Date
Erweiterung der SAP-Workloads mit AWS Transfer Family	13. Juli 2023
Verschlüsseln und entschlüsseln Sie Dateien mit PGP und AWS Transfer Family	21. Juni 2023
Authentifizierung AWS Transfer Family mit Azure Active Directory und AWS Lambda	15. Dezember 2022
Passen Sie Benachrichtigungen zur Dateizustellung mithilfe AWS Transfer Family verwalteter Workflows an	14. Oktober 2022
Aufbau einer Cloud-nativen Dateiübertragungspattform mithilfe von Workflows AWS Transfer Family	5. Januar 2022
Aktivierung der Self-Service-Schlüsselverwaltung für Benutzer mit A AWS Transfer Family und. AWS Lambda	17. Dezember 2021
Verbessern Sie die Datenzugriffskontrolle mit AWS Transfer Family Amazon S3	5. Oktober 2021
Verbessern Sie den Durchsatz für Dateiübertragungen mit Internetzugriff mithilfe von AWS Global AcceleratorAWS Transfer Family Services	7. Juni 2021
Sicherung AWS Transfer Family mit AWS Web Application Firewall und Amazon API Gateway	5. Mai 2021
Sicherung AWS Transfer Family mit AWS Web Application Firewall und Amazon API Gateway	15. Januar 2021
AWS Transfer Family Unterstützung für Amazon Elastic File System	7. Januar 2021

Titel und Link des Blogbeitrags	Date
Aktivieren Sie die Passwortauthentifizierung für die AWS Transfer Family Verwendung AWS Secrets Manager	5. November 2020
Zentralisieren Sie den Datenzugriff mit AWS Transfer Family und AWS Storage Gateway	22. Juni 2020
Verwenden von Amazon EFS für AWS Lambda in Ihren serverlosen Anwendungen	18. Juni 2020
Verwenden Sie die IP-Zulassungsliste, um Ihre AWS Transfer Family Server zu sichern	8. April 2020
Minimiere die Netzwerklatenz mit deiner AWS Übertragung für SFTP-Server	19. Februar 2020
Lift-and-Shift-Migration von SFTP-Servern zu AWS	12. Februar 2020
Vereinfachen Sie Ihre AWS SFTP-Struktur mit Chroot und logischen Verzeichnissen	26. September 2019
Verwenden Sie Okta als Identitätsanbieter mit AWS Transfer Family	30. Mai 2019

Voraussetzungen

In den folgenden Abschnitten werden die Voraussetzungen beschrieben, die für die Nutzung des AWS Transfer Family Dienstes erforderlich sind. Sie müssen mindestens einen Amazon Simple Storage Service (Amazon S3) -Bucket erstellen und über eine AWS Identity and Access Management (IAM) -Rolle Zugriff auf diesen Bucket gewähren. Die Rolle muss zudem eine Vertrauensstellung einrichten. Diese Vertrauensstellung ermöglicht es Transfer Family, die IAM-Rolle für den Zugriff auf Ihren Bucket zu übernehmen, sodass er die Dateiübertragungsanfragen Ihrer Benutzer bearbeiten kann.

Informationen zur IPv6-Unterstützung für AWS Transfer Family Server finden Sie [IPv6-Unterstützung für Transfer Family Family-Server](#) im Kapitel Server verwalten.

Themen

- [Unterstützte AWS Regionen, Endpunkte und Kontingente für Transfer Family Family-Server](#)
- [Melden Sie sich an für AWS](#)
- [Konfigurieren Sie den Speicher für die Verwendung mit Servern AWS Transfer Family](#)
- [Erstellen Sie eine IAM-Rolle und -Richtlinie](#)

Unterstützte AWS Regionen, Endpunkte und Kontingente für Transfer Family Family-Server

Um programmgesteuert eine Verbindung zu einem AWS Dienst herzustellen, verwenden Sie einen Endpunkt. Der Endpunkt für Kunden in der Region USA Ost (Ohio) (us-east-2) ist beispielsweise `transfer.us-east-2.amazonaws.com`. Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Servicere Ressourcen oder -vorgängen für Ihr AWS-Konto. In diesem Handbuch finden Sie Kontingente in [AS2-Kontingente](#) und [Kontingente für SFTP-Anschlüsse](#).

Weitere Informationen zu unterstützten AWS Regionen, Endpunkten und Servicekontingenten finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine Amazon Web Services-Referenz

Für Transfer Family Family-Web-Apps sind die unterstützten Regionen unter aufgeführt [AWS-Regionen für Transfer Family Family-Web-Apps](#). Kontingente für Transfer Family Family-Web-Apps finden Sie unter [Kontingente für Web-Apps](#).

Melden Sie sich an für AWS

Wenn Sie sich für Amazon Web Services (AWS) registrieren, wird Ihr AWS Konto automatisch für alle Dienste in angemeldet AWS, einschließlich AWS Transfer Family. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Wenn Sie bereits ein AWS Konto haben, fahren Sie mit der nächsten Aufgabe fort. Wenn Sie kein AWS -Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos aus.

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

Um sich für eine anzumelden AWS-Konto

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

Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

Informationen zur Preisgestaltung und zur Schätzung der Kosten für die Nutzung von Transfer Family finden Sie unter [AWS Transfer Family Preise](#). AWS Pricing Calculator

Informationen zur AWS regionalen Verfügbarkeit finden Sie unter den [AWS Transfer Family Endpunkten und Kontingenten](#) in der Allgemeine AWS-Referenz.

Konfigurieren Sie den Speicher für die Verwendung mit Servern AWS Transfer Family

In diesem Thema werden die Speicheroptionen beschrieben, die Sie zusammen verwenden können AWS Transfer Family. Sie können entweder Amazon S3 oder Amazon EFS als Speicher für Ihre Transfer Family Family-Server verwenden.

Inhalt

- [Einen Amazon S3 S3-Bucket konfigurieren](#)
 - [Amazon S3 Access Points](#)
 - [HeadObject Verhalten von Amazon S3](#)
 - [Gewähren Sie die Möglichkeit, nur Dateien zu schreiben und aufzulisten](#)
 - [Eine große Anzahl von Null-Byte-Objekten verursacht Latenzprobleme](#)
- [Ein Amazon EFS-Dateisystem konfigurieren](#)
 - [Besitz von Amazon EFS-Dateien](#)
 - [Amazon EFS-Benutzer für Transfer Family einrichten](#)
 - [Transfer Family Family-Benutzer auf Amazon EFS konfigurieren](#)
 - [Einen Amazon EFS-Root-Benutzer erstellen](#)
 - [Unterstützte Amazon EFS-Befehle](#)

Einen Amazon S3 S3-Bucket konfigurieren

AWS Transfer Family greift auf Ihren Amazon S3 S3-Bucket zu, um die Übertragungsanfragen Ihrer Benutzer zu bearbeiten. Daher müssen Sie im Rahmen der Einrichtung Ihres File-Transfer-Protokoll-fähigen Servers einen Amazon S3 S3-Bucket bereitstellen. Sie können einen vorhandenen Bucket verwenden oder einen neuen Bucket erstellen.

Note

Sie müssen keinen Server und keinen Amazon S3 S3-Bucket verwenden, die sich in derselben AWS Region befinden, aber wir empfehlen dies als bewährte Methode.

Wenn Sie Ihre Benutzer einrichten, weisen Sie ihnen jeweils eine IAM-Rolle zu. Diese Rolle bestimmt die Zugriffsebene, die sie auf Ihren Amazon S3 S3-Bucket haben.

Informationen zum Erstellen eines neuen Buckets finden Sie unter [Wie erstelle ich einen S3-Bucket?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Note

Sie können Amazon S3 Object Lock verwenden, um zu verhindern, dass Objekte für einen bestimmten Zeitraum oder auf unbestimmte Zeit überschrieben werden. Dies funktioniert bei Transfer Family genauso wie bei anderen Diensten. Wenn ein Objekt existiert und geschützt

ist, ist es nicht erlaubt, in diese Datei zu schreiben oder sie zu löschen. Weitere Informationen zu Amazon S3 Object Lock finden Sie unter [Verwenden von Amazon S3 Object Lock](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Amazon S3 Access Points

AWS Transfer Family unterstützt [Amazon S3 Access Points](#), eine Funktion von Amazon S3, mit der Sie den detaillierten Zugriff auf gemeinsam genutzte Datensätze einfach verwalten können. Sie können S3 Access Point-Aliase überall verwenden, wo Sie einen S3-Bucket-Namen verwenden. Sie können in Amazon S3 Hunderte von Access Points für Benutzer erstellen, die über unterschiedliche Berechtigungen für den Zugriff auf gemeinsam genutzte Daten in einem Amazon S3 S3-Bucket verfügen.

Beispielsweise können Sie Access Points verwenden, um drei verschiedenen Teams den Zugriff auf denselben gemeinsamen Datensatz zu ermöglichen, wobei ein Team Daten aus S3 lesen kann, ein zweites Team Daten in S3 schreiben kann und das dritte Team Daten aus S3 lesen, schreiben und löschen kann. Um eine detaillierte Zugriffskontrolle wie oben erwähnt zu implementieren, können Sie einen S3-Zugriffspunkt erstellen, der eine Richtlinie enthält, die verschiedenen Teams asymmetrischen Zugriff gewährt. Sie können S3-Zugriffspunkte mit Ihrem Transfer Family Family-Server verwenden, um eine differenzierte Zugriffskontrolle zu erreichen, ohne eine komplexe S3-Bucket-Richtlinie zu erstellen, die Hunderte von Anwendungsfällen umfasst. Weitere Informationen zur Verwendung von S3 Access Points mit einem Transfer Family Family-Server finden Sie im Blogbeitrag [Enhance data access control with AWS Transfer Family and Amazon S3](#).

Note

AWS Transfer Family unterstützt derzeit keine Amazon S3 Multi-Region Access Points.

HeadObject Verhalten von Amazon S3

Note

Wenn Sie einen Transfer Family Family-Server erstellen oder aktualisieren, können Sie die Leistung Ihrer Amazon S3 S3-Verzeichnisse optimieren, wodurch HeadObject Anrufe vermieden werden.

In Amazon S3 sind Buckets und Objekte die primären Ressourcen, in denen Objekte in Buckets gespeichert werden. Amazon S3 kann ein hierarchisches Dateisystem nachahmen, sich aber manchmal anders verhalten als ein typisches Dateisystem. Beispielsweise sind Verzeichnisse in Amazon S3 kein erstklassiges Konzept, sondern basieren stattdessen auf Objektschlüsseln. AWS Transfer Family leitet einen Verzeichnispfad ab, indem der Schlüssel eines Objekts durch den Schrägstrich (/) geteilt wird, das letzte Element als Dateinamen behandelt und dann Dateinamen, die dasselbe Präfix haben, unter demselben Pfad gruppiert werden. Zero-byte Objekte werden erstellt, um den Pfad eines Ordners darzustellen, wenn Sie mit `mkdir` oder mithilfe der Amazon S3 S3-Konsole ein leeres Verzeichnis erstellen. Der Schlüssel für diese Objekte endet mit einem abschließenden Schrägstrich. Diese Null-Byte-Objekte werden unter [Organisieren von Objekten in der Amazon S3 S3-Konsole mithilfe von Ordern](#) im Amazon S3 S3-Benutzerhandbuch beschrieben.

Wenn Sie einen `ls` Befehl ausführen und einige Ergebnisse Amazon S3 S3-Null-Byte-Objekte sind (diese Objekte haben Schlüssel, die mit einem Schrägstrich enden), gibt Transfer Family eine `HeadObject` Anfrage für jedes dieser Objekte aus (Einzelheiten finden Sie [HeadObject](#) in der Amazon Simple Storage Service API-Referenz). Dies kann zu den folgenden Problemen führen, wenn Sie Amazon S3 als Speicher mit Transfer Family verwenden.

Gewähren Sie die Möglichkeit, nur Dateien zu schreiben und aufzulisten

In einigen Fällen möchten Sie möglicherweise nur Schreibzugriff auf Ihre Amazon S3 S3-Objekte anbieten. Beispielsweise möchten Sie möglicherweise Zugriff auf Schreib- (oder Upload) und Auflisten von Objekten in einem Bucket gewähren, nicht jedoch auf Objekte zum Lesen (Herunterladen). Um `mkdir` Befehle mithilfe von Dateiübertragungsclients ausführen zu können, benötigen Sie Amazon S3 `ListObjects` und die `PutObject` entsprechenden Berechtigungen. Wenn Transfer Family jedoch einen `HeadObject` Aufruf tätigen muss, um Dateien zu schreiben oder aufzulisten, schlägt der Anruf mit der Fehlermeldung Zugriff verweigert fehl, da für diesen Aufruf die `GetObject` entsprechende Genehmigung erforderlich ist.

Note

Wenn Sie einen Transfer Family Family-Server erstellen oder aktualisieren, können Sie die Leistung Ihrer Amazon S3 S3-Verzeichnisse optimieren, wodurch `HeadObject` Anrufe vermieden werden.

In diesem Fall können Sie Zugriff gewähren, indem Sie eine AWS Identity and Access Management (IAM-) Richtlinienbedingung hinzufügen, die die `GetObject` Berechtigung nur für Objekte hinzufügt,

die mit einem Schrägstrich (/) enden. Diese Bedingung verhindert das GetObject Aufrufen von Dateien (sodass sie nicht gelesen werden können), ermöglicht es dem Benutzer jedoch, Ordner aufzulisten und zu durchsuchen. Die folgende Beispielrichtlinie bietet nur Schreib- und Listenzugriff auf Ihre Amazon S3 S3-Buckets. Um diese Richtlinie zu verwenden, *amzn-s3-demo-bucket* ersetzen Sie sie durch den Namen Ihres Buckets.

 Note

Um das Upload-Verhalten von WinSCP zu korrigieren, stellen Sie sicher, dass Sie die "arn:aws:s3:::amzn-s3-demo-bucket/*.filepart" Zeile hinzufügen, wie in der folgenden Beispielrichtlinie aufgeführt. Diese Zeile gewährleistet die korrekte Behandlung von .filepart-Objekten, um Fehler zu vermeiden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListing",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AllowReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "DenyIfNotFolder",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ]
    }
  ]
}
```

```
    ],  
    "NotResource": [  
        "arn:aws:s3:::amzn-s3-demo-bucket/*/",  
        "arn:aws:s3:::amzn-s3-demo-bucket/*.filepart"  
    ]  
  }  
]  
}
```

Note

Diese Richtlinie erlaubt es Benutzern nicht, Dateien anzuhängen. Mit anderen Worten, ein Benutzer, dem diese Richtlinie zugewiesen wurde, kann keine Dateien öffnen, um ihnen Inhalte hinzuzufügen oder sie zu ändern. Wenn Ihr Anwendungsfall außerdem vor dem Hochladen einer Datei einen `HeadObject` Aufruf erfordert, funktioniert diese Richtlinie nicht für Sie.

Eine große Anzahl von Null-Byte-Objekten verursacht Latenzprobleme

Wenn Ihre Amazon S3 S3-Buckets eine große Anzahl dieser Null-Byte-Objekte enthalten, gibt Transfer Family viele `HeadObject` Aufrufe aus, was zu Verarbeitungsverzögerungen führen kann. Die empfohlene Lösung für dieses Problem besteht darin, `Optimized Directories` zu aktivieren, um die Latenz zu reduzieren.

Nehmen wir zum Beispiel an, Sie gehen in Ihr Home-Verzeichnis und Sie haben 10.000 Unterverzeichnisse. Mit anderen Worten, Ihr Amazon S3 S3-Bucket hat 10.000 Ordner. Wenn Sie in diesem Szenario den Befehl `ls` (`list`) ausführen, dauert der Listenvorgang zwischen sechs und acht Minuten. Wenn Sie Ihre Verzeichnisse optimieren, dauert dieser Vorgang jedoch nur wenige Sekunden. Sie legen diese Option während der Servererstellung oder -aktualisierung im Fenster [Zusätzliche Details konfigurieren](#) fest. Diese Verfahren werden unter dem [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#) Thema detailliert beschrieben.

Note

GUI-Clients geben möglicherweise einen `ls` Befehl aus, auf den Sie keinen Einfluss haben. Daher ist es wichtig, diese Einstellung zu aktivieren, wenn Sie können.

Wenn Sie Ihre Verzeichnisse nicht optimieren oder nicht optimieren können, besteht eine alternative Lösung für dieses Problem darin, alle Ihre Null-Byte-Objekte zu löschen. Beachten Sie Folgendes:

- Leere Verzeichnisse werden nicht mehr existieren. Verzeichnisse existieren nur, weil ihre Namen im Schlüssel eines Objekts stehen.
- Hindert jemanden nicht daran, erneut anzurufen `mkdir` und Dinge kaputt zu machen. Sie könnten dies mildern, indem Sie eine Richtlinie erstellen, die die Erstellung von Verzeichnissen verhindert.
- In einigen Szenarien werden diese 0-Byte-Objekte verwendet. Sie haben beispielsweise eine Struktur wie `inboxes/customer1000` und das Posteingangsverzeichnis wird jeden Tag gereinigt.

Schließlich besteht eine weitere mögliche Lösung darin, die Anzahl der sichtbaren Objekte durch eine Richtlinienbedingung zu begrenzen, um die Anzahl der `HeadObject` Aufrufe zu reduzieren. Damit dies eine praktikable Lösung ist, müssen Sie akzeptieren, dass Sie möglicherweise nur eine begrenzte Anzahl all Ihrer Unterverzeichnisse anzeigen können.

Ein Amazon EFS-Dateisystem konfigurieren

AWS Transfer Family greift auf Amazon Elastic File System (Amazon EFS) zu, um die Übertragungsanfragen Ihrer Benutzer zu bearbeiten. Daher müssen Sie im Rahmen der Einrichtung Ihres File-Transfer-Protokoll-fähigen Servers ein Amazon EFS-Dateisystem bereitstellen. Sie können ein vorhandenes Dateisystem verwenden oder ein neues erstellen.

Beachten Sie Folgendes:

- Wenn Sie einen Transfer Family Family-Server und ein Amazon EFS-Dateisystem verwenden, müssen sich der Server und das Dateisystem im selben System befinden AWS-Region.
- Der Server und das Dateisystem müssen sich nicht im selben Konto befinden. Wenn sich der Server und das Dateisystem nicht in demselben Konto befinden, muss die Dateisystemrichtlinie der Benutzerrolle eine ausdrückliche Genehmigung erteilen.

Informationen zum Einrichten mehrerer Konten finden Sie im AWS Organizations Benutzerhandbuch unter [Verwaltung der AWS Konten in Ihrer Organisation](#).

- Wenn Sie Ihre Benutzer einrichten, weisen Sie ihnen jeweils eine IAM-Rolle zu. Diese Rolle bestimmt die Zugriffsebene, die sie auf Ihr Amazon EFS-Dateisystem haben.
- Einzelheiten zum Mounten eines Amazon EFS-Dateisystems finden Sie unter Bereitstellen [von Amazon EFS-Dateisystemen](#).

Weitere Informationen zur Zusammenarbeit mit AWS Transfer Family Amazon EFS finden Sie unter [Verwenden für AWS Transfer Family den Zugriff auf Dateien in Ihrem Amazon EFS-Dateisystem](#) im Amazon Elastic File System-Benutzerhandbuch.

Besitz von Amazon EFS-Dateien

Amazon EFS verwendet das POSIX-Dateiberechtigungsmodell (Portable Operating System Interface), um den Dateibesitz darzustellen.

In POSIX werden Benutzer im System in drei verschiedene Berechtigungsklassen eingeteilt: Wenn Sie einem Benutzer den Zugriff auf Dateien ermöglichen, die in einem Amazon EFS-Dateisystem gespeichert sind AWS Transfer Family, müssen Sie ihm ein „POSIX-Profil“ zuweisen. Dieses Profil wird verwendet, um ihren Zugriff auf Dateien und Verzeichnisse im Amazon EFS-Dateisystem zu bestimmen.

- Benutzer (u): Besitzer der Datei oder des Verzeichnisses. Normalerweise ist der Ersteller einer Datei oder eines Verzeichnisses auch der Eigentümer.
- Gruppe (g): Gruppe von Benutzern, die identischen Zugriff auf Dateien und Verzeichnisse benötigen, die sie gemeinsam nutzen.
- Andere (o): Alle anderen Benutzer, die Zugriff auf das System haben, mit Ausnahme des Besitzers und der Gruppenmitglieder. Diese Berechtigungsklasse wird auch als „Öffentlich“ bezeichnet.

Im POSIX-Berechtigungsmodell ist jedes Dateisystemobjekt (Dateien, Verzeichnisse, symbolische Links, Named Pipes und Sockets) mit den zuvor genannten drei Berechtigungssätzen verknüpft. Amazon EFS-Objekten ist ein Unix-style Modus zugeordnet. Dieser Moduswert definiert die Berechtigungen zum Ausführen von Aktionen für dieses Objekt.

Darüber hinaus werden Benutzer und Gruppen auf Unix-style Systemen numerischen Identifikatoren zugeordnet, die Amazon EFS verwendet, um den Dateibesitz darzustellen. Bei Amazon EFS gehören Objekte einem einzelnen Besitzer und einer einzelnen Gruppe. Amazon EFS verwendet die zugeordneten numerischen IDs, um die Berechtigungen zu prüfen, wenn ein Benutzer versucht, auf ein Dateisystemobjekt zuzugreifen.

Amazon EFS-Benutzer für Transfer Family einrichten

Bevor Sie Ihre Amazon EFS-Benutzer einrichten, können Sie einen der folgenden Schritte ausführen:

- Sie können Benutzer erstellen und ihre Basisordner in Amazon EFS einrichten. Details dazu finden Sie unter [Transfer Family Family-Benutzer auf Amazon EFS konfigurieren](#).

- Wenn Sie mit dem Hinzufügen eines Root-Benutzers vertraut sind, können Sie das tun [Einen Amazon EFS-Root-Benutzer erstellen](#).

 Note

Transfer Family Family-Server unterstützen keine Amazon EFS-Zugriffspunkte zur Festlegung von POSIX-Berechtigungen. Die POSIX-Profile von Transfer Family Family-Benutzern (im vorherigen Abschnitt beschrieben) bieten die Möglichkeit, POSIX-Berechtigungen festzulegen. Diese Berechtigungen werden auf Benutzerebene für einen detaillierten Zugriff auf der Grundlage von UID, GID und sekundären GIDs festgelegt.

Transfer Family Family-Benutzer auf Amazon EFS konfigurieren

Transfer Family ordnet die Benutzer den von Ihnen angegebenen Verzeichnissen UID/GID und zu. Wenn sie noch UID/GID/directories nicht in EFS vorhanden sind, sollten Sie sie erstellen, bevor Sie sie in Transfer an einen Benutzer zuweisen. Die Einzelheiten zum Erstellen von Amazon EFS-Benutzern werden unter [Arbeiten mit Benutzern, Gruppen und Berechtigungen auf Netzwerkdateisystemebene \(NFS\)](#) im Amazon Elastic File System-Benutzerhandbuch beschrieben.

Schritte zum Einrichten von Amazon EFS-Benutzern in Transfer Family

1. Ordnen Sie die EFS-UID und GID für Ihren Benutzer in Transfer Family mithilfe der [PosixProfile](#)Felder zu.
2. Wenn Sie möchten, dass der Benutzer bei der Anmeldung in einem bestimmten Ordner startet, können Sie das EFS-Verzeichnis unter dem [HomeDirectory](#)Feld angeben.

Sie können den Prozess automatisieren, indem Sie eine CloudWatch Regel und eine Lambda-Funktion verwenden. Ein Beispiel für eine Lambda-Funktion, die mit EFS interagiert, finden Sie unter [Verwenden von Amazon EFS für AWS Lambda in Ihren serverlosen Anwendungen](#).

Darüber hinaus können Sie logische Verzeichnisse für Ihre Transfer Family Family-Benutzer konfigurieren. Einzelheiten finden Sie im [Logische Verzeichnisse für Amazon EFS konfigurieren](#) Abschnitt des [Verwendung logischer Verzeichnisse zur Vereinfachung Ihrer Transfer Family Family-Verzeichnisstrukturen](#) Themas.

Einen Amazon EFS-Root-Benutzer erstellen

Wenn Ihr Unternehmen bereit ist, den Root-Benutzerzugriff SFTP/FTPS für die Konfiguration Ihrer Benutzer zu aktivieren, können Sie einen Benutzer erstellen, dessen UID und GID 0 sind (Root-Benutzer), und dann diesen Root-Benutzer verwenden, um Ordner zu erstellen und den übrigen Benutzern POSIX-ID-Besitzer zuzuweisen. Der Vorteil dieser Option besteht darin, dass das Amazon EFS-Dateisystem nicht bereitgestellt werden muss.

Führen Sie die unter beschriebenen Schritte aus und geben Sie sowohl für die Benutzer-ID als auch für die Gruppen-ID 0 (Null) ein. [Hinzufügen von vom Service verwalteten Amazon EFS-Benutzern](#)

Tip

Lassen Sie dieses Superuser-Konto nicht länger als nötig bestehen. Oder, falls Sie das Root-Benutzerkonto behalten, stellen Sie sicher, dass Sie es gut schützen.

Unterstützte Amazon EFS-Befehle

Die folgenden Befehle werden für Amazon EFS for unterstützt AWS Transfer Family.

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: Nur Root-Benutzer (d. h. Benutzer mit uid=0) können den Besitz und die Berechtigungen von Dateien und Verzeichnissen ändern.
- `chmod`: Nur Root kann den Besitz und die Berechtigungen von Dateien und Verzeichnissen ändern.
- `chgrp`: Wird entweder für Root-Benutzer oder für den Eigentümer der Datei unterstützt, der die Gruppe einer Datei nur in eine seiner sekundären Gruppen ändern kann.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`

- `rmdir`
- `chmtime`

Erstellen Sie eine IAM-Rolle und -Richtlinie

In diesem Thema werden die Arten von Richtlinien und Rollen beschrieben, die zusammen mit Benutzerrollen verwendet werden können AWS Transfer Family, und der Prozess der Erstellung einer Benutzerrolle wird schrittweise beschrieben. Außerdem wird beschrieben, wie Sitzungsrichtlinien funktionieren, und es wird ein Beispiel für eine Benutzerrolle bereitgestellt.

AWS Transfer Family verwendet die folgenden Rollentypen:

- **Benutzerrolle** — Ermöglicht dienstverwalteten Benutzern den Zugriff auf die erforderlichen Transfer Family Family-Ressourcen. AWS Transfer Family nimmt diese Rolle im Kontext eines Transfer Family Family-Benutzer-ARN an.
- **Zugriffsrolle** — Ermöglicht den Zugriff nur auf die Amazon S3 S3-Dateien, die übertragen werden. Für eingehende AS2-Übertragungen verwendet die Zugriffsrolle den Amazon-Ressourcennamen (ARN) für die Vereinbarung. Für ausgehende AS2-Übertragungen verwendet die Zugriffsrolle den ARN für den Connector.
- **Aufruflerrolle** — Zur Verwendung mit Amazon API Gateway als benutzerdefiniertem Identitätsanbieter des Servers. Transfer Family übernimmt diese Rolle im Kontext eines Transfer Family Family-Servers ARN.
- **Rolle „Protokollierung“** — Wird verwendet, um Einträge bei Amazon zu protokollieren CloudWatch. Transfer Family verwendet diese Rolle, um Erfolgs- und Fehlschlagsdetails sowie Informationen zu Dateiübertragungen zu protokollieren. Transfer Family übernimmt diese Rolle im Kontext eines Transfer Family Family-Servers ARN. Für ausgehende AS2-Übertragungen verwendet die Protokollierungsrolle den Connector-ARN.
- **Ausführungsrolle** — Ermöglicht es einem Transfer Family Family-Benutzer, Workflows aufzurufen und zu starten. Transfer Family übernimmt diese Rolle im Zusammenhang mit einem Transfer Family Family-Workflow-ARN.

Zusätzlich zu diesen Rollen können Sie auch Sitzungsrichtlinien verwenden. Eine Sitzungsrichtlinie wird verwendet, um den Zugriff bei Bedarf einzuschränken. Beachten Sie, dass es sich bei diesen Richtlinien um eigenständige Richtlinien handelt, d. h., Sie fügen diese Richtlinien keiner Rolle hinzu. Stattdessen fügen Sie einem Transfer Family Family-Benutzer direkt eine Sitzungsrichtlinie hinzu.

 Note

Wenn Sie einen vom Dienst verwalteten Transfer Family Family-Benutzer erstellen, können Sie eine Auto-generate Richtlinie basierend auf dem Basisordner auswählen. Dies ist eine nützliche Tastenkombination, wenn Sie den Benutzerzugriff auf ihre eigenen Ordner einschränken möchten. Einzelheiten zu Sitzungsrichtlinien und ein Beispiel finden Sie auch unter [So funktionieren Sitzungsrichtlinien](#). Weitere Informationen zu Sitzungsrichtlinien finden Sie auch unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Themen

- [Eine Benutzerrolle erstellen](#)
- [So funktionieren Sitzungsrichtlinien](#)
- [Beispiel für eine read/write Zugriffsrichtlinie](#)

Eine Benutzerrolle erstellen

Wenn Sie einen Benutzer erstellen, treffen Sie eine Reihe von Entscheidungen über den Benutzerzugriff. Zu diesen Entscheidungen gehört, auf welche Amazon S3 S3-Buckets oder Amazon EFS-Dateisysteme der Benutzer zugreifen kann, auf welche Teile jedes Amazon S3 S3-Buckets und auf welche Dateien im Dateisystem zugegriffen werden kann und welche Berechtigungen der Benutzer hat (z. B. PUT oder GET).

Um den Zugriff festzulegen, erstellen Sie eine identitätsbasierte AWS Identity and Access Management (IAM) -Richtlinie und Rolle, die diese Zugriffsinformationen bereitstellen. Im Rahmen dieses Prozesses gewähren Sie Ihrem Benutzer Zugriff auf den Amazon S3-Bucket oder das Amazon EFS-Dateisystem, das das Ziel oder die Quelle für Dateioperationen ist. Die folgenden grundlegenden Schritte, die im Weiteren detailliert erläutert werden, skizzieren das Verfahren:

Eine Benutzerrolle erstellen

1. Erstellen Sie eine IAM-Richtlinie für AWS Transfer Family. Dieser Vorgang wird unter [Um eine IAM-Richtlinie zu erstellen für AWS Transfer Family](#) beschrieben.
2. Erstellen Sie eine IAM-Rolle und fügen Sie die neue IAM-Richtlinie an. Ein Beispiel finden Sie unter [Beispiel für eine read/write Zugriffsrichtlinie](#).
3. Stellen Sie eine Vertrauensbeziehung zwischen AWS Transfer Family und der IAM-Rolle her. Dieser Vorgang wird unter [So stellen Sie eine Vertrauensbeziehung her](#) beschrieben.

In den folgenden Verfahren wird beschrieben, wie eine IAM-Richtlinie und -Rolle erstellt wird.

Um eine IAM-Richtlinie zu erstellen für AWS Transfer Family

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Richtlinien und dann Richtlinie erstellen.
3. Wählen Sie auf der Seite Create Policy (Richtlinie erstellen) die Registerkarte JSON aus.
4. Ersetzen Sie im daraufhin angezeigten Editor den Inhalt des Editors durch die IAM-Richtlinie, die Sie der IAM-Rolle zuordnen möchten.

Sie können Benutzern read/write Zugriff gewähren oder sie auf ihr Home-Verzeichnis beschränken. Weitere Informationen finden Sie unter [Beispiel für eine read/write Zugriffsrichtlinie](#).

5. Wählen Sie Richtlinie überprüfen aus, geben Sie einen Namen und eine Beschreibung für Ihre Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.

Nun erstellen Sie eine IAM-Rolle und fügen an diese die neue IAM-Richtlinie an.

Um eine IAM-Rolle zu erstellen für AWS Transfer Family

1. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.

Vergewissern Sie sich, dass auf der Seite Rolle erstellen der AWS Dienst ausgewählt ist.

2. Wählen Sie in der Service-Liste Transfer (Übertragung) und dann Next: Permissions (Weiter: Berechtigungen) aus. Dadurch wird eine Vertrauensbeziehung zwischen AWS Transfer Family und hergestellt AWS.
3. Suchen Sie im Abschnitt Berechtigungsrichtlinien anhängen nach der Richtlinie, die Sie gerade erstellt haben, wählen Sie sie aus und klicken Sie dann auf Weiter: Tags.
4. (Optional) Geben Sie einen Schlüssel und einen Wert für ein Tag ein und wählen Sie Next: Review (Weiter: Prüfen) aus.
5. Geben Sie auf der Seite Review (Prüfen) einen Namen und eine Beschreibung für die neue Rolle ein und wählen Sie dann Create role (Rolle erstellen) aus.

Als Nächstes richten Sie eine Vertrauensbeziehung zwischen AWS Transfer Family und ein AWS.

So stellen Sie eine Vertrauensbeziehung her

Note

In unseren Beispielen verwenden wir `ArnLike` sowohl als auch `ArnEquals`. Sie sind funktionell identisch, weshalb Sie beide verwenden können, wenn Sie Ihre Richtlinien erstellen. Die Dokumentation Transfer Family verwendet `ArnLike`, wenn die Bedingung ein Platzhalterzeichen enthält, und `ArnEquals` um eine exakte Übereinstimmungsbedingung anzugeben.

1. Wählen Sie in der IAM-Konsole die von Ihnen eben erstellte Rolle aus.
2. Wählen Sie auf der Seite Summary (Übersicht) die Option Trust relationships (Vertrauensbeziehungen) und anschließend Edit trust relationship (Vertrauensbeziehung bearbeiten) aus.
3. Stellen Sie im Editor „Vertrauensverhältnis bearbeiten“ sicher, dass der Dienst aktiviert ist `transfer.amazonaws.com`. Die Zugriffsrichtlinie wird im Folgenden dargestellt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Wir empfehlen Ihnen, die Zustandsschlüssel `aws:SourceAccount` und `aws:SourceArn` zu verwenden, um sich vor dem Problem der verwechselten Stellvertreter zu schützen. Das Quellkonto ist der Besitzer des Servers und der Quell-ARN ist der ARN des Benutzers. Beispiel:

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
```

```
    },  
    "ArnLike": {  
        "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"  
    }  
}
```

Sie können die ArnLike Bedingung auch verwenden, wenn Sie die Einschränkung auf einen bestimmten Server statt auf einen beliebigen Server im Benutzerkonto vornehmen möchten. Beispiel:

```
"Condition": {  
    "ArnLike": {  
        "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"  
    }  
}
```

 Note

Ersetzen Sie in den obigen Beispielen jedes *user input placeholder* durch Ihre eigenen Informationen.

Einzelheiten zum Problem mit dem verwirrten Stellvertreter und weitere Beispiele finden Sie unter [Cross-service verwirrter Stellvertreter, Prävention](#).

4. Wählen Sie „Vertrauensrichtlinie aktualisieren“, um die Zugriffsrichtlinie zu aktualisieren.

Sie haben jetzt eine IAM-Rolle erstellt, die es AWS Transfer Family ermöglicht, AWS Dienste in Ihrem Namen aufzurufen. Sie haben der Rolle die IAM-Richtlinie angehängt, die Sie erstellt haben, um Ihrem Benutzer Zugriff zu gewähren. In diesem [Erste Schritte mit AWS Transfer Family Server-Endpunkten](#) Abschnitt werden diese Rolle und Richtlinie Ihrem oder Ihren Benutzern zugewiesen.

Informationen finden Sie auch unter:

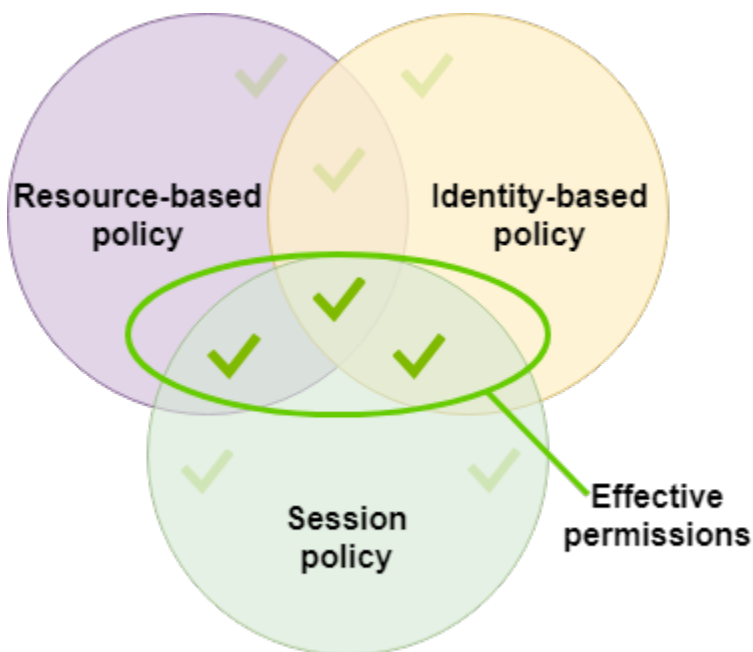
- Weitere allgemeine Informationen zu IAM-Rollen finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst](#).
- Weitere Informationen zu identitätsbasierten Richtlinien für Amazon S3-Ressourcen finden Sie unter [Identitäts- und Zugriffsmanagement in Amazon S3](#) im Amazon Simple Storage Service-Benutzerhandbuch.

- Weitere Informationen zu identitätsbasierten Richtlinien für Amazon EFS-Ressourcen finden Sie unter [Verwenden von IAM zur Steuerung des Dateisystemdatenzugriffs](#) im Amazon Elastic File System-Benutzerhandbuch.

So funktionieren Sitzungsrichtlinien

Wenn ein Administrator eine Rolle erstellt, umfasst die Rolle häufig umfassende Berechtigungen, die mehrere Anwendungsfälle oder Teammitglieder abdecken. Wenn ein Administrator eine [Konsolen-URL](#) konfiguriert, kann er mithilfe einer Sitzungsrichtlinie die Berechtigungen für die resultierende Sitzung reduzieren. Wenn Sie beispielsweise eine Rolle mit [read/write Zugriff](#) erstellen, können Sie eine URL einrichten, die den Zugriff der Benutzer nur auf ihre Home-Verzeichnisse beschränkt.

Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie programmgesteuert eine temporäre Sitzung für eine Rolle oder einen Benutzer erstellen. Sitzungsrichtlinien sind nützlich, um Benutzer zu sperren, sodass sie nur Zugriff auf Bereiche Ihres Buckets haben, in denen Objektpräfixe ihren Benutzernamen enthalten. Das folgende Diagramm zeigt, dass die Berechtigungen der Sitzungsrichtlinie die Schnittmenge der Sitzungsrichtlinien und der ressourcenbasierten Richtlinien sowie die Schnittmenge der Sitzungsrichtlinien und identitätsbasierten Richtlinien bilden.



Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

In AWS Transfer Family, eine Sitzungsrichtlinie wird nur unterstützt, wenn Sie zu oder von Amazon S3 übertragen. Die folgende Beispielrichtlinie ist eine Sitzungsrichtlinie, die den Zugriff von Benutzern nur auf ihre home Verzeichnisse beschränkt. Beachten Sie Folgendes:

- Die PutObjectACL Anweisungen GetObjectACL und sind nur erforderlich, wenn Sie den kontenübergreifenden Zugriff aktivieren müssen. Das heißt, Ihr Transfer Family Family-Server muss auf einen Bucket in einem anderen Konto zugreifen.
- Die maximale Länge einer Sitzungsrichtlinie beträgt 2048 Zeichen. Weitere Informationen finden Sie unter dem [Anforderungsparameter Policy](#) für die CreateUser Aktion in der API-Referenz.
- Wenn Ihr Amazon S3 S3-Bucket mit AWS Key Management Service (AWS KMS) verschlüsselt ist, müssen Sie in Ihrer Richtlinie zusätzliche Berechtigungen angeben. Details hierzu finden Sie unter [Datenschutz und Verschlüsselung](#).
- Informationen zur Verwendung von Sitzungsrichtlinien zur Erstellung von Zugriffsberechtigungen auf der Grundlage von Benutzerattributen, ohne separate IAM-Rollen für jeden Benutzer zu erstellen, finden Sie unter [Dynamische Ansätze zur Rechteverwaltung](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    },
    {
      "Sid": "HomeDirObjectAccess",
```

```

        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
    }
}

```

Note

Im obigen Richtlinienbeispiel wird davon ausgegangen, dass die Basisverzeichnisse der Benutzer so eingestellt sind, dass sie einen abschließenden Schrägstrich enthalten, um anzuzeigen, dass es sich um ein Verzeichnis handelt. Wenn Sie dagegen das eines Benutzers HomeDirectory ohne den abschließenden Schrägstrich angeben, sollten Sie es in Ihre Richtlinie aufnehmen.

Beachten Sie in der vorherigen Beispielrichtlinie die Verwendung der `transfer:HomeFolder` `transfer:HomeDirectory` Richtlinienparameter `transfer:HomeBucket`, und. Diese Parameter werden für den festgelegt `HomeDirectory`, der für den Benutzer konfiguriert ist, wie unter [HomeDirectory](#) und beschrieben [Implementierung Ihrer API-Gateway-Methode](#). Diese Parameter haben die folgenden Definitionen:

- Der `transfer:HomeBucket` Parameter wird durch die erste Komponente von `ersetztHomeDirectory`.
- Der `transfer:HomeFolder` Parameter wird durch die verbleibenden Teile des `HomeDirectory` Parameters ersetzt.
- Für den `transfer:HomeDirectory` Parameter wurde der führende Schrägstrich (/) entfernt, sodass er als Teil eines S3-Amazon-Ressourcennamens (ARN) in einer `Resource` Anweisung verwendet werden kann.

 Note

Wenn Sie logische Verzeichnisse verwenden, also die Verzeichnisse des `homeDirectoryType` Benutzers, werden LOGICAL diese Richtlinienparameter (`HomeBucketHomeDirectory`, und `HomeFolder`) nicht unterstützt.

Nehmen wir beispielsweise an, dass der `HomeDirectory` Parameter, der für den Transfer Family Family-Benutzer konfiguriert ist, lautet `/home/bob/amazon/stuff/`.

- ist `transfer:HomeBucket` auf `/home` gesetzt.
- ist `transfer:HomeFolder` auf `/bob/amazon/stuff/` gesetzt.
- `transfer:HomeDirectory` wird `home/bob/amazon/stuff/`.

Die erste "Sid" ermöglicht es dem Benutzer, alle Verzeichnisse aufzulisten, beginnend mit `/home/bob/amazon/stuff/`.

Die zweite "Sid" schränkt den `get` Zugriff des Benutzers `put` auf denselben Pfad ein, `/home/bob/amazon/stuff/`.

Beispiel für eine read/write Zugriffsrichtlinie

read/write Zugriff auf den Amazon S3 S3-Bucket gewähren

Die folgende Beispielrichtlinie AWS Transfer Family gewährt read/write Zugriff auf Objekte in Ihrem Amazon S3 S3-Bucket.

Beachten Sie Folgendes:

- Ersetzen Sie `amzn-s3-demo-bucket` durch den Namen Ihres Amazon-S3-Buckets.
- Die `PutObjectACL` Anweisungen `GetObjectACL` und sind nur erforderlich, wenn Sie den kontoübergreifenden Zugriff aktivieren müssen. Das heißt, Ihr Transfer Family Family-Server muss auf einen Bucket in einem anderen Konto zugreifen.
- Die `DeleteObjectVersion` Anweisungen `GetObjectVersion` und sind nur erforderlich, wenn die Versionierung für den Amazon S3 S3-Bucket aktiviert ist, auf den zugegriffen wird.

Note

Wenn Sie jemals die Versionierung für Ihren Bucket aktiviert haben, benötigen Sie diese Berechtigungen, da Sie die Versionierung in Amazon S3 nur aussetzen und nicht vollständig ausschalten können. Weitere Informationen finden Sie unter Buckets [ohne Version, mit aktivierter Versionsverwaltung und Sperrung der Versionierung](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```


Dateisystemzugriff auf Dateien im Amazon EFS-Dateisystem gewähren

Note

Zusätzlich zur Richtlinie müssen Sie auch sicherstellen, dass Ihre POSIX-Dateiberechtigungen den entsprechenden Zugriff gewähren. Weitere Informationen finden Sie unter [Arbeiten mit Benutzern, Gruppen und Berechtigungen auf Netzwerkdateisystem \(NFS\)-Ebene](#) im Benutzerhandbuch für Amazon Elastic File System.

Die folgende Beispielrichtlinie gewährt Root-Dateisystemzugriff auf Dateien in Ihrem Amazon EFS-Dateisystem.

Note

Ersetzen Sie in den folgenden Beispielen *region* durch Ihre Region, *account-id* das Konto, in dem sich die Datei befindet, und *file-system-id* durch die ID Ihres Amazon Elastic File System (Amazon EFS).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RootFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
    }
  ]
}
```

Die folgende Beispielrichtlinie gewährt Benutzerdateisystemzugriff auf Dateien in Ihrem Amazon EFS-Dateisystem.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UserFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
    }
  ]
}
```

Familiëntutorials übertragen

Das AWS Transfer Family Benutzerhandbuch bietet detaillierte Anleitungen für verschiedene Anwendungsfälle.

- [Erste Schritte mit AWS Transfer Family Server-Endpunkten](#)- Erstellen Sie einen SFTP Transfer Family Family-Server mit einem vom Service verwalteten Benutzer und übertragen Sie Dateien mithilfe eines Clients.
- [Einrichtung und Verwendung von SFTP-Anschlüssen](#)- Richten Sie einen SFTP-Connector ein, um Dateien zwischen Amazon S3 S3-Speicher und einem SFTP-Server zu übertragen.
- [Einrichtung einer Amazon API Gateway Gateway-Methode als benutzerdefinierter Identitätsanbieter](#)- Konfigurieren Sie eine Amazon API Gateway Gateway-Methode als benutzerdefinierten Identitätsanbieter für das Hochladen von Dateien auf einen AWS Transfer Family Server.
- [Einen verwalteten Workflow für die Entschlüsselung einer Datei einrichten](#)- Erstellen Sie einen verwalteten Workflow zum Entschlüsseln von Dateien, zum Hochladen verschlüsselter Dateien auf Amazon S3 und zum Anzeigen entschlüsselter Inhalte.
- [Einrichtung einer AS2-Konfiguration](#)- Richten Sie einen AS2 Transfer Family Family-Server ein, einschließlich Zertifikatsimport, Profil- und Vereinbarungserstellung, optionaler AS2-Connectorkonfiguration und Tests.
- Die folgenden Tutorials führen Sie durch die Erstellung und Konfiguration von Transfer Family Family-Webanwendungen. Wählen Sie das Tutorial, das Ihren Bedürfnissen am besten entspricht:

[Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#)- Erfahren Sie, wie Sie eine Transfer Family Family-Webanwendung erstellen und konfigurieren.

[Tutorial: AWS Transfer Family Web-App mit selektivem Multi-Bucket-Zugriff einrichten](#)- Konfigurieren Sie eine Transfer Family Family-Webanwendung mit detaillierten Amazon S3 S3-Bucket-Berechtigungen für einen einzelnen Benutzer.

Themen

- [Erste Schritte mit AWS Transfer Family Server-Endpunkten](#)
- [Einen verwalteten Workflow für die Entschlüsselung einer Datei einrichten](#)
- [Einrichtung und Verwendung von SFTP-Anschlüssen](#)

- [Einrichtung einer Amazon API Gateway Gateway-Methode als benutzerdefinierter Identitätsanbieter](#)
- [Einrichtung einer AS2-Konfiguration](#)
- [Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#)
- [Tutorial: AWS Transfer Family Web-App mit selektivem Multi-Bucket-Zugriff einrichten](#)

Erste Schritte mit AWS Transfer Family Server-Endpunkten

Verwenden Sie dieses Tutorial, um mit AWS Transfer Family (Transfer Family) zu beginnen. Sie erfahren, wie Sie mithilfe von Amazon S3 S3-Speicher einen SFTP-enabled Server mit öffentlich zugänglichem Endpunkt erstellen, einen Benutzer mit service-verwalteter Authentifizierung hinzufügen und eine Datei mit Cyberduck übertragen.

Themen

- [Voraussetzungen](#)
- [Schritt 1: Melden Sie sich bei der AWS Transfer Family Konsole an](#)
- [Schritt 2: Einen SFTP-enabled Server erstellen](#)
- [Schritt 3: Fügen Sie einen vom Service verwalteten Benutzer hinzu](#)
- [Schritt 4: Eine Datei mit einem Client übertragen](#)

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Anforderungen unter erfüllen. [Voraussetzungen](#)
Im Rahmen dieser Einrichtung erstellen Sie einen Amazon Simple Storage Service (Amazon S3) - Bucket und eine AWS Identity and Access Management (IAM) -Benutzerrolle.

Es sind Berechtigungen für die Verwendung der AWS Transfer Family Konsole erforderlich, und es sind Berechtigungen für die Konfiguration anderer AWS Dienste erforderlich, die Transfer Family verwendet, wie Amazon Simple Storage Service AWS Certificate Manager, Amazon Elastic File System und Amazon Route 53. Erteilt beispielsweise Benutzern, die AWS mit Transfer Family Dateien in und aus Transfer Family übertragen, Berechtigungen AmazonS3FullAccesszum Einrichten und Verwenden eines Amazon S3 S3-Buckets. Einige der Berechtigungen in dieser Richtlinie sind erforderlich, um Amazon S3 S3-Buckets zu erstellen.

Um die Transfer Family Family-Konsole verwenden zu können, benötigen Sie Folgendes:

- `AWSTransferConsoleFullAccess` gewährt Ihrem SFTP-Benutzer Berechtigungen zum Erstellen von Transfer Family Family-Ressourcen.
- `IAMFullAccess` (oder speziell eine Richtlinie, die die Erstellung von IAM-Rollen ermöglicht) ist nur erforderlich, wenn Sie möchten, dass Transfer Family automatisch eine Protokollierungsrolle für Ihren Server in Amazon CloudWatch Logs oder eine Benutzerrolle für einen Benutzer erstellt, der sich bei einem Server anmeldet.
- Um VPC-Servertypen zu erstellen und zu löschen, müssen Sie Ihrer Richtlinie die Aktionen `ec2:CreateVpcEndpoint` und `ec2:DeleteVpcEndpoints` hinzufügen. Informationen zur Beschränkung des VPC-Endpunktzugriffs aus Sicherheitsgründen finden Sie unter [Beschränkung des VPC-Endpunktzugriffs für Transfer Family Family-Server](#).

 Note

Die `IAMFullAccess` Richtlinien `AmazonS3FullAccess` und selbst sind für die allgemeine Verwendung von nicht erforderlich. AWS Transfer Family Sie werden hier vorgestellt, um auf einfache Weise sicherzustellen, dass alle von Ihnen benötigten Berechtigungen abgedeckt sind. Darüber hinaus handelt AWS es sich um verwaltete Richtlinien, bei denen es sich um Standardrichtlinien handelt, die allen AWS Kunden zur Verfügung stehen. Sie können die einzelnen Berechtigungen in diesen Richtlinien einsehen und festlegen, welche Mindestberechtigungen Sie für Ihre Zwecke benötigen.

Schritt 1: Melden Sie sich bei der AWS Transfer Family Konsole an

Um sich bei Transfer Family anzumelden

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Geben Sie als Konto-ID oder Alias die ID für Ihr Konto ein AWS-Konto.
3. Geben Sie als IAM-Benutzername den Namen der Benutzerrolle ein, die Sie für Transfer Family erstellt haben.
4. Geben Sie unter Passwort Ihr AWS Kontopasswort ein.
5. Klicken Sie auf Sign in.

Schritt 2: Einen SFTP-enabled Server erstellen

Das Secure Shell (SSH) File Transfer Protocol (SFTP) ist ein Netzwerkprotokoll, das für die sichere Übertragung von Daten über das Internet verwendet wird. Das Protokoll unterstützt die volle Sicherheits- und Authentifizierungsfunktionalität von SSH. Es wird häufig für den Austausch von Daten, einschließlich sensibler Informationen, zwischen Geschäftspartnern in einer Vielzahl von Branchen wie Finanzdienstleistungen, Gesundheitswesen, Einzelhandel und Werbung verwendet.

Um einen SFTP-enabled Server zu erstellen

1. Wählen Sie im Navigationsbereich Server und dann Server erstellen aus.
2. Wählen Sie unter Protokolle auswählen die Option SFTP und dann Weiter aus.
3. Wählen Sie unter Wählen Sie einen Identitätsanbieter die Option Service managed to storage user identities and keys in Transfer Family aus, und klicken Sie dann auf Weiter.
4. Gehen Sie unter Endpunkt auswählen wie folgt vor:
 - a. Wählen Sie als Endpunktyp den Typ Öffentlich zugänglicher Endpunkt aus.
 - b. Wählen Sie für Benutzerdefinierter Hostname die Option Keine aus.
 - c. Wählen Sie Weiter aus.
5. Wählen Sie unter Domain auswählen die Option Amazon S3 aus.
6. Wählen Sie unter Zusätzliche Details konfigurieren unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind. Unsere neueste Sicherheitsrichtlinie ist die Standardeinstellung: Einzelheiten finden Sie unter [Sicherheitsrichtlinien für Server AWS Transfer Family](#)

Note

Nur wenn Sie einen verwalteten Workflow für Ihren Server hinzufügen, wählen Sie Neue Rolle für die CloudWatchProtokollierung erstellen. Um Serverereignisse zu protokollieren, müssen Sie keine IAM-Rolle erstellen.

7. Wählen Sie unter Überprüfen und erstellen die Option Server erstellen aus. Sie werden zur Seite Server weitergeleitet.

Es kann einige Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Zu diesem Zeitpunkt kann Ihr Server Dateioperationen ausführen, aber Sie müssen zuerst einen Benutzer erstellen. Einzelheiten zum Erstellen von Benutzern finden Sie unter [Benutzer für Serverendpunkte verwalten](#).

Schritt 3: Fügen Sie einen vom Service verwalteten Benutzer hinzu

Um einen Benutzer zum SFTP-enabled Server hinzuzufügen

1. Wählen Sie auf der Seite Server den Server aus, zu dem Sie einen Benutzer hinzufügen möchten.
2. Wählen Sie Benutzer hinzufügen.
3. Geben Sie im Abschnitt Benutzerkonfiguration unter Benutzername den Benutzernamen ein. Dieser Benutzername muss mindestens 3 und maximal 100 Zeichen lang sein. Sie können die folgenden Zeichen im Benutzernamen verwenden: a—z, 0—9 A-Z, Unterstrich '_', Bindestrich '-', Punkt '.' und das Zeichen '@'. Der Benutzername darf nicht mit einem Bindestrich '-', einem Punkt '.' oder einem Zeichen '@' beginnen.
4. Wählen Sie für Access die IAM-Rolle aus, die Sie in erstellt haben. [Erstellen Sie eine IAM-Rolle und -Richtlinie](#) Diese IAM-Rolle umfasst eine IAM-Richtlinie, die Berechtigungen für den Zugriff auf Ihren Amazon S3 S3-Bucket sowie eine Vertrauensbeziehung mit dem AWS Transfer Family Service enthält. Das unter beschriebene Verfahren [So stellen Sie eine Vertrauensbeziehung her](#) zeigt, wie Sie die richtige Vertrauensbeziehung aufbauen.
5. Wählen Sie für Richtlinie die Option Keine aus.
6. Wählen Sie für das Home-Verzeichnis den Amazon S3 S3-Bucket aus, in dem Sie die Daten speichern möchten, mit denen Sie die Daten übertragen AWS Transfer Family. Geben Sie den Pfad zum home Verzeichnis ein. Dies ist das Verzeichnis, das Ihren Benutzern angezeigt wird, wenn sie sich mit ihrem Client anmelden.

Wir empfehlen, einen Verzeichnispfad zu verwenden, der den Benutzernamen enthält, sodass Sie die Möglichkeit haben, eine Sitzungsrichtlinie zu verwenden. Eine Sitzungsrichtlinie beschränkt den Zugriff eines Benutzers im Amazon S3 S3-Bucket auf das home Verzeichnis dieses Benutzers. Weitere Informationen zur Verwendung von Sitzungsrichtlinien finden Sie unter [So funktionieren Sitzungsrichtlinien](#).

Wenn Sie möchten, können Sie diesen Parameter leer lassen, um das root Verzeichnis Ihres Amazon S3 S3-Buckets zu verwenden. Wenn Sie diese Option wählen, stellen Sie sicher, dass Ihre IAM-Rolle Zugriff auf das root Verzeichnis bietet.

7. Aktivieren Sie das Kontrollkästchen **Eingeschränkt**, um zu verhindern, dass Ihre Benutzer auf Inhalte außerhalb ihres home Verzeichnisses zugreifen. Dadurch wird auch verhindert, dass Benutzer den Amazon S3 S3-Bucket- oder Ordernamen sehen.
8. Geben Sie für den öffentlichen SSH-Schlüssel den öffentlichen SSH-Schlüsselteil des SSH-Schlüsselpaars im Format ein. `ssh-rsa <string>`

Ihr Schlüssel muss vom Dienst validiert werden, bevor Sie Ihren neuen Benutzer hinzufügen können. Weitere Hinweise zum Generieren eines SSH-Schlüsselpaars finden Sie unter [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).
9. (Optional) Geben Sie für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie Tag hinzufügen aus.
10. Wählen Sie **Add (Hinzufügen)**, um den neuen Benutzer dem ausgewählten Server hinzuzufügen.

Der neue Benutzer wird auf der Seite mit den Serverdetails im Bereich Benutzer angezeigt.

Schritt 4: Eine Datei mit einem Client übertragen

Sie übertragen Dateien über den AWS Transfer Family Service, indem Sie den Übertragungsvorgang in einem Client angeben. AWS Transfer Family unterstützt mehrere Clients. Details hierzu finden Sie unter [Übertragung von Dateien über einen Serverendpunkt mit einem Client](#)

Dieser Abschnitt enthält Verfahren zur Verwendung von Cyberduck und OpenSSH.

Themen

- [Verwenden Sie Cyberduck](#)
- [OpenSSH verwenden](#)

Verwenden Sie Cyberduck

Um Dateien AWS Transfer Family mit Cyberduck zu übertragen

1. Öffnen Sie den [Cyberduck-Client](#).
2. Wählen Sie **Verbindung öffnen**.
3. Wählen Sie im Dialogfeld „Verbindung öffnen“ die Option SFTP (SSH File Transfer Protocol).
4. Geben Sie für Server Ihren Serverendpunkt ein. Der Serverendpunkt befindet sich auf der Seite mit den Serverdetails, siehe [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#).

5. Geben Sie als Portnummer den Wert **22** für SFTP ein.
6. Geben Sie in das Feld Username (Benutzername) den Namen des Benutzers ein, den Sie in [Benutzer für Serverendpunkte verwalten](#) erstellt haben.
7. Wählen Sie für SSH Private Key den privaten SSH-Schlüssel aus oder geben Sie ihn ein.
8. Wählen Sie Connect aus.
9. Führen Sie Ihre Dateiübertragung durch.

Führen Sie nun – abhängig von der Position der Dateien – einen der folgenden Schritte durch:

- Wählen Sie in Ihrem lokalen Verzeichnis (der Quelle) die Dateien aus, die Sie übertragen möchten, und ziehen Sie sie per Drag & Drop in das Amazon S3 S3-Verzeichnis (das Ziel).
- Wählen Sie im Amazon S3 S3-Verzeichnis (der Quelle) die Dateien aus, die Sie übertragen möchten, und ziehen Sie sie per Drag & Drop in Ihr lokales Verzeichnis (das Ziel).

OpenSSH verwenden

Unten wird beschrieben, wie Dateien in der Befehlszeile mit OpenSSH übertragen werden.

Note

Dieser Client funktioniert nur mit einem SFTP-enabled Server.

Um Dateien AWS Transfer Family mit dem OpenSSH-Befehlszeilenprogramm zu übertragen

1. Öffnen Sie unter Linux oder Macintosh ein Befehls-Terminal.
2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `% sftp -i transfer-key sftp_user@service_endpoint`

Im vorherigen Befehl `sftp_user` ist dies der Benutzername und `transfer-key` der private SSH-Schlüssel. Hier `service_endpoint` ist der Endpunkt des Servers, wie er in der AWS Transfer Family Konsole für den ausgewählten Server angezeigt wird.

Eine `sftp`-Eingabeaufforderung sollte angezeigt werden.

3. (Optional) Um das Home-Verzeichnis des Benutzers anzuzeigen, geben Sie an der `sftp` Eingabeaufforderung den folgenden Befehl ein: `sftp> pwd`

4. Geben Sie den folgenden Text in die nächste Zeile ein: `sftp> cd /amzn-s3-demo-bucket/home/sftp_user`

In dieser Übung für die ersten Schritte ist dieser Amazon S3 S3-Bucket das Ziel der Dateiübertragung.

5. Geben Sie den folgenden Befehl in die nächste Zeile ein: `sftp> put filename.txt`

Der `put` Befehl überträgt die Datei in den Amazon S3 S3-Bucket.

Eine Meldung wie die Folgende wird angezeigt und gibt an, dass die Dateiübertragung läuft oder abgeschlossen wurde.

```
Uploading filename.txt to /amzn-s3-demo-bucket/home/sftp_user/
filename.txt
```

```
some-file.txt 100% 127 0.1KB/s 00:00
```

Einen verwalteten Workflow für die Entschlüsselung einer Datei einrichten

In diesem Tutorial wird veranschaulicht, wie Sie einen verwalteten Workflow einrichten, der einen Entschlüsselungsschritt enthält. Das Tutorial zeigt auch, wie Sie eine verschlüsselte Datei in einen Amazon S3 S3-Bucket hochladen und dann die entschlüsselte Datei in demselben Bucket anzeigen.

Note

Der AWS Speicher-Blog enthält einen Beitrag, in dem beschrieben wird, wie Dateien mithilfe von Transfer Family Managed Workflows, Verschlüsseln und [Entschlüsseln von Dateien mit PGP und einfach entschlüsselt werden können, ohne Code zu](#) schreiben, beschrieben werden. AWS Transfer Family

Themen

- [Schritt 1: Konfigurieren Sie eine Ausführungsrolle](#)
- [Schritt 2: Erstellen Sie einen verwalteten Workflow](#)
- [Schritt 3: Fügen Sie den Workflow einem Server hinzu und erstellen Sie einen Benutzer](#)
- [Schritt 4: Erstellen Sie ein PGP-Schlüsselpaar](#)

- [Schritt 5: Speichern Sie den privaten PGP-Schlüssel in AWS Secrets Manager](#)
- [Schritt 6: Verschlüsseln Sie eine Datei](#)
- [Schritt 7: Führen Sie den Workflow aus und sehen Sie sich die Ergebnisse an](#)

Schritt 1: Konfigurieren Sie eine Ausführungsrolle

Erstellen Sie eine AWS Identity and Access Management (IAM-) Ausführungsrolle, mit der Transfer Family einen Workflow starten kann. Der Prozess der Erstellung einer Ausführungsrolle wird unter [beschriebenIAM-Richtlinien für Workflows](#).

Note

Stellen Sie beim Erstellen einer Ausführungsrolle sicher, dass eine Vertrauensbeziehung zwischen der Ausführungsrolle und der Transfer Family hergestellt wird, wie unter [beschriebenSo stellen Sie eine Vertrauensbeziehung her](#).

Die folgende Richtlinie für Ausführungsrollen enthält alle erforderlichen Berechtigungen, um den Workflow zu starten, den Sie in diesem Tutorial erstellen. Wenn Sie diese Beispielrichtlinie verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre eigenen Informationen. `amzn-s3-demo-bucket` Ersetzen Sie es durch den Namen des Amazon S3 S3-Buckets, in den Sie Ihre verschlüsselten Dateien hochladen.

Note

Nicht jeder Workflow benötigt alle Berechtigungen, die in diesem Beispiel aufgeführt sind. Sie können die Berechtigungen je nach Art der Schritte in Ihrem spezifischen Workflow einschränken. Die für jeden vordefinierten Schritttyp erforderlichen Berechtigungen werden unter [beschriebenVerwenden Sie vordefinierte Schritte](#). Die für einen benutzerdefinierten Schritt erforderlichen Berechtigungen werden unter [beschriebenIAM-Berechtigungen für einen benutzerdefinierten Schritt](#).

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "iam:PassRole",  
      "Resource": "arn:aws:iam::123456789012:role/TransferFamilyRole",  
      "Condition": {  
        "StringEquals": {  
          "iam:PassedToService": "transferfamily.amazonaws.com",  
          "iam:AWSTransferFamilyRole": true  
        }  
      }  
    }  
  ]  
}
```

```

{
  "Sid": "WorkflowsS3Permissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion",
    "s3:PutObject",
    "s3:PutObjectTagging",
    "s3:ListBucket",
    "s3:PutObjectTagging",
    "s3:PutObjectVersionTagging",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
},
{
  "Sid": "DecryptSecret",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue"
  ],
  "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
}
]
}

```

Schritt 2: Erstellen Sie einen verwalteten Workflow

Jetzt müssen Sie einen Workflow erstellen, der einen Entschlüsselungsschritt enthält.

Um einen Workflow zu erstellen, der einen Entschlüsselungsschritt enthält

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich Workflows und dann Workflow erstellen aus.
3. Geben Sie folgende Details ein:

- Geben Sie beispielsweise eine Beschreibung ein **Decrypt workflow example**.
 - Wählen Sie im Abschnitt Nominale Schritte die Option Schritt hinzufügen aus.
4. Wählen Sie unter Schritttyp auswählen die Option Datei entschlüsseln und dann Weiter aus.
 5. Geben Sie im Dialogfeld „Parameter konfigurieren“ Folgendes an:
 - Geben Sie einen aussagekräftigen Schrittnamen ein, **decrypt-step** z. B. Leerzeichen sind in Schrittnamen nicht zulässig.
 - Wählen Sie als Ziel für entschlüsselte Dateien Amazon S3 aus.
 - Wählen Sie für den Namen des Ziel-Buckets denselben Amazon S3 S3-Bucket aus, den Sie amzn-s3-demo-bucket in der IAM-Richtlinie, die Sie in Schritt 1 erstellt haben, angegeben haben.
 - Geben Sie für das Zielschlüsselpräfix den Namen des Präfixes (Ordners) ein, in dem Sie Ihre entschlüsselten Dateien in Ihrem Ziel-Bucket speichern möchten, z. B. **decrypted-files/**

 Note

Achten Sie darauf, Ihrem Präfix einen abschließenden Schrägstrich (/) hinzuzufügen.

- Lassen Sie für dieses Tutorial die Option Existierendes überschreiben deaktiviert. Wenn diese Einstellung deaktiviert ist und Sie versuchen, eine Datei mit dem identischen Namen einer vorhandenen Datei zu entschlüsseln, wird die Workflow-Verarbeitung gestoppt und die neue Datei wird nicht verarbeitet.

Wählen Sie Weiter, um zum Überprüfungsbildschirm zu gelangen.

6. Überprüfen Sie die Details für den Schritt. Wenn alles korrekt ist, wählen Sie Schritt erstellen.
7. Ihr Workflow benötigt nur den einzigen Entschlüsselungsschritt, sodass keine zusätzlichen Schritte zur Konfiguration erforderlich sind. Wählen Sie Workflow erstellen aus, um den neuen Workflow zu erstellen.

Notieren Sie sich die Workflow-ID für Ihren neuen Workflow. Sie benötigen diese ID für den nächsten Schritt. In diesem Tutorial wird die Workflow-ID *w-1234abcd5678efghi* als Beispiel verwendet.

Schritt 3: Fügen Sie den Workflow einem Server hinzu und erstellen Sie einen Benutzer

Da Sie nun über einen Workflow mit einem Entschlüsselungsschritt verfügen, müssen Sie ihn einem Transfer Family Family-Server zuordnen. Dieses Tutorial zeigt, wie Sie den Workflow an einen vorhandenen Transfer Family Family-Server anhängen. Alternativ können Sie einen neuen Server für Ihren Workflow erstellen.

Nachdem Sie den Workflow an einen Server angehängt haben, müssen Sie einen Benutzer erstellen, der per SFTP auf den Server zugreifen und die Ausführung des Workflows auslösen kann.

So konfigurieren Sie einen Transfer Family Family-Server für die Ausführung eines Workflows

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann einen Server aus der Liste aus. Stellen Sie sicher, dass dieser Server das SFTP-Protokoll unterstützt.
3. Scrollen Sie auf der Detailseite für den Server nach unten zum Abschnitt Zusätzliche Details und wählen Sie dann Bearbeiten aus.
4. Wählen Sie auf der Seite Zusätzliche Details bearbeiten im Abschnitt Verwaltete Workflows Ihren Workflow und wählen Sie eine entsprechende Ausführungsrolle aus.
 - Wählen Sie unter Workflow für vollständige Datei-Uploads den Workflow aus, den Sie erstellt haben [Schritt 2: Erstellen Sie einen verwalteten Workflow](#), **w-1234abcd5678efghi** z. B. in.
 - Wählen Sie für die Ausführungsrolle für verwaltete Workflows die IAM-Rolle aus, in der Sie sie erstellt haben. [Schritt 1: Konfigurieren Sie eine Ausführungsrolle](#)
5. Scrollen Sie zum Ende der Seite und wählen Sie Speichern, um Ihre Änderungen zu speichern.

Notieren Sie sich die ID des Servers, den Sie verwenden. Der Name des AWS Secrets Manager Geheimnisses, das Sie zum Speichern Ihrer PGP-Schlüssel verwenden, basiert teilweise auf der Server-ID.

Um einen Benutzer hinzuzufügen, der den Workflow auslösen kann

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann den Server aus, den Sie für den Entschlüsselungsschritt verwenden.

3. Scrollen Sie auf der Seite mit den Serverdetails nach unten zum Abschnitt Benutzer und wählen Sie Benutzer hinzufügen aus.
4. Geben Sie für Ihren neuen Benutzer die folgenden Details ein:
 - Geben Sie für Username (Benutzername) **decrypt-user** ein.
 - Wählen Sie unter Rolle eine Benutzerrolle aus, die auf Ihren Server zugreifen kann.
 - Wählen Sie für Home-Verzeichnis den Amazon S3 S3-Bucket aus, den Sie zuvor verwendet haben, zum Beispiel `amzn-s3-demo-bucket`.
 - Fügen Sie für öffentliche SSH-Schlüssel einen öffentlichen Schlüssel ein, der einem privaten Schlüssel entspricht, den Sie haben. Details hierzu finden Sie unter [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).
5. Wählen Sie Hinzufügen, um Ihren neuen Benutzer zu speichern.

Notieren Sie sich den Namen Ihres Transfer Family Family-Benutzers für diesen Server. Das Geheimnis basiert teilweise auf dem Namen des Benutzers. Der Einfachheit halber verwendet dieses Tutorial ein Standardgeheimnis, das von jedem Benutzer des Servers verwendet werden kann.

Schritt 4: Erstellen Sie ein PGP-Schlüsselpaar

Verwenden Sie einen der [unterstützten PGP-Clients, um ein PGP-Schlüsselpaar](#) zu generieren. Dieser Vorgang wird ausführlich unter beschrieben. [Generieren Sie PGP-Schlüssel](#)

Um ein PGP-Schlüsselpaar zu generieren

1. Für dieses Tutorial können Sie den Client gpg (GnuPG) Version 2.0.22 verwenden, um ein PGP-Schlüsselpaar zu generieren, das RSA als Verschlüsselungsalgorithmus verwendet. Führen Sie für diesen Client den folgenden Befehl aus und geben Sie eine E-Mail-Adresse und eine Passphrase ein. Sie können einen beliebigen Namen oder eine E-Mail-Adresse verwenden. Stellen Sie sicher, dass Sie sich die von Ihnen verwendeten Werte merken, da Sie sie später im Tutorial eingeben müssen.

```
gpg --gen-key
```

Note

Wenn Sie GnuPG Version 2.3.0 oder neuer verwenden, müssen Sie `ausführengpg --full-gen-key`. Wenn Sie nach dem Typ des zu erstellenden Schlüssels gefragt

werden, wählen Sie RSA oder ECC aus. Wenn Sie ECC wählen, können Sie zwischen BrainPool und Curve25519 für die NIST elliptische Kurve wählen.

2. Exportieren Sie den privaten Schlüssel, indem Sie den folgenden Befehl ausführen.
user@example.com Ersetzen Sie ihn durch die E-Mail-Adresse, die Sie bei der Generierung des Schlüssels verwendet haben.

```
gpg --output workflow-tutorial-key.pgp --armor --export-secret-key user@example.com
```

Dieser Befehl exportiert den privaten Schlüssel in die **workflow-tutorial-key.pgp** Datei. Sie können der Ausgabedatei einen beliebigen Namen geben. Sie können die Datei mit dem privaten Schlüssel auch löschen, nachdem Sie sie hinzugefügt haben AWS Secrets Manager.

Schritt 5: Speichern Sie den privaten PGP-Schlüssel in AWS Secrets Manager

Sie müssen den privaten Schlüssel in Secrets Manager auf eine ganz bestimmte Weise speichern, damit der Workflow den privaten Schlüssel finden kann, wenn der Workflow einen Entschlüsselungsschritt für eine hochgeladene Datei ausführt.

Note

Wenn Sie Geheimnisse im Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu den Preisen erhalten Sie unter [AWS Secrets Manager Preise](#).

Um einen privaten PGP-Schlüssel in Secrets Manager zu speichern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Secrets Manager Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie im linken Navigationsbereich Secrets aus.
3. Wählen Sie auf der Seite Secrets die Option Neues Geheimnis speichern aus.
4. Wählen Sie auf der Seite Geheimtyp auswählen für Geheimtyp die Option Anderer Geheimtyp aus.
5. Wählen Sie im Bereich Key/value Paare die Key/value Registerkarte aus.

- Schlüssel — Geben Sie ein **PGPPrivateKey**.
 - Wert — Fügen Sie den Text Ihres privaten Schlüssels in das Wertfeld ein.
6. Wählen Sie Zeile hinzufügen und wählen Sie im Bereich Key/valuePaare den Key/valueTab aus.
- Schlüssel — Enter **PGPPassphrase**.
 - Wert — Geben Sie die Passphrase ein, die Sie bei der Generierung Ihres PGP-Schlüsselpaars in verwendet haben. [Schritt 4: Erstellen Sie ein PGP-Schlüsselpaar](#)
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Geheimes Passwort konfigurieren einen Namen und eine Beschreibung für Ihr Geheimnis ein. Sie können ein Geheimnis für einen bestimmten Benutzer oder ein Geheimnis erstellen, das von allen Benutzern verwendet werden kann. Wenn Ihre Server-ID lautet **s-11112222333344445**, benennen Sie das Geheimnis wie folgt.
- Um ein Standardgeheimnis für alle Benutzer zu erstellen, geben Sie dem Geheimnis einen Namen **aws/transfer/s-11112222333344445/@pgp-default**.
 - Um ein Geheimnis nur für den Benutzer zu erstellen, den Sie zuvor erstellt haben, geben Sie dem Geheimnis einen Namen **aws/transfer/s-11112222333344445/decrypt-user**.
9. Wählen Sie Weiter und akzeptieren Sie dann die Standardeinstellungen auf der Seite „Rotation konfigurieren“. Klicken Sie anschließend auf Weiter.
10. Wählen Sie auf der Seite „Überprüfen“ die Option Speichern aus, um das Geheimnis zu erstellen und zu speichern.

Weitere Informationen zum Hinzufügen Ihres privaten PGP-Schlüssels zu Secrets Manager finden Sie unter [AWS Secrets Manager Zum Speichern Ihres PGP-Schlüssels verwenden](#).

Schritt 6: Verschlüsseln Sie eine Datei

Verwenden Sie das gpg Programm, um eine Datei für die Verwendung in Ihrem Workflow zu verschlüsseln. Führen Sie den folgenden Befehl aus, um eine Datei zu verschlüsseln:

```
gpg -e -r marymajor@example.com --openpgp testfile.txt
```

Bevor Sie diesen Befehl ausführen, beachten Sie Folgendes:

- Ersetzen ***marymajor@example.com*** Sie das **-r** Argument durch die E-Mail-Adresse, die Sie bei der Erstellung des PGP-Schlüsselpaars verwendet haben.

- Die `--openpgp` Markierung ist optional. Dieses Flag sorgt dafür, dass die verschlüsselte Datei dem [OpenPGP-Standard](#) RFC4880 entspricht.
- Dieser Befehl erstellt eine Datei mit dem Namen **testfile.txt.gpg** am selben Ort wie. **testfile.txt**

 Important

Achten Sie beim Verschlüsseln von Dateien zur Verwendung mit AWS Transfer Family Workflows immer darauf, dass Sie mit dem Parameter einen nicht anonymen Empfänger angeben. `-r` Anonyme Verschlüsselung (ohne Angabe eines Empfängers) kann zu Entschlüsselungsfehlern im Workflow führen, da das System nicht erkennen kann, welcher Schlüssel für die Entschlüsselung verwendet werden soll. Informationen zum Debuggen dieses Problems finden Sie unter. [Beheben Sie Probleme mit der Verschlüsselung anonymer Empfänger](#)

Schritt 7: Führen Sie den Workflow aus und sehen Sie sich die Ergebnisse an

Um den Workflow auszuführen, stellen Sie mit dem Benutzer, den Sie in Schritt 3 erstellt haben, eine Verbindung zum Transfer Family Family-Server her. Anschließend können Sie in dem Amazon S3 S3-Bucket, den Sie in [Schritt 2.5 angegeben haben, die Zielparameter so konfigurieren](#), dass die entschlüsselte Datei angezeigt wird.

Um den Entschlüsselungs-Workflow auszuführen

1. Öffnen Sie ein Befehlsterminal.
2. Führen Sie den folgenden Befehl aus und *your-endpoint* ersetzen Sie ihn durch Ihren tatsächlichen Endpunkt und *transfer-key* den privaten SSH-Schlüssel Ihres Benutzers:

```
sftp -i transfer-key decrypt-user@your-endpoint
```

Wenn der private Schlüssel beispielsweise in `~/.ssh/decrypt-user` gespeichert ist und Ihr Endpunkt darin gespeichert ist `-11112222333344445.server.transfer.us-east-2.amazonaws.com`, lautet der Befehl wie folgt:

```
sftp -i ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-east-2.amazonaws.com
```

3. Führen Sie den Befehl `pwd` aus. Bei Erfolg gibt dieser Befehl Folgendes zurück:

```
Remote working directory: /amzn-s3-demo-bucket/decrypt-user
```

Ihr Verzeichnis spiegelt den Namen Ihres Amazon S3 S3-Buckets wider.

4. Führen Sie den folgenden Befehl aus, um die Datei hochzuladen und die Ausführung des Workflows auszulösen:

```
put testfile.txt.gpg
```

5. Für das Ziel der entschlüsselten Dateien haben Sie den `decrypted-files/` Ordner angegeben, als Sie den Workflow erstellt haben. Jetzt können Sie zu diesem Ordner navigieren und den Inhalt auflisten.

```
cd ../decrypted-files/  
ls
```

Bei Erfolg listet der `ls` Befehl die `testfile.txt` Datei auf. Sie können diese Datei herunterladen und überprüfen, ob sie mit der Originaldatei identisch ist, die Sie zuvor verschlüsselt haben.

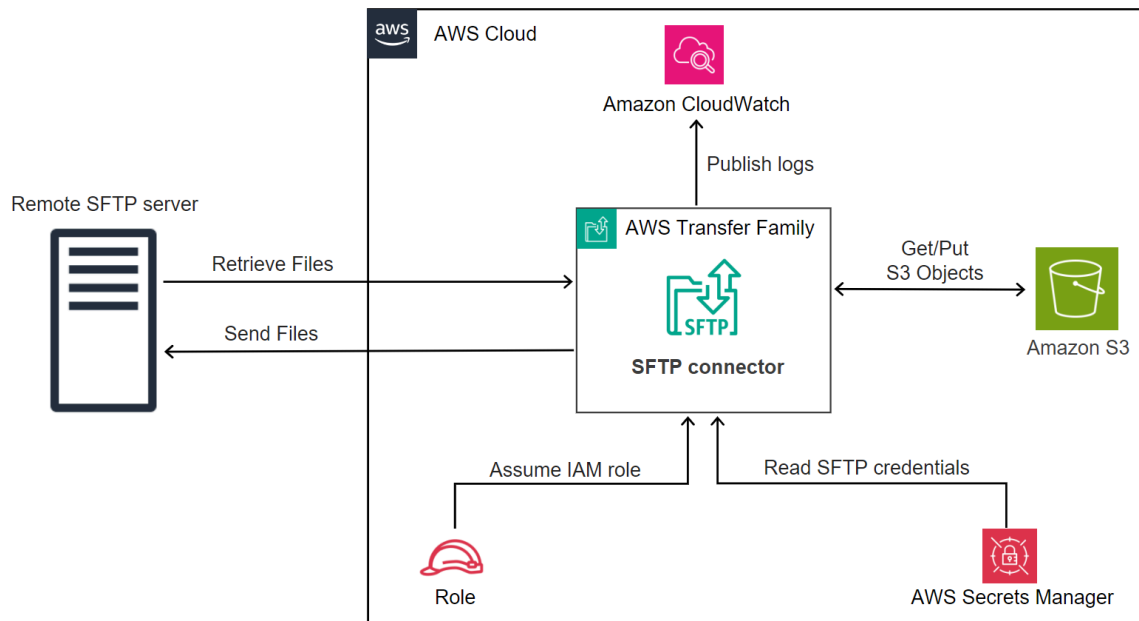
Einrichtung und Verwendung von SFTP-Anschlüssen

Der Zweck eines Connectors besteht darin, eine Beziehung zwischen Ihrem AWS Speicher und dem SFTP-Server eines Partners herzustellen. Sie können Dateien von Amazon S3 an ein externes, partnereigenes Ziel senden. Sie können auch einen SFTP-Connector verwenden, um Dateien vom SFTP-Server eines Partners abzurufen.

Dieses Tutorial zeigt, wie Sie einen SFTP-Connector mit den Ausgangstypen Service Managed und VPC_LATTICE einrichten und anschließend Dateien zwischen Amazon S3 S3-Speicher und einem SFTP-Server übertragen.

Ein SFTP-Connector ruft SFTP-Anmeldeinformationen ab, um sich bei einem Remote-SFTP-Server AWS Secrets Manager zu authentifizieren und eine Verbindung herzustellen. Der Connector sendet

Dateien an den Remote-Server oder ruft Dateien vom Remote-Server ab und speichert die Dateien in Amazon S3. Sie können zwischen Service Managed Egress (mithilfe AWS verwalteter Infrastruktur) oder VPC Egress (Routing durch Ihre VPC mithilfe Cross-VPC von Resource Access) wählen. Eine IAM-Rolle wird verwendet, um den Zugriff auf den Amazon S3 S3-Bucket und auf die in Secrets Manager gespeicherten Anmeldeinformationen zu ermöglichen. Und Sie können sich bei Amazon anmelden CloudWatch.



Der folgende Blogbeitrag bietet eine Referenzarchitektur für die Erstellung eines MFT-Workflows mithilfe von SFTP-Konnektoren, einschließlich der Verschlüsselung von Dateien mit PGP, bevor sie mithilfe von SFTP-Konnektoren an einen Remote-SFTP-Server gesendet werden: [Architektur sicherer und richtlinienkonformer verwalteter Dateiübertragungen mit SFTP-Konnektoren und PGP-Verschlüsselung](#). AWS Transfer Family

Ausgangstypen für Konnektoren

SFTP-Konnektoren unterstützen zwei Ausgangstypen, die bestimmen, wie Ihr Connector den Datenverkehr an Remote-SFTP-Server weiterleitet:

- **SERVICE_MANAGED (Standard):** Verwendet die von AWS Transfer Family verwaltete Infrastruktur mit statischen IP-Adressen für ausgehende Verbindungen.
- **VPC:** Leitet den Datenverkehr mithilfe von Cross-VPC Resource Access durch Ihre VPC weiter und ermöglicht so private Endpunktkonnektivität und die Verwendung Ihrer eigenen NAT-Gateways.

Dieses Tutorial behandelt beide Ausgangstypen. Wählen Sie den VPC-Ausgangstyp, wenn Sie:

- Connect zu privaten SFTP-Servern in Ihrer VPC her (private IP-Adressen)
- Stellen Sie über Direct Connect oder VPN eine Verbindung zu lokalen SFTP-Servern her
- Leiten Sie öffentlichen Endpunktverkehr für Sicherheitskontrollen durch Ihre VPC
- Verwenden Sie Ihre eigenen Elastic IP-Adressen für ausgehende Verbindungen

Themen

- [Schritt 1: Erstellen Sie die erforderlichen unterstützenden Ressourcen](#)
- [Schritt 2: Erstellen und testen Sie einen SFTP-Connector](#)
- [Schritt 3: Senden und Abrufen von Dateien mithilfe des SFTP-Connectors](#)
- [Verfahren zum Erstellen eines Transfer Family Family-Servers, der als Remote-SFTP-Server verwendet werden kann](#)

Schritt 1: Erstellen Sie die erforderlichen unterstützenden Ressourcen

Sie können SFTP-Konnektoren verwenden, um Dateien zwischen Amazon S3 und einem beliebigen Remote-SFTP-Server zu kopieren. Für dieses Tutorial verwenden wir einen AWS Transfer Family Server als Remote-SFTP-Server. Wir müssen die folgenden Ressourcen erstellen und konfigurieren:

- Erstellen Sie Amazon S3 S3-Buckets, um Dateien in Ihrer AWS Umgebung zu speichern und Dateien vom Remote-SFTP-Server zu senden und abzurufen.: [Amazon S3 S3-Buckets erstellen](#)
- Erstellen Sie eine AWS Identity and Access Management Rolle für den Zugriff auf Amazon S3 S3-Speicher und unser Geheimnis in Secrets Manager: [Erstellen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen](#).
- Erstellen Sie einen Transfer Family Family-Server, der das SFTP-Protokoll verwendet, und einen vom Dienst verwalteten Benutzer, der den SFTP-Connector verwendet, um Dateien zum oder vom SFTP-Server zu übertragen.: [Erstellen Sie einen Transfer Family SFTP-Server und einen Benutzer](#)
- Erstellen Sie einen AWS Secrets Manager geheimen Schlüssel, der die Anmeldeinformationen speichert, die der SFTP-Connector für die Anmeldung am Remote-SFTP-Server verwendet.: [Erstellen und speichern Sie ein Geheimnis in AWS Secrets Manager](#)

Für VPC-Ausgangsanschlüsse benötigen Sie außerdem:

- Eine VPC mit entsprechenden Subnetzen und Sicherheitsgruppen

- Ein Resource Gateway (mindestens 2 Availability Zones erforderlich):. [Erstellen Sie ein Resource Gateway \(nur VPC-Ausgangstyp\)](#)
- Eine Ressourcenkonfiguration, die auf Ihren SFTP-Server verweist:[Erstellen Sie eine Ressourcenkonfiguration \(nur VPC-Ausgangstyp\)](#). Weitere Informationen finden Sie unter [Ressourcenkonfigurationen](#) im Benutzerhandbuch für Amazon VPC Lattice.

Amazon S3 S3-Buckets erstellen

So erstellen Sie einen Amazon-S3-Bucket

1. Melden Sie sich bei der AWS Transfer Family Konsole an unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie eine Region und geben Sie einen Namen ein.

In diesem Tutorial ist unser Bucket **US East (N. Virginia) us-east-1** dabei und der Name lautet **sftp-server-storage-east**.

3. Akzeptieren Sie die Standardeinstellungen und wählen Sie Create Bucket.

Vollständige Informationen zum Erstellen von Amazon S3 S3-Buckets finden Sie unter [Wie erstelle ich einen S3-Bucket?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Erstellen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen

Erstellen Sie für die Zugriffsrolle eine Richtlinie mit den folgenden Berechtigungen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

```

    ],
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}

```

Ersetzen Sie Elemente wie folgt:

- Für `amzn-s3-demo-bucket` verwendet das Tutorial **sftp-server-storage-east**.
- Für *region* verwendet das Tutorial **us-east-1**.
- Verwenden *account-id* Sie für Ihre AWS-Konto ID.
- Denn *SecretName-6RandomCharacters* wir sind **using sftp-connector1** für den Namen (Sie werden Ihre eigenen sechs zufälligen Zeichen für Ihr Geheimnis haben).

Sie müssen außerdem sicherstellen, dass diese Rolle eine Vertrauensstellung beinhaltet, die es dem Connector ermöglicht, auf Ihre Ressourcen zuzugreifen, wenn er Übertragungsanfragen Ihrer Benutzer bearbeitet. Einzelheiten zum Aufbau einer Vertrauensbeziehung finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

 Note

Einzelheiten zu der Rolle, die wir für das Tutorial verwenden, finden Sie unter [Kombinierte Benutzer- und Zugriffsrolle](#).

Erstellen und speichern Sie ein Geheimnis in AWS Secrets Manager

Wir müssen ein Geheimnis in Secrets Manager speichern, um Benutzeranmeldeinformationen für Ihren SFTP-Connector zu speichern. Sie können ein Passwort, einen privaten SSH-Schlüssel oder beides verwenden. Für das Tutorial verwenden wir einen privaten Schlüssel.

 Note

Wenn Sie Geheimnisse im Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu den Preisen erhalten Sie unter [AWS Secrets Manager Preise](#).

Bevor Sie mit dem Verfahren zum Speichern des Geheimnisses beginnen, müssen Sie Ihren privaten Schlüssel abrufen und formatieren. Der private Schlüssel muss dem öffentlichen Schlüssel entsprechen, der für den Benutzer auf dem Remote-SFTP-Server konfiguriert ist. Für unser Tutorial muss der private Schlüssel dem öffentlichen Schlüssel entsprechen, der für unseren Testbenutzer auf dem Transfer Family SFTP-Server gespeichert ist, den wir als Remote-Server verwenden.

Führen Sie dazu den folgenden Befehl aus:

```
jq -sR . path-to-private-key-file
```

Wenn sich Ihre private Schlüsseldatei beispielsweise in befindet `~/ .ssh/sftp-testuser-privatekey`, lautet der Befehl wie folgt.

```
jq -sR . ~/ .ssh/sftp-testuser-privatekey
```

Dadurch wird der Schlüssel im richtigen Format (mit eingebetteten Zeilenumbruchzeichen) in die Standardausgabe ausgegeben. Kopieren Sie diesen Text irgendwo, da Sie ihn im folgenden Verfahren (in Schritt 6) einfügen müssen.

Um Benutzeranmeldeinformationen in Secrets Manager für einen SFTP-Connector zu speichern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Secrets Manager Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie im linken Navigationsbereich Secrets aus.
3. Wählen Sie auf der Seite Secrets die Option Neues Geheimnis speichern aus.
4. Wählen Sie auf der Seite Geheimtyp auswählen für Geheimtyp die Option Anderer Geheimtyp aus.
5. Wählen Sie im Bereich Key/value Paare die Key/value Registerkarte aus.
 - Schlüssel — Enter **Username**.
 - Wert — Geben Sie den Namen unseres Benutzers ein, **sftp-testuser**.
6. Um den Schlüssel einzugeben, empfehlen wir, die Registerkarte Klartext zu verwenden.
 - a. Wählen Sie Zeile hinzufügen und geben Sie dann die Eingabetaste ein **PrivateKey**.
 - b. Wählen Sie die Registerkarte Klartext. Das Feld enthält jetzt den folgenden Text:

```
{"Username": "sftp-testuser", "PrivateKey": ""}
```
 - c. Fügen Sie den Text für Ihren privaten Schlüssel (zuvor gespeichert) zwischen den leeren doppelten Anführungszeichen („“) ein.

Ihr Bildschirm sollte wie folgt aussehen (Schlüsseldaten sind ausgegraut).



7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Geheim konfigurieren einen Namen für Ihr Geheimnis ein. In diesem Tutorial geben wir dem Geheimnis einen Namen **aws/transfer/sftp-connector1**.
9. Wählen Sie Weiter und akzeptieren Sie dann die Standardeinstellungen auf der Seite „Rotation konfigurieren“. Klicken Sie anschließend auf Weiter.
10. Wählen Sie auf der Seite „Überprüfen“ die Option Speichern aus, um das Geheimnis zu erstellen und zu speichern.

Erstellen Sie ein Resource Gateway (nur VPC-Ausgangstyp)

Für VPC-Egress-Connectors müssen Sie in Ihrer VPC ein Resource Gateway erstellen. Das Resource Gateway dient als Einstiegspunkt für Cross-VPC Resource Access.

Um ein Resource Gateway zu erstellen

1. Führen Sie den folgenden Befehl aus, um ein Resource Gateway zu erstellen (ersetzen Sie die VPC-ID und die Subnetz-IDs durch Ihre Werte):

```
aws vpc-lattice create-resource-gateway \
  --name my-sftp-resource-gateway \
  --vpc-identifier vpc-12345678 \
```

```
--subnet-ids subnet-12345678 subnet-87654321
```

 Note

Resource Gateways benötigen Subnetze in mindestens 2 Availability Zones.

2. Notieren Sie sich die Resource Gateway-ID aus der Antwort zur Verwendung im nächsten Schritt.

Erstellen Sie eine Ressourcenkonfiguration (nur VPC-Ausgangstyp)

Erstellen Sie eine Ressourcenkonfiguration, die auf Ihren SFTP-Server verweist. Dies kann eine private IP-Adresse für Server in Ihrer VPC oder ein öffentlicher DNS-Name für externe Server sein. Weitere Informationen zu Ressourcenkonfigurationen finden Sie unter [Ressourcenkonfigurationen](#) im Amazon VPC Lattice-Benutzerhandbuch.

Um eine Ressourcenkonfiguration zu erstellen

1. Führen Sie für einen privaten SFTP-Server Folgendes aus:

```
aws vpc-lattice create-resource-configuration \  
  --name my-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"}
```

2. Führen Sie für einen öffentlichen SFTP-Server (nur DNS-Name) Folgendes aus:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
```

 Note

Öffentliche Endpunkte müssen DNS-Namen verwenden, keine IP-Adressen.

3. Notieren Sie sich den ARN für die Ressourcenkonfiguration aus der Antwort, der beim Erstellen des Connectors verwendet werden soll.

Schritt 2: Erstellen und testen Sie einen SFTP-Connector

In diesem Abschnitt erstellen wir einen SFTP-Connector, der alle Ressourcen verwendet, die wir zuvor erstellt haben. Weitere Details finden Sie unter [SFTP-Konnektoren erstellen](#).

Um einen SFTP-Connector zu erstellen

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich SFTP-Connectors und anschließend Create SFTP-Connector aus.
3. Wählen Sie als Ausgangstyp eine der folgenden Optionen aus:
 - Service managed (Standard): Verwendet die von AWS Transfer Family verwaltete Infrastruktur mit statischen IP-Adressen für ausgehende Verbindungen.
 - VPC Lattice: Leitet den Datenverkehr mithilfe Cross-VPC von Resource Access durch Ihre VPC weiter. Wählen Sie diese Option für private Endpunktkonnektivität oder um Ihre eigenen NAT-Gateways zu verwenden.

Important

Sie können den Ausgangstyp nicht ändern, nachdem Sie den Connector erstellt haben. Wählen Sie sorgfältig auf der Grundlage Ihrer Konnektivitätsanforderungen aus.

4. Geben Sie im Abschnitt Connector-Konfiguration die folgenden Informationen an:
 - Geben Sie für die URL die URL des Remote-SFTP-Servers ein. Für das Tutorial geben wir die URL des Transfer Family Family-Servers ein, den wir als Remote-SFTP-Server verwenden.

```
sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

1111aaaa2222bbbb3 Ersetzen Sie es durch Ihre Transfer Family Family-Server-ID.

- Geben Sie für die Access-Rolle die Rolle ein, die wir zuvor erstellt haben **sftp-connector-role**.

- Geben Sie für Resource Configuration ARN (nur VPC Lattice Egress Type) den ARN der Ressourcenkonfiguration ein, die Sie zuvor erstellt haben:

```
arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678
```

- Wählen Sie für die Rolle Logging eine Rolle aus, die `transfer.amazonaws.com` im Principal-Element eine Vertrauensrichtlinie enthält.

Tipp: Sie können Transfer Family nicht nur als vertrauenswürdige Entität hinzufügen, sondern auch die `AWSTransferLoggingAccess` AWS verwaltete Richtlinie zur Rolle hinzufügen. Diese Richtlinie wird ausführlich unter beschrieben [AWSTransferLoggingAccess](#).

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

5. Geben Sie im Abschnitt SFTP-Konfiguration die folgenden Informationen ein:

- Wählen Sie für Connector-Anmeldeinformationen den Namen Ihrer Secrets Manager Manager-Ressource, die SFTP-Anmeldeinformationen enthält. Für das Tutorial wählen **aws/transfer/sftp-connector1** Sie.
- Fügen Sie für vertrauenswürdige Hostschlüssel den öffentlichen Teil des Hostschlüssels ein. Sie können diesen Schlüssel abrufen, indem Sie ihn `ssh-keyscan` für Ihren SFTP-Server ausführen. Einzelheiten zum Formatieren und Speichern des vertrauenswürdigen Host-Schlüssels finden Sie in der Dokumentation zum [SftpConnectorConfig](#)Datentyp.
- Wählen Sie für Maximale Anzahl gleichzeitiger Verbindungen einen Ganzzahlwert zwischen 1 und 5 aus: Der Standardwert ist 5.

SFTP configuration [Info](#)**Connector credentials** [Info](#)

Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server


[Store a new secret](#)
Trusted host keys - optional [Info](#)

Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

i Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

[Remove](#)
[Add trusted host key](#)
Maximum concurrent connections [Info](#)

Select the maximum number of concurrent connections that your connector can create to the remote server

- Nachdem Sie alle Ihre Einstellungen bestätigt haben, wählen Sie **Connector erstellen**, um den SFTP-Connector zu erstellen.

Sie können Konnektoren auch mit dem AWS Command Line Interface erstellen.

- Führen Sie den folgenden Befehl aus, um einen SFTP-Connector mit vom Service verwaltetem Ausgang zu erstellen:

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-
rsa AAAAB3NzaC..."
```

- Führen Sie den folgenden Befehl aus, um einen SFTP-Connector mit VPC-based Egress zu erstellen:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa
AAAAB3NzaC..." \
```

```
--egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

Nachdem Sie einen SFTP-Connector erstellt haben, empfehlen wir, ihn zu testen, bevor Sie versuchen, Dateien mit Ihrem neuen Connector zu übertragen.

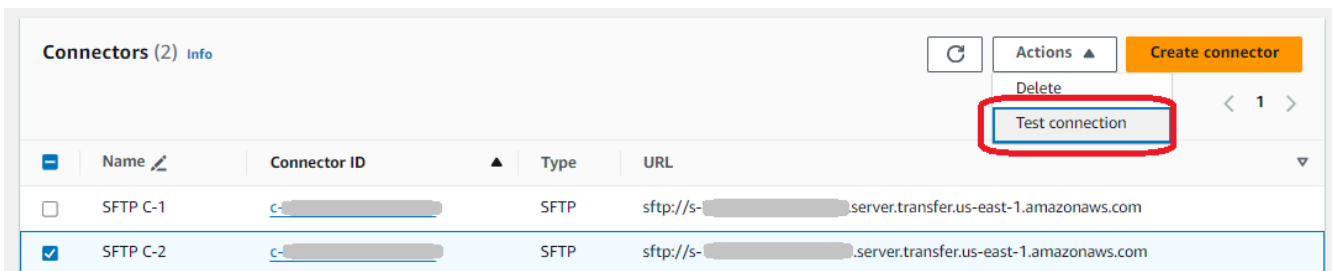
Note

Bei VPC-Ausgangsverbindern kann die DNS-Auflösung nach der Erstellung mehrere Minuten dauern. Während dieser Zeit wird der Connector-Status „Connector not available“ TestConnection angezeigt PENDING und auch wieder angezeigt. Warten Sie, bis der Status erreicht ist, ACTIVE bevor Sie versuchen, Dateien zu übertragen.

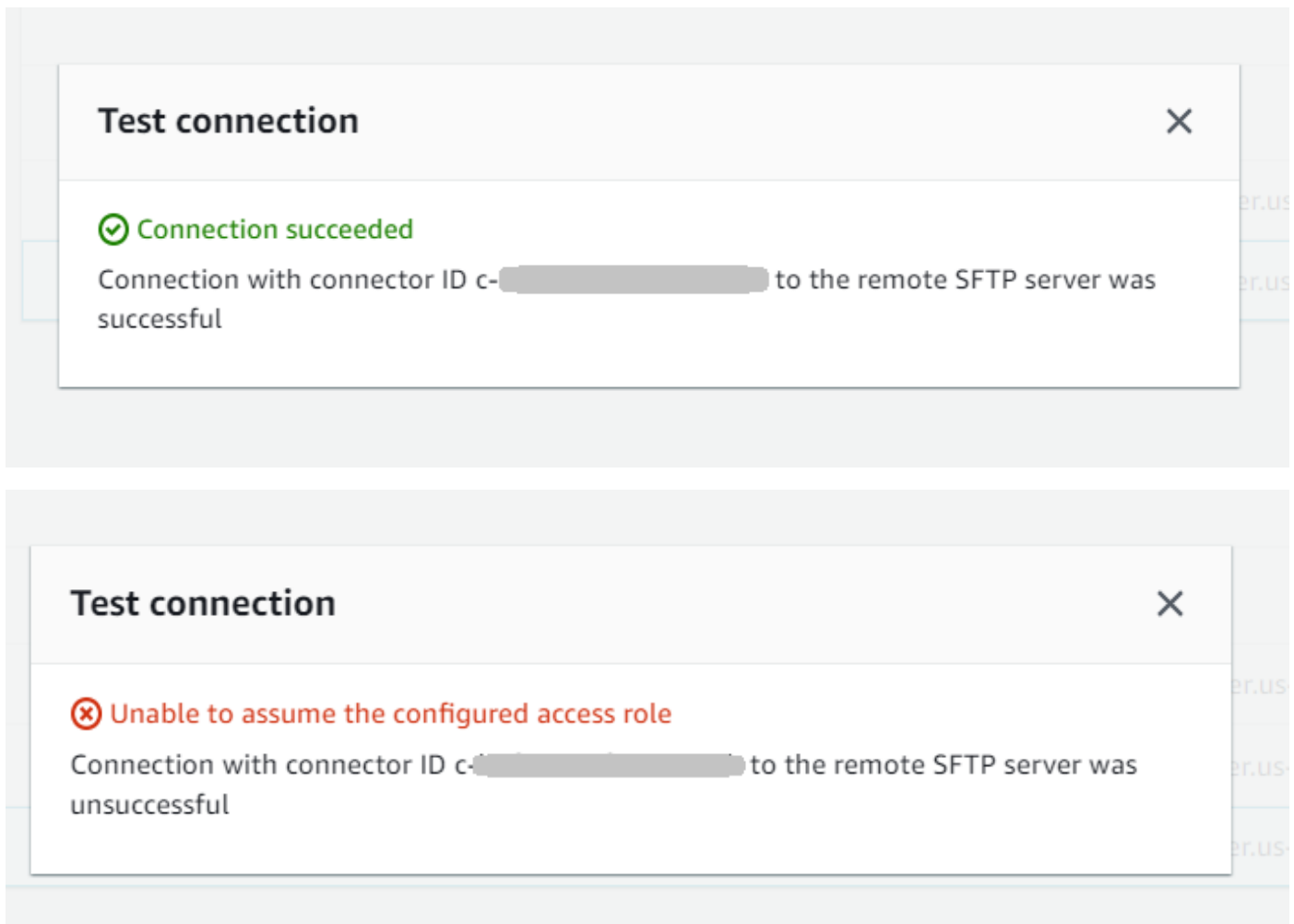
Test a connector using the console

Um einen SFTP-Connector zu testen

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich SFTP-Konnektoren und wählen Sie einen Connector aus.
3. Wählen Sie im Menü Aktionen die Option Verbindung testen aus.



Das System gibt eine Meldung zurück, die angibt, ob der Test erfolgreich war oder nicht. Wenn der Test fehlschlägt, gibt das System eine Fehlermeldung aus, die auf dem Grund basiert, warum der Test fehlgeschlagen ist.



Test a connector using the CLI

Um einen Connector mit dem zu testen AWS Command Line Interface, führen Sie den folgenden Befehl an einer Eingabeaufforderung aus (*connector-id* ersetzen Sie ihn durch Ihre tatsächliche Connector-ID):

```
aws transfer test-connection --connector-id c-connector-id
```

Wenn der Test erfolgreich ist, werden die folgenden Zeilen zurückgegeben:

```
{
  "Status": "OK",
  "StatusMessage": "Connection succeeded"
}
```

Wenn der Test nicht erfolgreich ist, erhalten Sie eine beschreibende Fehlermeldung, zum Beispiel:


```
{
  "Status": "ERROR",
  "StatusMessage": "Unable to assume the configured access role"
}
```

Wenn Sie einen VPC-Ausgangsconnector beschreiben, enthält die Antwort die neuen Felder:

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::219573224423:role/sftp-connector-role",
    "Arn": "arn:aws:transfer:us-east-1:219573224423:connector/c-5dfa309ccabf40759",
    "ConnectorId": "c-5dfa309ccabf40759",
    "Status": "ACTIVE",
    "EgressConfig": {
      "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:025066256552:resourceconfiguration/rcfg-079259b27a357a190"
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/sftp-connector1"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Beachten Sie, dass dieser Wert für VPC-Ausgangs-Connectors Null `ServiceManagedEgressIpAddresses` ist, da der Datenverkehr über Ihre VPC und nicht über die verwaltete Infrastruktur geleitet wird. AWS

Schritt 3: Senden und Abrufen von Dateien mithilfe des SFTP-Connectors

Der Einfachheit halber gehen wir davon aus, dass Sie bereits Dateien in Ihrem Amazon S3 S3-Bucket haben.

Note

Das Tutorial verwendet Amazon S3 S3-Buckets sowohl für Quell- als auch für Zielspeicherorte. Wenn Ihr SFTP-Server keinen Amazon S3 S3-Speicher verwendet, können

Sie, wo immer Sie `sftp-server-storage-east` in den folgenden Befehlen sehen, den Pfad durch einen Pfad zu Dateispeicherorten ersetzen, auf die von Ihrem SFTP-Server aus zugegriffen werden kann.

- Wir senden eine `SEND-to-SERVER.txt` vom Amazon S3 S3-Speicher benannte Datei an den SFTP-Server.
- Wir rufen eine Datei mit dem Namen `RETRIEVE-to-S3.txt` vom SFTP-Server in den Amazon S3 S3-Speicher ab.

 Note

Ersetzen Sie die Befehle in den folgenden Befehlen *connector-id* durch Ihre Connector-ID.

Zunächst senden wir eine Datei von unserem Amazon S3 S3-Bucket an den Remote-SFTP-Server. Führen Sie in einer Befehlszeile den folgenden Befehl aus:

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/  
sftp-server-storage-east/SEND-to-SERVER.txt" /  
--remote-directory-path "/sftp-server-storage-east/incoming"
```

Ihr `sftp-server-storage-east` Bucket sollte jetzt so aussehen.

Amazon S3 > Buckets > sftp-server-storage-east > incoming/

incoming/

[Copy S3 URI](#)

Objects | Properties

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#)
[Copy S3 URI](#)
[Copy URL](#)
[Download](#)
[Open](#)
[Delete](#)
[Actions](#)
[Create folder](#)

[Upload](#)

Find objects by prefix

☐	Name	Type	Last modified	Size	Storage class
☐	SEND-to-SERVER.txt	txt	December 18, 2023, 10:36:40 (UTC-05:00)	4.1 KB	Standard

Wenn Sie die Datei nicht wie erwartet sehen, überprüfen Sie Ihre CloudWatch Protokolle.

Um deine CloudWatch Logs zu überprüfen

1. Öffnen Sie die CloudWatch Amazon-Konsole unter <https://console.aws.amazon.com/cloudwatch/>
2. Wählen Sie im linken Navigationsmenü Protokollgruppen aus.
3. Geben Sie Ihre Connector-ID in die Suchleiste ein, um Ihre Logs zu finden.
4. Wählen Sie den Protokollstream aus, der bei der Suche zurückgegeben wird.
5. Erweitern Sie den neuesten Protokolleintrag.

Bei Erfolg sieht der Protokolleintrag wie folgt aus:

```
{
  "operation": "SEND",
  "timestamp": "2023-12-18T15:26:57.346283Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/SEND-to-SERVER.txt",
```

```

"status-code": "COMPLETED",
"start-time": "2023-12-18T15:26:56.915864Z",
"end-time": "2023-12-18T15:26:57.298122Z",
"account-id": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/sftp-server-storage-east/incoming"
}

```

Wenn die Dateiübertragung fehlgeschlagen ist, enthält der Protokolleintrag eine Fehlermeldung, die das Problem spezifiziert. Häufige Ursachen für Fehler sind Probleme mit den IAM-Berechtigungen und falsche Dateipfade.

Als Nächstes rufen wir eine Datei vom SFTP-Server in einen Amazon S3-Bucket ab. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus:

```

aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths
"/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/sftp-server-
storage-east/incoming"

```

Wenn die Übertragung erfolgreich ist, enthält Ihr Amazon S3 S3-Bucket die übertragene Datei, wie hier gezeigt.

The screenshot shows the Amazon S3 console interface for the bucket 'sftp-server-storage-east' and the directory 'incoming/'. The 'incoming/' directory is selected, and the 'Objects' tab is active. Below the directory name, there is a 'Copy S3 URI' button. The 'Objects (1)' section shows a list of objects with the following details:

Name	Type	Last modified	Size	Storage class
RETRIEVE-to-S3.txt	txt	December 18, 2023, 10:26:58 (UTC-05:00)	4.1 KB	Standard

Bei Erfolg sieht der Protokolleintrag wie folgt aus:

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-12-18T15:36:40.017800Z",
  "connector-id": "c-connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://s-server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/RETRIEVE-to-S3.txt",
  "status-code": "COMPLETED",
  "start-time": "2023-12-18T15:36:39.727626Z",
  "end-time": "2023-12-18T15:36:39.895726Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/c-connector-id",
  "local-directory-path": "/sftp-server-storage-east/incoming"
}
```

Fehlerbehebung bei VPC-Ausgangssteckern

Wenn Sie Probleme mit VPC-Ausgangsverbindern haben, überprüfen Sie Folgendes:

- Der Connector-Status ist AUSSTEHEND: Die DNS-Auflösung für VPC-Connectoren kann mehrere Minuten dauern. Warten Sie, bis der Status AKTIV wird, bevor Sie versuchen, Verbindungen herzustellen.
- Verbindungstimeouts: Stellen Sie sicher, dass Sicherheitsgruppen Datenverkehr auf Port 22 zwischen Ihren Resource Gateway-Subnetzen und dem Ziel-SFTP-Server zulassen.
- Fehler bei der Ressourcenkonfiguration: Stellen Sie sicher, dass Ihre Ressourcenkonfiguration auf die richtige IP-Adresse oder den richtigen DNS-Namen verweist und dass sich das Resource Gateway in derselben VPC wie Ihr SFTP-Server befindet (für private Endpunkte). Weitere Informationen finden Sie unter [Ressourcenkonfigurationen](#) im Benutzerhandbuch für Amazon VPC Lattice.
- Probleme mit öffentlichen Endpunkten: Stellen Sie bei öffentlichen Endpunkten sicher, dass Sie in Ihrer Ressourcenkonfiguration einen DNS-Namen und keine IP-Adresse verwenden. Stellen Sie sicher, dass Ihre VPC über ein NAT-Gateway für ausgehenden Internetzugang verfügt.
- AZ-Verfügbarkeit: Resource Gateways benötigen Subnetze in mindestens 2 Availability Zones. Nicht alle AZs unterstützen VPC Lattice — überprüfen Sie die unterstützten AZs in Ihrer Region.

Überlegungen zu den Kosten für den VPC-Ausgangstyp:

- VPC Lattice berechnet 0\$. 006/GB für die Datenverarbeitung als Ressourcenanbieter (direkt von VPC Lattice in Rechnung gestellt)
- AWS Transfer Family übernimmt die 0\$. 01/GB Kosten für den Ressourcenverbrauch (erstes 1 PB)
- Für öffentliche Endpunkte über VPC können zusätzliche NAT-Gateway- und Datenübertragungsgebühren anfallen
- Keine zusätzlichen Transfer Family Family-Gebühren, die über die Standardgebühren von 0 USD hinausgehen. 40/GB Gebühr für die Datenverarbeitung

Verfahren zum Erstellen eines Transfer Family Family-Servers, der als Remote-SFTP-Server verwendet werden kann

Im Folgenden beschreiben wir die Schritte zum Erstellen eines Transfer Family Family-Servers, der als Remote-SFTP-Server für dieses Tutorial dient. Beachten Sie Folgendes:

- Wir verwenden einen Transfer Family Family-Server, um einen Remote-SFTP-Server darzustellen. Typische Benutzer von SFTP-Connectoren haben ihren eigenen Remote-SFTP-Server. Siehe [Erstellen Sie einen Transfer Family SFTP-Server und einen Benutzer](#).
- Da wir einen Transfer Family Family-Server verwenden, verwenden wir auch einen vom Service verwalteten SFTP-Benutzer. Der Einfachheit halber haben wir die Berechtigungen, die dieser Benutzer für den Zugriff auf den Transfer Family Family-Server benötigt, mit den Berechtigungen kombiniert, die er für die Verwendung unseres Connectors benötigt. Auch hier haben die meisten Anwendungsfälle für SFTP-Connectoren einen separaten SFTP-Benutzer, der keinem Transfer Family Family-Server zugeordnet ist. Siehe [Erstellen Sie einen Transfer Family SFTP-Server und einen Benutzer](#).
- Da wir Amazon S3-Speicher für unseren Remote-SFTP-Server verwenden, müssen wir für das Tutorial einen zweiten Bucket erstellen **sftp-server-storage-east**, damit wir Dateien von einem Bucket in einen anderen übertragen können.

Erstellen Sie einen Transfer Family SFTP-Server und einen Benutzer

Die meisten Benutzer müssen keinen Transfer Family Family-SFTP-Server und keinen Benutzer erstellen, da Sie bereits über einen SFTP-Server mit Benutzern verfügen und diesen Server verwenden können, um Dateien von und zu übertragen. In diesem Tutorial verwenden wir der Einfachheit halber jedoch einen Transfer Family Family-Server, der als Remote-SFTP-Server fungiert.

Folgen Sie dem unter [Erstellen Sie einen SFTP-enabled Server](#) Erstellen eines Servers und [Schritt 3: Fügen Sie einen vom Service verwalteten Benutzer hinzu](#) Hinzufügen eines Benutzers beschriebenen Verfahren. Dies sind die Benutzerdetails, die wir für das Tutorial verwenden:

- Erstellen Sie Ihren vom Service verwalteten Benutzer, `sftp-testuser`.
 - Stellen Sie das Home-Verzeichnis ein auf `/sftp-server-storage-east/sftp-testuser`
 - Wenn Sie den Benutzer erstellen, speichern Sie einen öffentlichen Schlüssel. Später, wenn Sie das Geheimnis in Secrets Manager erstellen, müssen Sie den entsprechenden privaten Schlüssel angeben.
- Rolle: `sftp-connector-role`. Für das Tutorial verwenden wir dieselbe IAM-Rolle sowohl für unseren SFTP-Benutzer als auch für den Zugriff auf den SFTP-Connector. Wenn Sie Konnektoren für Ihre Organisation erstellen, haben Sie möglicherweise separate Benutzer- und Zugriffsrollen.
- Server-Hostschlüssel: Sie müssen den Server-Hostschlüssel verwenden, wenn Sie den Connector erstellen. Sie können diesen Schlüssel abrufen, indem Sie ihn `ssh-keyscan` für Ihren Server ausführen. Wenn Ihre Server-ID beispielsweise lautet `s-1111aaaa2222bbbb3` und ihr Endpunkt in `istus-east-1`, ruft der folgende Befehl den Server-Host-Schlüssel ab:

```
ssh-keyscan s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

Kopieren Sie diesen Text irgendwo, da Sie ihn in die [Schritt 2: Erstellen und testen Sie einen SFTP-Connector](#) Prozedur einfügen müssen.

Kombinierte Benutzer- und Zugriffsrolle

Für das Tutorial verwenden wir eine einzelne, kombinierte Rolle. Wir verwenden diese Rolle sowohl für unseren SFTP-Benutzer als auch für den Zugriff auf den Connector. Das folgende Beispiel enthält die Details für diese Rolle, falls Sie die Aufgaben im Tutorial ausführen möchten.

Das folgende Beispiel gewährt die erforderlichen Berechtigungen für den Zugriff auf unsere beiden Buckets in Amazon S3 und das Secret namens, das in Secrets Manager `aws/transfer/sftp-connector1` gespeichert ist. Für das Tutorial wird diese Rolle benannt `sftp-connector-role`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
```

```

        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::sftp-server-storage-east",
            "arn:aws:s3:::sftp-server-storage-east"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": [
            "arn:aws:s3:::sftp-server-storage-east/*",
            "arn:aws:s3:::sftp-server-storage-east/*"
        ]
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:aws/transfer/sftp-connector1-6RandomCharacters"
    }
]
}

```

Vollständige Informationen zum Erstellen von Rollen für Transfer Family finden Sie unter [Eine Benutzerrolle erstellen](#). So erstellen Sie eine Rolle.

Einrichtung einer Amazon API Gateway Gateway-Methode als benutzerdefinierter Identitätsanbieter

Dieses Tutorial zeigt, wie Sie eine Amazon API Gateway Gateway-Methode einrichten und sie als benutzerdefinierten Identitätsanbieter verwenden, um Dateien auf einen AWS Transfer Family Server hochzuladen. In diesem Tutorial werden die [Stack-Vorlage Basic](#) und andere grundlegende Funktionen nur als Beispiel verwendet.

Themen

- [Voraussetzungen](#)
- [Schritt 1: Erstellen Sie einen CloudFormation Stack](#)
- [Schritt 2: Überprüfen Sie die Konfiguration der API Gateway Gateway-Methode für Ihren Server](#)
- [Schritt 3: Die Transfer Family Family-Serverdetails anzeigen](#)
- [Schritt 4: Testen Sie, ob Ihr Benutzer eine Verbindung zum Server herstellen kann](#)
- [Schritt 5: Testen Sie die SFTP-Verbindung und die Dateiübertragung](#)
- [Schritt 6: Beschränken Sie den Zugriff auf den Bucket](#)
- [Aktualisieren Sie Lambda, wenn Sie Amazon EFS verwenden](#)

Voraussetzungen

Bevor Sie die Transfer Family Family-Ressourcen in erstellen CloudFormation, erstellen Sie Ihren Speicher und Ihre Benutzerrolle.

Um Speicherplatz anzugeben und eine Benutzerrolle zu erstellen

1. Je nachdem, welchen Speicher Sie verwenden, finden Sie weitere Informationen in der folgenden Dokumentation:
 - Informationen zum Erstellen eines Amazon S3 S3-Buckets finden Sie unter [Wie erstelle ich einen S3-Bucket?](#) im Amazon Simple Storage Service-Benutzerhandbuch.
 - Informationen zum Erstellen eines Amazon EFS-Dateisystems finden Sie unter [Ein Amazon EFS-Dateisystem konfigurieren](#).
2. Informationen zum Erstellen einer Benutzerrolle finden Sie unter [Erstellen Sie eine IAM-Rolle und -Richtlinie](#)

Sie geben die Details für Ihren Speicher und Ihre Benutzerrolle ein, wenn Sie Ihren CloudFormation Stack im nächsten Abschnitt erstellen.

Schritt 1: Erstellen Sie einen CloudFormation Stack

Um einen AWS CloudFormation Stapel aus der bereitgestellten Vorlage zu erstellen

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Wählen Sie Stack erstellen und anschließend Mit neuen Ressourcen (Standard) aus.
3. Wählen Sie im Bereich Voraussetzung — Vorlage vorbereiten die Option Vorhandene Vorlage auswählen aus.
4. Kopieren Sie diesen Link, [Basic Stack Template](#), und fügen Sie ihn in das Amazon S3 S3-URL-Feld ein.
5. Klicken Sie auf Weiter.
6. Geben Sie Parameter an, einschließlich eines Namens für Ihren Stack. Stellen Sie sicher, dass Sie Folgendes tun:
 - Ersetzen Sie die Standardwerte für UserName und UserPassword.
 - Geben Sie für UserHomeDirectory die Details für den Speicher (entweder einen Amazon S3 S3-Bucket oder ein Amazon EFS-Dateisystem) ein, den Sie zuvor erstellt haben.
 - Ersetzen Sie den Standard UserRoleArn durch die Benutzerrolle, die Sie zuvor erstellt haben. Die AWS Identity and Access Management (IAM-) Rolle muss über die entsprechenden Berechtigungen verfügen. Ein Beispiel für eine IAM-Rolle und eine Bucket-Richtlinie finden Sie unter [Schritt 6: Beschränken Sie den Zugriff auf den Bucket](#)
 - Wenn Sie sich mit einem öffentlichen Schlüssel statt mit einem Passwort authentifizieren möchten, geben Sie Ihren öffentlichen Schlüssel in das UserPublicKey1 Feld ein. Wenn Sie zum ersten Mal über SFTP eine Verbindung zum Server herstellen, geben Sie anstelle eines Kennworts den privaten Schlüssel an.
7. Wählen Sie Weiter und klicken Sie dann auf der Seite Stack-Optionen konfigurieren erneut auf Weiter.
8. Überprüfen Sie die Details für den Stack, den Sie gerade erstellen, und wählen Sie dann Stapel erstellen aus.

 Note

Unten auf der Seite müssen Sie unter Funktionen angeben, dass dadurch CloudFormation möglicherweise IAM-Ressourcen erstellt werden.

Schritt 2: Überprüfen Sie die Konfiguration der API Gateway Gateway-Methode für Ihren Server

 Note

Um die Sicherheit zu verbessern, können Sie eine Firewall für Webanwendungen konfigurieren. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an ein Amazon API Gateway weitergeleitet werden. Details hierzu finden Sie unter [Fügen Sie eine Firewall für Webanwendungen hinzu](#).

 API-Gateway-Caching nicht aktivieren

Aktivieren Sie das Caching nicht für Ihre API-Gateway-Methode, wenn Sie sie als benutzerdefinierten Identitätsanbieter für Transfer Family verwenden. Caching ist aus folgenden Gründen unangemessen und für Authentifizierungsanfragen ungültig:

- Jede Authentifizierungsanfrage ist einzigartig und erfordert eine Live-Antwort, keine zwischengespeicherte Antwort
- Caching bietet keine Vorteile, da Transfer Family niemals doppelte oder wiederholte Anfragen an das API Gateway sendet.
- Wenn Sie das Caching aktivieren, antwortet das API Gateway mit nicht übereinstimmenden Daten, was zu ungültigen Antworten auf Authentifizierungsanfragen führt.

Um die Konfiguration der API Gateway Gateway-Methode für Ihren Server zu überprüfen und bereitzustellen

1.

Öffnen Sie die API Gateway Gateway-Konsole unter <https://console.aws.amazon.com/apigateway/>.

2. Wählen Sie die Basisvorlagen-API für Transfer Custom Identity Provider aus, die von der CloudFormation Vorlage generiert wurde.
3. Wählen Sie im Bereich Ressourcen die Option GET und anschließend Method Request aus.
4. Wählen Sie für Aktionen die Option Deploy API aus. Wählen Sie für die Bereitstellungsphase die Option prod und dann Deploy aus.

Nachdem die API Gateway Gateway-Methode erfolgreich bereitgestellt wurde, können Sie sich ihre Leistung im Abschnitt Stage Editor ansehen.

 Note

Kopieren Sie die Aufruf-URL-Adresse, die oben auf der Seite angezeigt wird. Sie benötigen sie für den nächsten Schritt.

Schritt 3: Die Transfer Family Family-Serverdetails anzeigen

Wenn Sie die Vorlage verwenden, um einen CloudFormation Stack zu erstellen, wird automatisch ein Transfer Family Family-Server erstellt.

So zeigen Sie Ihre Transfer Family Family-Serverdetails an

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Wählen Sie den Stapel aus, den Sie erstellt haben.
3. Wählen Sie die Registerkarte Resources (Ressourcen) aus.

Resources (18)			
Search resources			
Logical ID	Physical ID	Type	
ApiCloudWatchLogsRole	-ApiCloudWatchLogsRole-	AWS::IAM::Role	
ApiDeployment202008		AWS::ApiGateway::Deployment	
ApiLoggingAccount		AWS::ApiGateway::Account	
ApiStage	prod	AWS::ApiGateway::Stage	
CloudWatchLoggingRole	-CloudWatchLoggingRole-	AWS::IAM::Role	
CustomIdentityProviderApi		AWS::ApiGateway::RestApi	
GetUserConfigLambda	-GetUserConfigLambda-	AWS::Lambda::Function	
GetUserConfigLambdaPermission	GetUserConfigLambdaPermission-	AWS::Lambda::Permission	
GetUserConfigRequest		AWS::ApiGateway::Method	
GetUserConfigResource		AWS::ApiGateway::Resource	
GetUserConfigResponseModel	UserConfigResponseModel	AWS::ApiGateway::Model	
LambdaExecutionRole	-LambdaExecutionRole-	AWS::IAM::Role	
ServerIdResource		AWS::ApiGateway::Resource	
ServersResource		AWS::ApiGateway::Resource	
TransferIdentityProviderRole	-TransferIdentityProviderRole-	AWS::IAM::Role	
TransferServer	arn:aws:transfer:us-east-2:::server/s-	AWS::Transfer::Server	
UserNameResource		AWS::ApiGateway::Resource	
UsersResource		AWS::ApiGateway::Resource	

Der Server-ARN wird in der Spalte Physikalische ID für die TransferServerZeile angezeigt. Die Server-ID ist im ARN enthalten, zum Beispiel s-11112222333344445.

- Öffnen Sie die AWS Transfer Family Konsole unter und wählen Sie auf der <https://console.aws.amazon.com/transfer/>Seite Server den neuen Server aus.

Die Server-ID entspricht der ID, die für die TransferServerRessource in angezeigt wird CloudFormation.

Schritt 4: Testen Sie, ob Ihr Benutzer eine Verbindung zum Server herstellen kann

Um zu testen, ob Ihr Benutzer mithilfe der Transfer Family Family-Konsole eine Verbindung zum Server herstellen kann

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie auf der Seite Server Ihren neuen Server aus, klicken Sie auf Aktionen und dann auf Test.
3. Geben Sie den Text für Ihre Anmeldeinformationen in das Feld Benutzername und in das Feld Passwort ein. Dies sind die Werte, die Sie bei der Bereitstellung des CloudFormation Stacks festgelegt haben.
4. Wählen Sie für Serverprotokoll die Option SFTP aus, und geben **127.0.0.1** Sie für Quell-IP den Wert ein.
5. Wählen Sie Test aus.

Wenn die Benutzerauthentifizierung erfolgreich ist, gibt der Test eine StatusCode: 200 HTML-Antwort und ein JSON-Objekt zurück, das die Details der Rollen und Berechtigungen des Benutzers enthält. Beispiel:

```
{
  "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/my-user-role\",
  \"HomeDirectory\": \"/${transfer:HomeBucket}/\",
  \"StatusCode\": 200,
  \"Message\": \"\",
  \"Url\": \"https://1a2b3c4d5e.execute-api.us-east-2.amazonaws.com/prod/servers/s-1234abcd5678efgh0/users/myuser/config\"
}
```

Wenn der Test fehlschlägt, fügen Sie der Rolle, die Sie für Ihre API verwenden, eine der von API Gateway AWS verwalteten Richtlinien hinzu.

Schritt 5: Testen Sie die SFTP-Verbindung und die Dateiübertragung

Um die SFTP-Verbindung zu testen

1. Öffnen Sie auf einem Linux- oder macOS-Gerät ein Befehlsterminal.

2. Geben Sie einen der folgenden Befehle ein, je nachdem, ob Sie ein Passwort oder ein key pair für die Authentifizierung verwenden.

- Wenn Sie ein Passwort verwenden, geben Sie diesen Befehl ein:

```
sftp -o PubkeyAuthentication=no myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Geben Sie bei der Aufforderung Ihr Passwort ein.

- Wenn Sie ein key pair verwenden, geben Sie diesen Befehl ein:

```
sftp -i private-key-file myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Note

Geben Sie für diese sftp Befehle den Code für den Standort AWS-Region Ihres Transfer Family Family-Servers ein. Wenn sich Ihr Server beispielsweise in USA Ost (Ohio) befindet, geben Sie ein **us-east-2**.

3. Stellen Sie bei der sftp> Aufforderung sicher, dass Sie Verzeichnisse und Dateien hochladen (putget), herunterladen () und anzeigen können (pwd und ls).

Schritt 6: Beschränken Sie den Zugriff auf den Bucket

Sie können einschränken, wer auf einen bestimmten Amazon S3 S3-Bucket zugreifen kann. Das folgende Beispiel zeigt die Einstellungen, die in Ihrem CloudFormation Stack und in der Richtlinie, die Sie für Ihren Benutzer auswählen, zu verwenden sind.

In diesem Beispiel legen wir die folgenden Parameter für den CloudFormation Stack fest:

- CreateServer: true
- UserHomeDirectory: /amzn-s3-demo-bucket1
- UserName: myuser
- UserPassword: MySuperSecretPassword

⚠ Important

Dies ist ein Beispielpasswort. Achten Sie bei der Konfiguration Ihrer API-Gateway-Methode darauf, dass Sie ein sicheres Passwort eingeben.

- UserPublicKey1: *your-public-key*
- UserRoleArn: arn:aws:iam::*role-id*:role/myuser-api-gateway-role

Das UserPublicKey1 ist ein öffentlicher Schlüssel, den Sie als Teil eines public/private key pair generiert haben.

Der *role-id* ist einzigartig für die Benutzerrolle, die Sie erstellen. Die dem beigefügte Richtlinie myuser-api-gateway-role lautet wie folgt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectAcl",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```


Um über SFTP eine Verbindung zum Server herzustellen, geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein.

- Wenn Sie ein Passwort zur Authentifizierung verwenden, führen Sie den folgenden Befehl aus:

```
sftp -o PubkeyAuthentication=no myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
```

Geben Sie bei der Aufforderung Ihr Passwort ein.

- Wenn Sie ein key pair zur Authentifizierung verwenden, führen Sie den folgenden Befehl aus:

```
sftp -i private-key-file myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
```

Note

Verwenden Sie für diese sftp Befehle die ID des Ortes, AWS-Region an dem sich Ihr Transfer Family Family-Server befindet. Wenn sich Ihr Server beispielsweise in USA Ost (Ohio) befindet, verwenden Sie `us-east-2`.

An der sftp Eingabeaufforderung werden Sie zu Ihrem Home-Verzeichnis weitergeleitet, das Sie anzeigen können, indem Sie den pwd Befehl ausführen. Beispiel:

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
```

Der Benutzer kann keine Verzeichnisse oberhalb des Home-Verzeichnisses anzeigen. Beispiel:

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

Aktualisieren Sie Lambda, wenn Sie Amazon EFS verwenden

Wenn Sie Amazon EFS als Speicheroption für Ihren Transfer Family Family-Server ausgewählt haben, müssen Sie die Lambda-Funktion für Ihren Stack bearbeiten.

Um Ihrer Lambda-Funktion ein Posix-Profil hinzuzufügen

1. Öffnen Sie die Lambda-Konsole unter <https://console.aws.amazon.com/lambda/>.
2. Wählen Sie die Lambda-Funktion aus, die Sie zuvor erstellt haben. Die Lambda-Funktion hat das Format ***stack-name***- GetUserConfigLambda - ***lambda-identifier***, wobei ***stack-name*** der CloudFormation Stack-Name und der Bezeichner für die Funktion ***lambda-identifier*** ist.
3. Wählen Sie auf der Registerkarte Code die Option index.js aus, um den Code für die Funktion anzuzeigen.
4. Fügen Sie im response die folgende Zeile zwischen Policy und hinzuHomeDirectory:

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

Wobei ***gid-value*** es sich bei ***uid-value*** und um ganze Zahlen (0 oder größer) handelt, die jeweils die Benutzer-ID und die Gruppen-ID darstellen.

Nachdem Sie das Posix-Profil hinzugefügt haben, könnte das Antwortfeld beispielsweise wie folgt aussehen:

```
response = {  
  Role: 'arn:aws:iam::123456789012:role/api-gateway-transfer-efs-role', // The  
  user will be authenticated if and only if the Role field is not blank  
  Policy: '', // Optional JSON blob to further restrict this user's permissions  
  PosixProfile: {"Gid": 65534, "Uid": 65534},  
  HomeDirectory: '/fs-fab2c234' // Not required, defaults to '/'  
};
```

Einrichtung einer AS2-Konfiguration

In diesem Tutorial wird beschrieben, wie Sie eine AS2-Konfiguration (Applicability Statement 2) mit einrichten. AWS Transfer Family Nachdem Sie die hier beschriebenen Schritte ausgeführt haben, verfügen Sie über einen AS2-enabled Server, der bereit ist, AS2-Nachrichten von einem Beispielhandelspartner anzunehmen. Sie werden auch über einen Konnektor verfügen, mit dem AS2-Nachrichten an den Musterhandelspartner gesendet werden können.

Note

In einigen Teilen des Beispiel-Setups wird das AWS Command Line Interface (AWS CLI) verwendet. Falls Sie das noch nicht installiert haben AWS CLI, finden Sie weitere

Informationen unter [Installieren oder Aktualisieren der neuesten Version von AWS CLI](#) im AWS Command Line Interface Benutzerhandbuch.

1. Erstellen Sie Zertifikate für sich und Ihren Handelspartner. Wenn Sie bereits Zertifikate haben, die Sie verwenden können, können Sie diesen Abschnitt überspringen.

Dieser Vorgang wird unter beschrieben [Schritt 1: Zertifikate für AS2 erstellen](#).

2. Importieren Sie die Zertifikate, die Sie in Schritt 1 erstellt haben.

Dieser Vorgang wird unter beschrieben [Schritt 2: Zertifikate als Transfer Family Family-Zertifikatsressourcen importieren](#).

3. Um Ihre Handelspartner einzurichten, erstellen Sie ein lokales Profil und ein Partnerprofil.

Dieser Vorgang wird unter beschrieben [Schritt 3: Erstellen Sie Profile für Sie und Ihren Handelspartner](#).

4. Erstellen Sie einen AWS Transfer Family Server, der das AS2-Protokoll verwendet. Optional können Sie dem Server eine Elastic IP-Adresse hinzufügen, sodass er mit dem Internet verbunden ist.

Dieser Prozess wird unter beschrieben. [Schritt 4: Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet](#)

 Note

Sie müssen einen Transfer Family Family-Server nur für eingehende Übertragungen erstellen. Wenn Sie nur ausgehende Übertragungen durchführen, benötigen Sie keinen Transfer Family Family-Server.

5. Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Handelspartner.

Dieser Prozess wird unter beschrieben [Schritt 5: Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Partner](#).

 Note

Sie müssen eine Vereinbarung nur für eingehende Übertragungen erstellen. Wenn Sie nur ausgehende Überweisungen durchführen, benötigen Sie keine Vereinbarung.

6. Stellen Sie eine Verbindung zwischen Ihnen und Ihrem Handelspartner her.

Dieser Prozess wird unter beschrieben [Schritt 6: Stellen Sie eine Verbindung zwischen Ihnen und Ihrem Partner her](#).

 Note

Sie müssen einen Connector nur für ausgehende Übertragungen erstellen. Wenn Sie nur eingehende Übertragungen durchführen, benötigen Sie keinen Connector.

7. Testen Sie einen AS2-Dateiaustausch.

Dieser Vorgang wird unter beschrieben. [Schritt 7: Testen Sie den Austausch von Dateien über AS2 mithilfe von Transfer Family](#)

Nachdem Sie diese Schritte abgeschlossen haben, können Sie wie folgt vorgehen:

- Senden Sie Dateien mit dem Befehl `Transfer Family start-file-transfer` AWS Command Line Interface (AWS CLI) an einen AS2-enabled Remote-Partnerserver.
- Empfangen Sie Dateien von einem AS2-enabled Remote-Partnerserver auf Port 5080 über Ihren Virtual Private Cloud (VPC) -Endpunkt.

Schritt 1: Zertifikate für AS2 erstellen

Beide Parteien an einer AS2-Börse benötigen X.509 Zertifikate. Sie können diese Zertifikate auf beliebige Weise erstellen. In diesem Thema wird beschrieben, wie Sie [OpenSSL](#) von der Befehlszeile aus verwenden, um ein Stammzertifikat zu erstellen und anschließend untergeordnete Zertifikate zu signieren. Beide Parteien müssen ihre eigenen Zertifikate generieren.

 Note

Die Schlüssellänge für AS2-Zertifikate muss mindestens 2048 Bit und höchstens 4096 Bit betragen.

Beachten Sie Folgendes, um Dateien mit einem Partner zu übertragen:

- Sie können Zertifikate an Profile anhängen. Die Zertifikate enthalten öffentliche oder private Schlüssel.
- Ihr Handelspartner sendet Ihnen seine öffentlichen Schlüssel und Sie senden ihm Ihre.
- Ihr Handelspartner verschlüsselt Nachrichten mit Ihrem öffentlichen Schlüssel und signiert sie mit seinem privaten Schlüssel. Umgekehrt verschlüsseln Sie Nachrichten mit dem öffentlichen Schlüssel Ihres Partners und signieren sie mit Ihrem privaten Schlüssel.

 Note

Wenn Sie es vorziehen, Schlüssel mit einer GUI zu verwalten, [Portecle](#) ist dies eine Option, die Sie verwenden können.

Um Beispielzertifikate zu generieren

 Important

Senden Sie Ihrem Partner nicht Ihre privaten Schlüssel. In diesem Beispiel generieren Sie einen Satz selbstsignierter öffentlicher und privater Schlüssel für eine Partei. Wenn Sie zu Testzwecken als beide Geschäftspartner agieren möchten, können Sie diese Anweisungen wiederholen, um zwei Schlüsselsätze zu generieren: einen für jeden Geschäftspartner. In diesem Fall müssen Sie nicht zwei Root-Zertifizierungsstellen (CAs) generieren.

1. Führen Sie den folgenden Befehl aus, um einen privaten RSA-Schlüssel mit einem 2048-Bit-Modul zu generieren.

```
/usr/bin/openssl genrsa -out root-ca-key.pem 2048
```

2. Führen Sie den folgenden Befehl aus, um ein selbstsigniertes Zertifikat mit Ihrer Datei zu erstellen. `root-ca-key.pem`

```
/usr/bin/openssl req \
-x509 -new -nodes -sha256 \
-days 1825 \
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=R00TCA" \
-key root-ca-key.pem \
-out root-ca.pem
```

Das `-subj` Argument besteht aus den folgenden Werten.

	Name	Description
C	Ländercode	Ein aus zwei Buchstaben bestehender Code für das Land, in dem Ihre Organisation ansässig ist.
ST	Bundesland, Region oder Provinz	Das Bundesland, die Region oder die Provinz, in der Ihre Organisation ansässig ist. (In diesem Fall bezieht sich Region nicht auf Ihre AWS-Region.)
L	Ortsname	Die Stadt, in der sich Ihre Organisation befindet.
O	Name der Organisation	Der vollständige offizielle Name Ihrer Organisation, einschließlich Suffixen wie LLC, Corp usw.
OU	Name der Organisationseinheit	Die Abteilung in Ihrer Organisation, die sich mit diesem Zertifikat befasst.

	Name	Description
CN	Allgemeiner Name oder vollqualifizierter Domänenna me (FQDN)	In diesem Fall erstellen wir ein Stammzertifikat, der Wert ist R00TCA also. In diesen Beispielen beschreiben wir den Zweck des Zertifikats. CN

- Erstellen Sie einen Signaturschlüssel und einen Verschlüsselungsschlüssel für Ihr lokales Profil.

```
/usr/bin/openssl genrsa -out signing-key.pem 2048
/usr/bin/openssl genrsa -out encryption-key.pem 2048
```

Note

Einige AS2-enabled Server, wie OpenAS2, erfordern, dass Sie dasselbe Zertifikat sowohl für das Signieren als auch für die Verschlüsselung verwenden. In diesem Fall können Sie denselben privaten Schlüssel und dasselbe Zertifikat für beide Zwecke importieren. Führen Sie dazu diesen Befehl anstelle der beiden vorherigen Befehle aus:

```
/usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
```

- Führen Sie die folgenden Befehle aus, um Certificate Signing Requests (CSRs) für den zu signierenden Stammschlüssel zu erstellen.

```
/usr/bin/openssl req -new -key signing-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Signer" -out signing-
key-csr.pem
```

```
/usr/bin/openssl req -new -key encryption-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Encrypter" -out
encryption-key-csr.pem
```

- Als Nächstes müssen Sie eine `signing-cert.conf` Datei und eine `encryption-cert.conf` Datei erstellen.

- Verwenden Sie einen Texteditor, um die `signing-cert.conf` Datei mit dem folgenden Inhalt zu erstellen:

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = digitalSignature, nonRepudiation
```

- Verwenden Sie einen Texteditor, um die `encryption-cert.conf` Datei mit dem folgenden Inhalt zu erstellen:

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = dataEncipherment
```

6. Schließlich erstellen Sie die signierten Zertifikate, indem Sie die folgenden Befehle ausführen.

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in signing-key-  
csr.pem -out signing-cert.pem -CA \  
root-ca.pem -CAkey root-ca-key.pem -extfile signing-cert.conf
```

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in encryption-key-  
csr.pem -out encryption-cert.pem \  
-CA root-ca.pem -CAkey root-ca-key.pem -extfile encryption-cert.conf
```

Schritt 2: Zertifikate als Transfer Family Family-Zertifikatsressourcen importieren

In diesem Verfahren wird erklärt, wie Zertifikate mithilfe von importiert AWS CLI werden. Wenn Sie stattdessen die Transfer Family Family-Konsole verwenden möchten, finden Sie weitere Informationen unter [the section called “AS2-Zertifikate importieren”](#).

Führen Sie die folgenden `import-certificate` Befehle aus, um die Signatur- und Verschlüsselungszertifikate zu importieren, die Sie in Schritt 1 erstellt haben. Wenn Sie dasselbe Zertifikat für Verschlüsselung und Signierung verwenden, importieren Sie dasselbe Zertifikat zweimal (einmal mit der SIGNING Verwendung und erneut mit der ENCRYPTION Verwendung).

Note

Wenn Sie über eine Datei verfügen, die sowohl ein Zertifikat als auch dessen Kette enthält, können Sie diese Datei nur mithilfe des `certificate` Parameters für den `import-certificate` Befehl bereitstellen. Beispiel:

```
aws transfer import-certificate --usage ENCRYPTION --certificate
file://combined-cert-and-chain-file.pem
```

Wenn Sie den `certificate` Parameter verwenden, um sowohl das Zertifikat als auch seine Kette hochzuladen, verwenden Sie den `certificate-chain` Parameter nicht.

Wenn Sie das Zertifikat und seine Kette kombinieren, wird Ihr Schlüssel nach herkömmlichen PEM-Standards formatiert, die alle 64 Zeichen einen Zeilenumbruch „\n“ enthalten. Das gespeicherte Zertifikat entspricht funktionell dem Zertifikat, das Sie hochgeladen haben, mit dem einzigen Unterschied, dass die `DescribeCertificate` Antwort über die AWS CLI diese Zeilenumbruchzeichen enthält.

```
aws transfer import-certificate --usage SIGNING --certificate file://signing-cert.pem \
--private-key file://signing-key.pem --certificate-chain file://root-ca.pem
```

Dieser Befehl gibt Ihre Signatur zurück. `CertificateId` Im nächsten Abschnitt wird diese Zertifikat-ID als bezeichnet *my-signing-cert-id*.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-
cert.pem \
--private-key file://encryption-key.pem --certificate-chain file://root-
ca.pem
```

Dieser Befehl gibt Ihre Verschlüsselung zurück `CertificateId`. Im nächsten Abschnitt wird diese Zertifikat-ID als bezeichnet *my-encrypt-cert-id*.

Importieren Sie als Nächstes die Verschlüsselungs- und Signaturzertifikate Ihres Partners, indem Sie die folgenden Befehle ausführen.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://partner-
encryption-cert.pem \
--certificate-chain file://partner-root-ca.pem
```

Dieser Befehl gibt die Verschlüsselung Ihres Partners zurück `CertificateId`. Im nächsten Abschnitt wird diese Zertifikat-ID als bezeichnet *partner-encrypt-cert-id*.

```
aws transfer import-certificate --usage SIGNING --certificate file:///partner-signing-  
cert.pem \  
--certificate-chain file:///partner-root-ca.pem
```

Dieser Befehl gibt die Signatur Ihres Partners zurück `CertificateId`. Im nächsten Abschnitt wird diese Zertifikat-ID als bezeichnet *partner-signing-cert-id*.

Schritt 3: Erstellen Sie Profile für Sie und Ihren Handelspartner

In diesem Verfahren wird erklärt, wie Sie AS2-Profile mithilfe AWS CLI von erstellen. Wenn Sie stattdessen die Transfer Family Family-Konsole verwenden möchten, finden Sie weitere Informationen unter [the section called “Erstellen Sie AS2-Profil”](#).

Erstellen Sie Ihr lokales AS2-Profil, indem Sie den folgenden Befehl ausführen. Dieser Befehl verweist auf die Zertifikate, die Ihre öffentlichen und privaten Schlüssel enthalten.

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \  
my-signing-cert-id my-encrypt-cert-id
```

Dieser Befehl gibt Ihre Profil-ID zurück. Im nächsten Abschnitt wird diese ID als bezeichnet *my-profile-id*.

Erstellen Sie nun das Partnerprofil, indem Sie den folgenden Befehl ausführen. Dieser Befehl verwendet nur die Public-Key-Zertifikate Ihres Partners. Um diesen Befehl zu verwenden, ersetzen Sie das *user input placeholders* durch Ihre eigenen Informationen, z. B. den AS2-Namen und die Zertifikat-IDs Ihres Partners.

```
aws transfer create-profile --as2-id PARTNER-COMPANY --profile-type PARTNER --  
certificate-ids \  
partner-signing-cert-id partner-encrypt-cert-id
```

Dieser Befehl gibt die Profil-ID Ihres Partners zurück. Im nächsten Abschnitt wird diese ID als bezeichnet *partner-profile-id*.

 Note

MYCORP Ersetzen Sie die Befehle in den vorherigen Befehlen durch den Namen Ihrer Organisation und **PARTNER-COMPANY** durch den Namen der Organisation Ihres Handelspartners.

Schritt 4: Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet

In diesem Verfahren wird erklärt, wie Sie mithilfe der Transfer Family einen AS2-enabled Server erstellen AWS CLI.

 Note

In vielen der Beispielschritte werden Befehle verwendet, mit denen Parameter aus einer Datei geladen werden. Weitere Informationen zur Verwendung von Dateien zum Laden von Parametern finden Sie unter [So laden Sie Parameter aus einer Datei](#).

Wenn Sie stattdessen die Konsole verwenden möchten, finden Sie weitere Informationen unter [Erstellen Sie einen AS2-Server mit der Transfer Family Family-Konsole](#).

Ähnlich wie beim Erstellen eines SFTP- oder AWS Transfer Family FTPS-Servers erstellen Sie einen AS2-enabled Server mithilfe des `--protocols AS2` Befehlsparameters `create-server` AWS CLI. Derzeit unterstützt Transfer Family nur VPC-Endpunkttypen und Amazon S3 S3-Speicher mit dem AS2-Protokoll.

Wenn Sie Ihren AS2-enabled Server für Transfer Family mithilfe des `create-server` Befehls erstellen, wird automatisch ein VPC-Endpunkt für Sie erstellt. Dieser Endpunkt macht den TCP-Port 5080 verfügbar, sodass er AS2-Nachrichten akzeptieren kann.

Wenn Sie Ihren VPC-Endpunkt öffentlich dem Internet zugänglich machen möchten, können Sie Elastic IP-Adressen mit Ihrem VPC-Endpunkt verknüpfen.

Um diese Anweisungen verwenden zu können, benötigen Sie Folgendes:

- Die ID Ihrer VPC (z. B. `vpc-abcdef01`).
- Die IDs Ihrer VPC-Subnetze (z. B. `subnet-abcdef01`, `subnet-subnet-abcdef01`, `subnet-021345ab`).

- Eine oder mehrere IDs der Sicherheitsgruppen, die eingehenden Datenverkehr über den TCP-Port 5080 von Ihren Handelspartnern zulassen (z. B. sg-1234567890abcdef0 und sg-abcdef01234567890).
- (Optional) Die Elastic IP-Adressen, die Sie Ihrem VPC-Endpunkt zuordnen möchten.
- Wenn Ihr Handelspartner nicht über ein VPN mit Ihrer VPC verbunden ist, benötigen Sie ein Internet-Gateway. Weitere Informationen finden Sie unter [Verbinden mit dem Internet über ein Internet-Gateway](#) im Amazon-VPC-Benutzerhandbuch.

Um einen Server zu erstellen AS2-enabled

1. Führen Sie den folgenden Befehl aus. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
aws transfer create-server --endpoint-type VPC \
--endpoint-details VpcId=vpc-abcdef01,SubnetIds=subnet-abcdef01,subnet-
abcdef01,subnet-
021345ab,SecurityGroupIds=sg-abcdef01234567890,sg-1234567890abcdef0 --protocols AS2
\
--protocol-details As2Transports=HTTP
```

2. (Optional) Sie können den VPC-Endpunkt öffentlich machen. Sie können Elastic IP-Adressen nur über einen update-server Vorgang an einen Transfer Family Family-Server anhängen. Die folgenden Befehle stoppen den Server, aktualisieren ihn mit Elastic IP-Adressen und starten ihn dann erneut.

```
aws transfer stop-server --server-id your-server-id
```

```
aws transfer update-server --server-id your-server-id --endpoint-details \
AddressAllocationIds=eipalloc-abcdef01234567890,eipalloc-
1234567890abcdef0,eipalloc-abcd012345ccccccc
```

```
aws transfer start-server --server-id your-server-id
```

Dieser start-server Befehl erstellt automatisch einen DNS-Eintrag für Sie, der die öffentliche IP-Adresse für Ihren Server enthält. Um Ihrem Handelspartner Zugriff auf den Server zu gewähren, stellen Sie ihm die folgenden Informationen zur Verfügung. *your-region* Bezieht sich in diesem Fall auf Ihre AWS-Region.

`s-your-server-id.server.transfer.your-region.amazonaws.com`

Die vollständige URL, die Sie Ihrem Handelspartner zur Verfügung stellen, lautet wie folgt:

`http://s-your-server-id.server.transfer.your-region.amazonaws.com:5080`

3. Verwenden Sie die folgenden Befehle, um zu testen, ob auf Ihren AS2-enabled Server zugegriffen werden kann. Stellen Sie sicher, dass auf Ihren Server entweder über die private DNS-Adresse Ihres VPC-Endpunkts oder über Ihren öffentlichen Endpunkt (falls Sie Ihrem Endpunkt eine Elastic IP-Adresse zugeordnet haben) zugegriffen werden kann.

Wenn Ihr Server korrekt konfiguriert ist, ist die Verbindung erfolgreich. Sie erhalten jedoch eine Antwort mit dem HTTP-Statuscode 400 (Bad Request), da Sie keine gültige AS2-Nachricht senden.

- Führen Sie für einen öffentlichen Endpunkt (wenn Sie im vorherigen Schritt eine Elastic IP-Adresse zugewiesen haben) den folgenden Befehl aus und ersetzen Sie dabei Ihre Server-ID und Region.

```
curl -vv -X POST http://s-your-server-id.transfer.your-region.amazonaws.com:5080
```

- Wenn Sie eine Verbindung innerhalb Ihrer VPC herstellen, suchen Sie den privaten DNS-Namen Ihres VPC-Endpunkts, indem Sie die folgenden Befehle ausführen.

```
aws transfer describe-server --server-id s-your-server-id
```

Dieser `describe-server` Befehl gibt Ihre VPC-Endpunkt-ID im `VpcEndpointId` Parameter zurück. Verwenden Sie diesen Wert, um den folgenden Befehl auszuführen.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-your-vpc-endpoint-id
```

Dieser `describe-vpc-endpoints` Befehl gibt ein `DNSEntries` Array mit mehreren `DnsName` Parametern zurück. Verwenden Sie im folgenden Befehl den regionalen DNS-Namen (den Namen, der die Availability Zone nicht enthält).

```
curl -vv -X POST http://vpce-your-vpce.vpce-svc-your-vpce-svc.your-region.vpce.amazonaws.com:5080
```

Der folgende Befehl zeigt beispielsweise Beispielwerte für die Platzhalter im vorherigen Befehl.

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-  
svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

4. (Optional) Konfigurieren Sie eine Protokollierungsrolle. Transfer Family protokolliert den Status von gesendeten und empfangenen Nachrichten in einem strukturierten JSON-Format in CloudWatch Amazon-Protokollen. Um Transfer Family Zugriff auf die CloudWatch Protokolle in Ihrem Konto zu gewähren, müssen Sie eine Protokollierungsrolle auf Ihrem Server konfigurieren.

Erstellen Sie eine `transfer.amazonaws.com` vertrauenswürdige AWS Identity and Access Management (IAM-) Rolle und fügen Sie die `AWSTransferLoggingAccess` verwaltete Richtlinie hinzu. Details hierzu finden Sie unter [Erstellen Sie eine IAM-Rolle und -Richtlinie](#). Notieren Sie sich den Amazon-Ressourcennamen (ARN) der IAM-Rolle, die Sie gerade erstellt haben, und verknüpfen Sie ihn mit dem Server, indem Sie den folgenden `update-server` Befehl ausführen:

```
aws transfer update-server --server-id your-server-id --logging-role  
arn:aws:iam::your-account-id:role/logging-role-name
```

Note

Obwohl die Logging-Rolle optional ist, empfehlen wir dringend, sie so einzurichten, dass Sie den Status Ihrer Nachrichten einsehen und Konfigurationsprobleme beheben können.

Schritt 5: Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Partner

In diesem Verfahren wird erklärt, wie Sie AS2-Vereinbarungen mithilfe von erstellen. AWS CLI Wenn Sie stattdessen die Transfer Family Family-Konsole verwenden möchten, finden Sie weitere Informationen unter [the section called “Erstellen Sie eine AS2-Vereinbarung”](#).

In Vereinbarungen werden die beiden Profile (lokal und Partner), ihre Zertifikate und eine Serverkonfiguration zusammengeführt, die eingehende AS2-Übertragungen zwischen zwei Parteien ermöglicht. Sie können Ihre Artikel auflisten, indem Sie die folgenden Befehle ausführen.

```
aws transfer list-profiles --profile-type LOCAL
```

```
aws transfer list-profiles --profile-type PARTNER
aws transfer list-servers
```

Für diesen Schritt sind ein Amazon S3 S3-Bucket und eine IAM-Rolle mit read/write Zugriff auf und vom Bucket erforderlich. Die Anweisungen zum Erstellen dieser Rolle entsprechen denen für die SFTP-, FTP- und FTPS-Protokolle der Transfer Family und sind unter verfügbar. [Erstellen Sie eine IAM-Rolle und -Richtlinie](#)

Um eine Vereinbarung zu erstellen, benötigen Sie die folgenden Elemente:

- Der Amazon S3 S3-Bucket-Name (und das Objektpräfix, falls angegeben) zum Speichern Ihrer AS2-Dateien. Wir empfehlen, separate Verzeichnisse für verschiedene Dateitypen anzugeben.
- Der ARN der IAM-Rolle mit Zugriff auf den Bucket
- Ihre Transfer Family Family-Server-ID
- Ihre Profil-ID und die Profil-ID Ihres Partners

Speichern Sie den folgenden Code in einer Datei, zum Beispiel `agreementDetails.json`. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
{
  "Description": "ExampleAgreementName",
  "ServerId": "your-server-id",
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "your-partner-profile-id",
  "AccessRole": "arn:aws:iam::111111111111:role/TransferAS2AccessRole",
  "Status": "ACTIVE",
  "PreserveFilename": "ENABLED",
  "EnforceMessageSigning": "ENABLED",
  "CustomDirectories": {
    "FailedFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-failed",
    "MdnFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-mdn",
    "PayloadFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-payload",
    "StatusFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-status",
    "TemporaryFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-temp"
  }
}
```

 Note

Um ein einzelnes Basisverzeichnis anstelle von separaten Verzeichnissen zu verwenden, entfernen Sie die `CustomDirectories` Zeile und ihre einzelnen Verzeichniszeilen aus dem vorherigen Code und verwenden Sie stattdessen den folgenden Parameter:

`"BaseDirectory": "/amzn-s3-demo-destination-bucket/AS2-inbox"`

Verwenden Sie nicht sowohl ein Basisverzeichnis als auch separate Verzeichnisparameter, da der Befehl sonst fehlschlägt.

Führen Sie anschließend den folgenden Befehl aus.

```
aws transfer create-agreement --cli-input-json file://agreementDetails.json
```

Bei Erfolg gibt dieser Befehl die ID für die Vereinbarung zurück. Sie können dann die Details der Vereinbarung mit dem folgenden Befehl anzeigen.

```
aws transfer describe-agreement --agreement-id agreement-id --server-id your-server-id
```

Schritt 6: Stellen Sie eine Verbindung zwischen Ihnen und Ihrem Partner her

In diesem Verfahren wird erklärt, wie Sie AS2-Konnektoren mithilfe von erstellen. AWS CLI Wenn Sie stattdessen die Transfer Family Family-Konsole verwenden möchten, finden Sie weitere Informationen unter [the section called "Konfigurieren Sie AS2-Konnektoren"](#).

Sie können den `StartFileTransfer` API-Vorgang verwenden, um Dateien, die in Amazon S3 gespeichert sind, mithilfe eines Connectors an den AS2-Endpunkt Ihres Handelspartners zu senden. Sie können die zuvor erstellten Profile finden, indem Sie den folgenden Befehl ausführen.

```
aws transfer list-profiles
```

Wenn Sie den Connector erstellen, müssen Sie die AS2-Server-URL Ihres Partners angeben. Kopieren Sie den folgenden Text in eine Datei mit dem Namen `testAS2Config.json`.

```
{  
  "Compression": "ZLIB",
```



```

"EncryptionAlgorithm": "AES256_CBC",
"LocalProfileId": "your-profile-id",
"MdnResponse": "SYNC",
"MdnSigningAlgorithm": "DEFAULT",
"MessageSubject": "Your Message Subject",
"PartnerProfileId": "partner-profile-id",
"PreserveContentType": "FALSE",
"SigningAlgorithm": "SHA256"
}

```

Note

Geben Sie den DES_EDE3_CBC Algorithmus nur anEncryptionAlgorithm, wenn Sie einen älteren Client unterstützen müssen, der ihn benötigt, da es sich um einen schwachen Verschlüsselungsalgorithmus handelt.

Führen Sie dann den folgenden Befehl aus, um den Connector zu erstellen.

```

aws transfer create-connector --url "http://partner-as2-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess \
--as2-config file:///path/to/testAS2Config.json

```

Schritt 7: Testen Sie den Austausch von Dateien über AS2 mithilfe von Transfer Family

Erhalten Sie eine Datei von Ihrem Handelspartner

Wenn Sie Ihrem VPC-Endpunkt eine öffentliche Elastic IP-Adresse zugeordnet haben, hat Transfer Family automatisch einen DNS-Namen erstellt, der Ihre öffentliche IP-Adresse enthält. Die Subdomain ist Ihre AWS Transfer Family Server-ID (im Format-1234567890abcdef0). Geben Sie Ihrem Handelspartner Ihre Server-URL im folgenden Format an.

```
http://s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com:5080
```

Wenn Sie Ihrem VPC-Endpunkt keine öffentliche Elastic IP-Adresse zugeordnet haben, suchen Sie nach dem Hostnamen des VPC-Endpunkts, der AS2-Nachrichten über HTTP POST von Ihnen

Handelspartnern auf Port 5080 annehmen kann. Verwenden Sie den folgenden Befehl, um die VPC-Endpunktdetails abzurufen.

```
aws transfer describe-server --server-id s-1234567890abcdef0
```

Nehmen wir beispielsweise an, der vorherige Befehl gibt die VPC-Endpunkt-ID von `vpce-1234abcd5678efghi` zurück. Dann würden Sie den folgenden Befehl verwenden, um die DNS-Namen abzurufen.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1234abcd5678efghi
```

Dieser Befehl gibt alle Details für den VPC-Endpunkt zurück, die Sie zum Ausführen des folgenden Befehls benötigen.

Der DNS-Name ist im `DnsEntries` Array aufgeführt. Ihr Handelspartner muss sich in Ihrer VPC befinden, um auf Ihren VPC-Endpunkt zugreifen zu können (z. B. über AWS PrivateLink oder ein VPN). Geben Sie Ihrem Partner Ihre VPC-Endpunkt-URL im folgenden Format an.

```
http://vpce-your-vpce-id.vpce-svc-your-vpce-svc-id.your-region.vpce.amazonaws.com:5080
```

Die folgende URL zeigt beispielsweise Beispielwerte für die Platzhalter in den vorherigen Befehlen.

```
http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

In diesem Beispiel werden erfolgreiche Übertragungen an dem Speicherort gespeichert, der in dem von Ihnen angegebenen `base-directory` Parameter angegeben ist.

[Schritt 5: Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Partner](#) Wenn wir erfolgreich Dateien mit dem Namen `myfile1.txt` und `empfangenmyfile2.txt`, werden die Dateien unter gespeichert/*path-defined-in-the-agreement*/processed/*original_filename.messageId.original_extension*. Hier werden die Dateien als `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` und gespeichert/`/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.messageId.txt`.

Wenn Sie bei der Erstellung Ihres Transfer Family Family-Servers eine Protokollierungsrolle konfiguriert haben, können Sie Ihre CloudWatch Protokolle auch auf den Status von AS2-Nachrichten überprüfen.

Senden Sie eine Datei an Ihren Handelspartner

Sie können Transfer Family verwenden, um AS2-Nachrichten zu senden, indem Sie auf die Connector-ID und die Pfade zu den Dateien verweisen, wie im folgenden Befehl `start-file-transfer` AWS Command Line Interface (AWS CLI) dargestellt:

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \  
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-  
bucket/myfile2.txt"
```

Führen Sie den folgenden Befehl aus, um die Details für Ihre Konnektoren abzurufen:

```
aws transfer list-connectors
```

Der `list-connectors` Befehl gibt die Connector-IDs, URLs und Amazon-Ressourcennamen (ARNs) für Ihre Konnektoren zurück.

Um die Eigenschaften eines bestimmten Connectors zurückzugeben, führen Sie den folgenden Befehl mit der ID aus, die Sie verwenden möchten:

```
aws transfer describe-connector --connector-id your-connector-id
```

Der `describe-connector` Befehl gibt alle Eigenschaften für den Connector zurück, einschließlich seiner URL, Rollen, Profile, MDNs (Message Disposition Notices), Tags und Überwachungsmetriken.

Sie können überprüfen, ob der Partner die Dateien erfolgreich erhalten hat, indem Sie sich die JSON- und MDN-Dateien ansehen. Diese Dateien werden gemäß den unter beschriebenen Konventionen benannt. [Dateinamen und Speicherorte](#) Wenn Sie bei der Erstellung des Connectors eine Protokollierungsrolle konfiguriert haben, können Sie Ihre CloudWatch Protokolle auch auf den Status von AS2-Nachrichten überprüfen.

Tutorial: Eine einfache Transfer Family Family-Web-App einrichten

In diesem Tutorial erfahren Sie, wie Sie eine Transfer Family Family-Web-App einrichten. Transfer Family Family-Web-Apps bieten eine einfache Schnittstelle für die Übertragung von Daten zu und von Amazon S3 über einen Webbrowser. Eine ausführliche Dokumentation zu dieser Funktion finden Sie unter [Familien-Web-Apps übertragen](#).

Web-App-Tutorial: Voraussetzungen

- Erstellen Sie entweder eine Kontoinstanz oder eine Organisationsinstanz von AWS IAM Identity Center. Details hierzu finden Sie unter [Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps](#).

Falls Sie IAM Identity Center nicht als Identitätsanbieter verwenden, [Integrieren Sie Okta als Ihren Identitätsanbieter für Web-Apps](#) wird veranschaulicht, wie Sie einen alternativen Identitätsanbieter (in diesem Fall Okta) verwenden.

- Sie benötigen einen Amazon S3 S3-Bucket, um mit Ihrer Transfer Family Family-Web-App zu interagieren. Details hierzu finden Sie unter [Einen Amazon S3 S3-Bucket konfigurieren](#)

Note

In diesem Tutorial wird davon ausgegangen, dass Sie das IAM Identity Center-Verzeichnis für Ihren Identitätsanbieter verwenden. Ist dies nicht der Fall, lesen Sie nach, [Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps](#) bevor Sie mit diesem Tutorial fortfahren.

Nachdem Sie das Tutorial abgeschlossen haben, kann sich Ihr Benutzer anmelden und mit der von Ihnen erstellten Web-App interagieren.

Schritt 1: Erstellen Sie die erforderlichen unterstützenden Ressourcen

Sie müssen Ihrem IAM Identity Center-Verzeichnis einen Benutzer hinzufügen. Sie benötigen außerdem zwei Rollen: eine für die Verwendung als Identitätsträgerrolle für Ihre Web-App und eine zweite für die Konfiguration einer Amazon S3 S3-Zugriffsgewährung. Für das Tutorial ermöglichen wir es den AWS Diensten, diese Rollen für uns zu erstellen.

So fügen Sie einen Benutzer hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie im linken Navigationsbereich Benutzer aus.
3. Wählen Sie Benutzer hinzufügen und geben Sie die Benutzerdetails an.

Geben Sie einen Benutzernamen, eine E-Mail-Adresse und andere erforderliche Informationen an. Sie können wählen, ob Sie dem Benutzer entweder eine E-Mail mit Anweisungen zur Einrichtung seines Passworts senden oder ein Einmalpasswort generieren, um es mit ihm zu teilen.

4. Wählen Sie Weiter und weisen Sie den neuen Benutzer optional einer oder mehreren Gruppen zu.
5. Wählen Sie Weiter und überprüfen Sie Ihre Auswahl.

Wenn alles gut aussieht, wählen Sie Benutzer hinzufügen aus, um den neuen Benutzer mit den von Ihnen angegebenen Details zu erstellen.

Für das Tutorial ist der Beispielbenutzer Bob Stiles, der Benutzername bobstiles und die E-Mail-Adresse bobstiles@example.com.

Schritt 2: Erstellen Sie eine Transfer Family Family-Web-App

So erstellen Sie eine Transfer Family Family-Web-App

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Web-Apps aus.
3. Wählen Sie Web-App erstellen aus.

Beachten Sie beim Authentifizierungszugriff, dass der Dienst die AWS IAM Identity Center Instanz, die Sie als Voraussetzung eingerichtet haben, automatisch findet.

4. Wählen Sie im Bereich Berechtigungstyp die Option Neue Servicerolle erstellen und verwenden aus. Der Dienst erstellt die Rolle des Identitätsträgers für Sie. Eine Identitätsträgerrolle umfasst die Identität eines authentifizierten Benutzers in seinen Sitzungen.
5. Akzeptieren Sie im Bereich Web-App-Einheiten den Standardwert 1, oder passen Sie ihn bei Bedarf auf einen höheren Wert an.
6. Fügen Sie ein Tag hinzu, das Ihnen bei der Organisation Ihrer Web-Apps hilft. Geben Sie für das Tutorial Name für den Schlüssel und Tutorial web app als Wert ein.

 Tip

Sie können den Namen der Web-App direkt auf der Listenseite der Web-Apps bearbeiten, nachdem Sie sie erstellt haben.

7. Wählen Sie Weiter, um die Seite Web-App entwerfen zu öffnen. Geben Sie auf diesem Bildschirm die folgenden Informationen ein.

Sie können optional einen Titel für Ihre Web-App angeben. Sie können auch Bilddateien für Ihr Logo und Favicon hochladen.

- Passen Sie für den Seitentitel den Titel für den Browser-Tab an, den Ihre Benutzer sehen, wenn sie eine Verbindung zur Web-App herstellen. Wenn Sie nichts für den Seitentitel eingeben, wird standardmäßig Transfer Web App verwendet.
- Laden Sie für das Logo eine Bilddatei hoch. Die maximale Dateigröße für Ihr Logobild beträgt 50 KB.
- Laden Sie für das Favicon eine Bilddatei hoch. Die maximale Dateigröße für Ihr Favicon beträgt 20 KB.

8. Wählen Sie Weiter und anschließend Web-App erstellen.

Um ein Markenerlebnis zu bieten, können Sie Ihren Benutzern eine benutzerdefinierte URL für den Zugriff auf Ihre Transfer Family Family-Web-App bereitstellen. Details hierzu finden Sie unter [Aktualisieren Sie Ihren Zugriffsendpunkt mit einer benutzerdefinierten URL](#).

Schritt 3: Konfigurieren Sie Cross-origin Resource Sharing (CORS) für Ihren Bucket

Sie müssen Cross-Origin Resource Sharing (CORS) für alle Buckets einrichten, die von Ihrer Web-App verwendet werden. Eine CORS-Konfiguration ist ein Dokument, das Regeln definiert, die die Ursprünge identifizieren, denen Sie Zugriff auf Ihren Bucket gewähren. Weitere Informationen zu CORS finden Sie unter [Konfiguration von Cross-Origin Resource Sharing \(CORS\)](#).

So richten Sie Cross-origin Resource Sharing (CORS) für Ihren Amazon S3 S3-Bucket ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.

2. Wählen Sie im linken Navigationsbereich Buckets aus, suchen Sie im Suchdialogfeld nach Ihrem Bucket und wählen Sie dann den Tab Permissions.
3. Wählen Sie unter Cross-origin Resource Sharing (CORS) die Option Bearbeiten aus und fügen Sie den folgenden Code ein. *AccessEndpoint* Ersetzen Sie es durch den tatsächlichen Zugriffsendpunkt für Ihre Web-App. Achten Sie darauf, keine abschließenden Schrägstriche einzugeben, da dies zu Fehlern führt, wenn Benutzer versuchen, sich bei Ihrer Web-App anzumelden.
 - Falsches Beispiel: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Richtiges Beispiel: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Wenn Sie einen Bucket für mehrere Web-Apps wiederverwenden, fügen Sie deren Web-App-Zugriffsendpunkte an die Liste an. AllowedOrigins

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://AccessEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
```

```
        "x-amz-cf-id",  
        "x-amz-storage-class",  
        "access-control-expose-headers"  
    ],  
    "MaxAgeSeconds": 3000  
}  
]
```

4. Wählen Sie Änderungen speichern, um das CORS zu aktualisieren.

Schritt 4: Fügen Sie Ihrer Transfer Family Family-Web-App einen Benutzer hinzu

Fügen Sie den Benutzer hinzu, den Sie zuvor in IAM Identity Center erstellt haben.

So weisen Sie Benutzer einer Transfer Family Family-Web-App zu

1. Navigieren Sie zu der Web-App, die Sie zuvor erstellt haben.
2. Wählen Sie Benutzer und Gruppen zuweisen aus.

webapp- Assign users and groups Clear customization Delete

Web app details Edit

Access endpoint [Info](#)
Share this with your users and add to your CORS policy.
<https://webapp-.transfer-webapp.us-east-2.on.aws>

Web app endpoint
<https://webapp-.webapp.us-east-2.on.aws>

Web app units [Info](#)
1

Identity provider
[AWS IAM Identity Center](#)

IAM role
-

Instance ARN
arn:aws:sso::instance/ssoins-

Users **Groups**

Users (2) Refresh Delete

After you assign users to your web app, set up user permissions to access your S3 data in [S3 Access Grants](#)

< 1 >

☐	Display name	User ID	Username
☐	-	-	-
☐	-	-	-

3. Um den Benutzer zuzuweisen, den Sie zuvor in IAM Identity Center erstellt haben, wählen Sie Vorhandene Benutzer und Gruppen zuweisen und dann Weiter aus.
 - a. Suchen Sie anhand des Anzeigenamens nach dem Benutzer. Beachten Sie, dass keine Benutzer angezeigt werden, bis Sie mit der Eingabe Ihrer Suchkriterien beginnen. Um etwas hinzuzufügen **Bob Stiles**, geben Sie Bob in das Suchfeld ein. Wenn Sie Ihren Benutzer nicht finden können, navigieren Sie zur IAM Identity Center-Managementkonsole, suchen Sie den Benutzer, kopieren Sie seinen Anzeigenamen und fügen Sie ihn hier ein.
 - b. Wählen Sie den **Bob Stiles** Benutzer aus und klicken Sie dann auf Zuweisen.

Schritt 5: Registrieren Sie einen Standort in Amazon S3 und erstellen Sie eine Zugriffsberechtigung

Nachdem Sie Ihrer Web-App einen Benutzer zugewiesen haben, müssen Sie einen Bucket registrieren und eine Zugriffsberechtigung für diesen Benutzer erstellen.

 Note

Sie müssen über eine S3 Access Grants-Instanz verfügen, bevor Sie fortfahren können. Einzelheiten finden Sie unter [Erstellen einer S3 Access Grants-Instanz](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Um einen Standort zu registrieren und eine Zugriffsberechtigung zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im linken Navigationsbereich Access Grants aus.
3. Wählen Sie Details anzeigen, um die Details für Ihre S3 Access Grants-Instanz anzuzeigen.
4. Wählen Sie den Tab Standorte und dann Standort registrieren aus.
5. Geben Sie die folgenden Informationen ein:
 - Suchen Sie für den Bereich nach einem Bucket oder geben Sie den Namen Ihres Buckets und optional ein Präfix ein. Beachten Sie, dass der Bereich mit der Zeichenfolge beginnt **s3://**.
 - Wählen Sie für die IAM-Rolle Create new role aus, damit Amazon S3 eine Rolle erstellt. Diese Rolle ermöglicht S3 Access Grants den Zugriff auf Ihren angegebenen Standortbereich.

Wählen Sie Standort registrieren, um fortzufahren.

6. Wählen Sie die Registerkarte „Zuschüsse“ und dann „Zuschuss erstellen“ und geben Sie die folgenden Informationen ein.
 - Wählen Sie unter Standort die Option Standorte durchsuchen und wählen Sie den Standort aus, den Sie im vorherigen Schritt registriert haben.
 - Geben Sie im Feld Subprefix ein, * um anzugeben, dass die Zugriffsgewährung für den gesamten Bucket gilt.
 - Wählen Sie für Berechtigungen die Option Lesen und Schreiben aus.
 - Wählen Sie als Grantee-Typ die Option Verzeichnisidentität aus IAM Identity Center aus.
 - Wählen Sie als Identitätstyp des Verzeichnisses die Option Benutzer aus.
 - Kopieren Sie in IAM Identity Center Benutzer/ID die Benutzer-ID für und fügen Sie sie ein. **Bob Stiles** Diese ID ist im Bereich Benutzer in Ihrer Transfer Family Family-Web-App verfügbar.
7. Wählen Sie „Zuschuss erstellen“.

Die Zugriffsberechtigung wird erstellt.

Schritt 6: Greifen Sie als Benutzer auf Ihre Transfer Family Family-Web-App zu

Jetzt navigieren wir zur URL der Web-App und melden uns als der Benutzer an, den wir zuvor zugewiesen haben.

Um sich bei der Transfer Family Family-Web-App anzumelden

1. Navigieren Sie zu Ihrer Web-App
2. Wählen Sie im Detailbereich der Web-App den Access-Endpunkt aus.

The screenshot displays the AWS IAM console interface for a web application. At the top, there are buttons for 'Assign users and groups', 'Clear customization', and 'Delete'. The main section is titled 'webapp-' and contains two panels. The left panel, 'Web app details', includes an 'Access endpoint' (https://webapp-.transfer-webapp.us-east-2.on.aws), 'Web app endpoint', and 'Web app units' (1). The right panel shows 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN'. Below these panels, there are tabs for 'Users' and 'Groups'. The 'Users' tab is active, showing a list of users. A red box highlights the user 'Bob Stiles' with the username 'bobstiles'.

webapp- Assign users and groups Clear customization Delete

Web app details Edit

Access endpoint Info
Share this with your users and add to your CORS policy.
<https://webapp-.transfer-webapp.us-east-2.on.aws>

Web app endpoint
<https://webapp-.transfer-webapp.us-east-2.on.aws>

Web app units Info
1

Identity provider
[AWS IAM Identity Center](#)

IAM role
[AWSTransferWebAppIdentityBearer-us-east-2](#)

Instance ARN
arn:aws:sso::instance/ssoins-

Users Groups

Users (1) Delete

After you assign users to your web app, set up user permissions to access your S3 data in [S3 Access Grants](#)

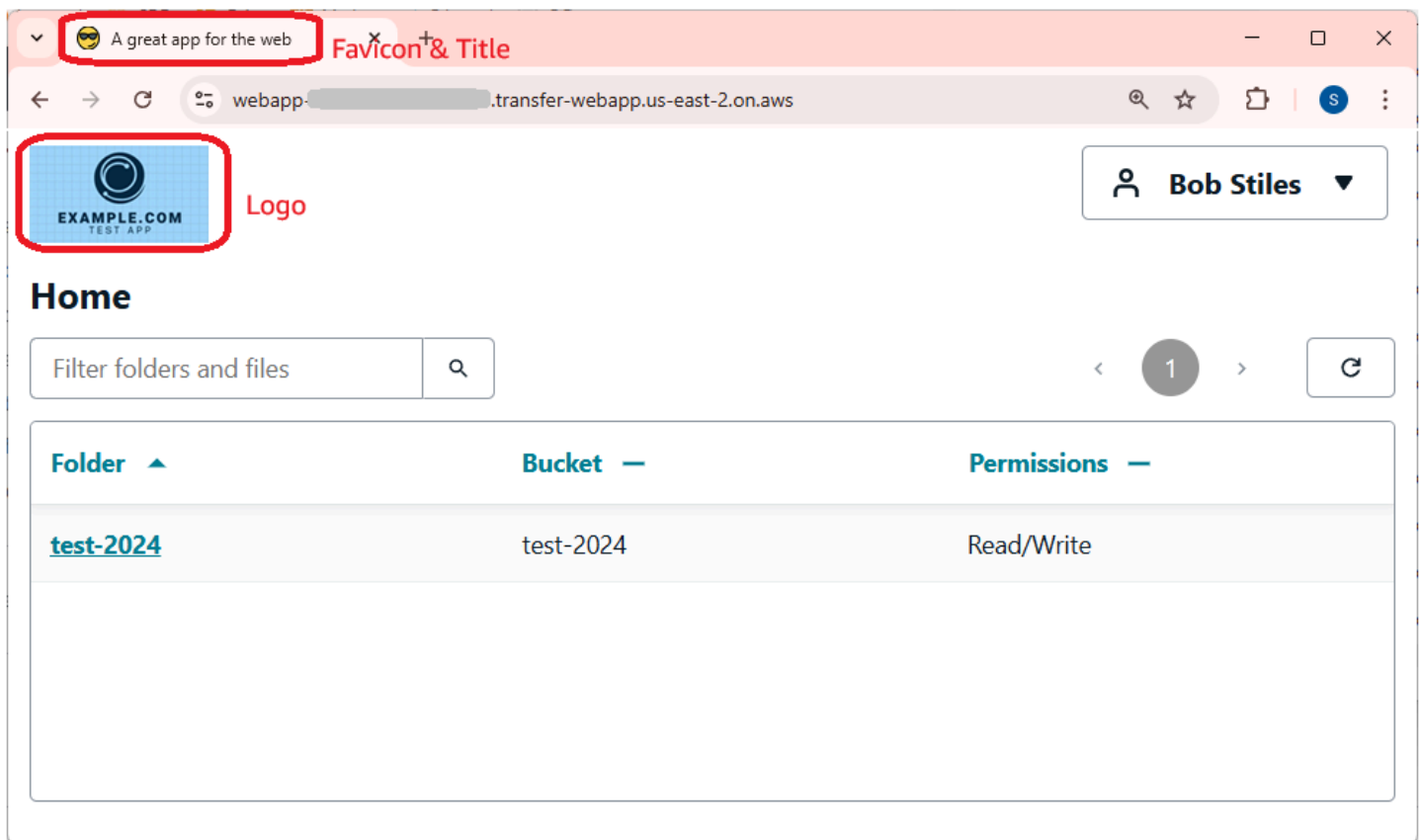
Find resources

☐	Display name	User ID	Username
☐	Bob Stiles		bobstiles

3. Geben Sie auf dem Anmeldebildschirm den Benutzer ein, den Sie erstellt haben **bobstiles**, und wählen Sie dann Weiter aus.
4. Geben Sie das Passwort ein, das das System diesem Benutzer bei der Erstellung zugewiesen hat, und wählen Sie Weiter aus.
5. Wenn Ihr Unternehmen eine Multi-Faktor-Authentifizierung (MFA) benötigt, müssen Sie diese jetzt einrichten. Wenn nicht, fahren Sie mit Schritt 6 fort.

- a. Es wird ein Bildschirm angezeigt, auf dem Sie Ihr MFA-Gerät registrieren können. Wählen Sie eine der verfügbaren Optionen und klicken Sie auf Weiter.
- b. Führen Sie die erforderlichen Schritte aus, um MFA für diesen Benutzer zu konfigurieren. Die Schritte hängen von der ausgewählten MFA-Option ab.
- c. Möglicherweise müssen Sie ein neues Passwort für Ihren Benutzer festlegen. Falls erforderlich, tun Sie dies jetzt. Das System verlangt möglicherweise auch, dass Sie sich mit den neuen MFA-Anmeldeinformationen, die Sie konfiguriert haben, erneut anmelden.

Ihrem Benutzer sollte ein Bildschirm ähnlich dem folgenden angezeigt werden. Beachten Sie, dass dieser Screenshot Anpassungen für das Favicon und das Logo enthält.



Nächste Schritte

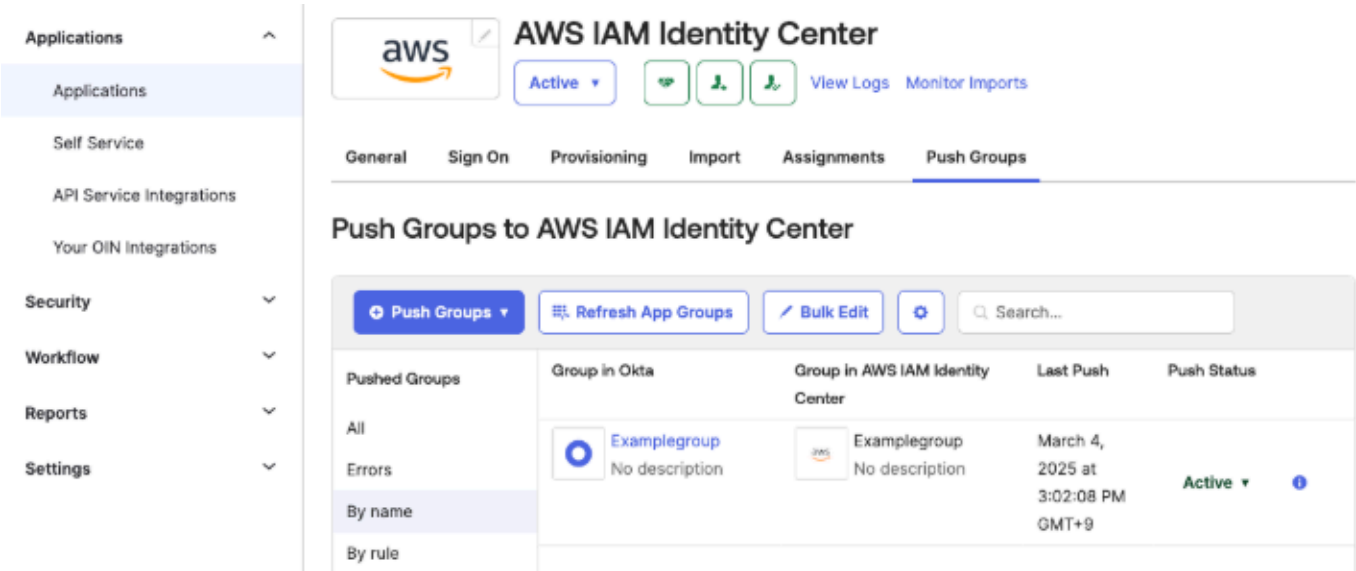
Sie haben erfolgreich eine grundlegende Transfer Family Family-Web-App mit standardmäßigem S3-Bucket-Zugriff eingerichtet. Wenn Sie eine detailliertere Kontrolle über Bucket-Berechtigungen benötigen, z. B. Benutzern das Herunterladen von einem Bucket und das Hochladen in einen

anderen ermöglichen möchten, finden Sie weitere Informationen unter [Tutorial: AWS Transfer Family Web-App mit selektivem Multi-Bucket-Zugriff einrichten](#).

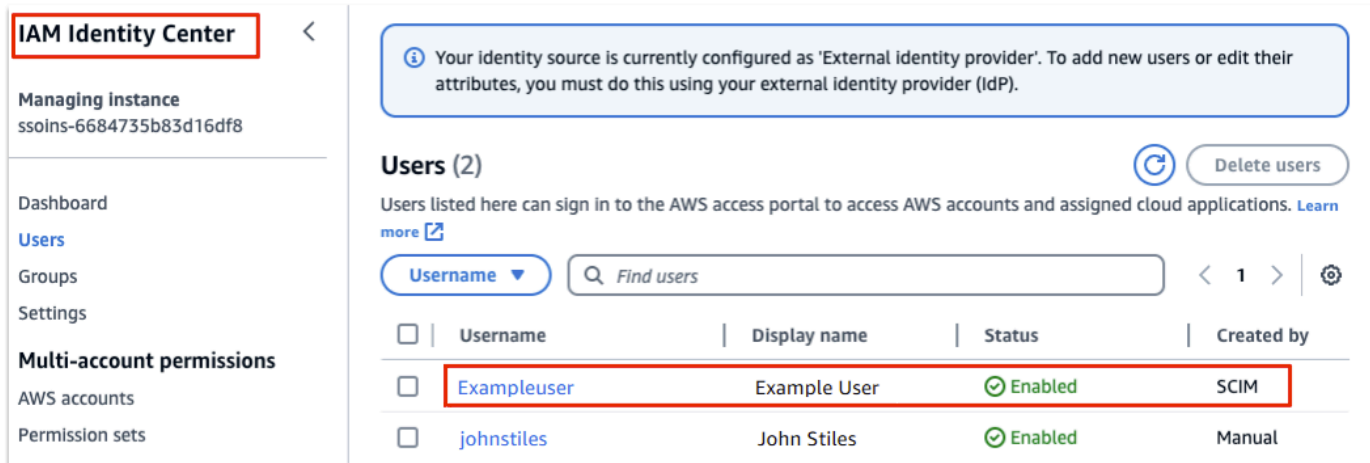
Integrieren Sie Okta als Ihren Identitätsanbieter für Web-Apps

Sie können einen externen Identitätsanbieter in die Transfer Family Family-Web-Apps integrieren. In diesem Abschnitt wird beschrieben, wie Sie Okta als Ihren Identitätsanbieter einrichten.

- Erstellen Sie in Okta einen Benutzer, eine Gruppe und eine Anwendung. Einzelheiten dazu finden Sie unter [Konfiguration von SAML und SCIM mit Okta und IAM Identity Center](#).



- Connect Okta und importieren Sie Benutzer und Gruppe von Okta nach. AWS IAM Identity Center Folgen Sie den Schritten 1—4 [unter SAML und SCIM mit Okta und IAM Identity Center konfigurieren](#).



IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.

Groups (2)

With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)

Find groups by group name

< 1 >

	Group name	Users	Description	Created by
☐	Examplegroup	1 user	-	SCIM
☐	dev	1 user	-	Manual

3. Vergewissern Sie sich, dass die Identitätsquelle in IAM Identity Center SAML 2.0 ist.

Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

Instance name - [Edit](#)

Region
US East (Ohio) | us-east-2

Instance ID
ssoins-

Date created
Thursday, November 14, 2024 at 4:11:19 PM EST

Organization ID
AWS Organizations not enabled

Instance ARN
[arn:aws:sso:::instance/ssoins-](#)

Identity source

Authentication

Management

Tags

Identity source

Choose the directory where you want to manage your users and groups. [Learn More](#)

Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
SCIM

AWS access portal URL
[https://.awsapps.com/start](#)

Identity store ID
d-

Issuer URL
[https://identitycenter.amazonaws.com/ssoins-](#)

Actions

Integrieren Sie Okta als Ihren Identitätsanbieter für Web-Apps

108

4. Weisen Sie Ihren Benutzer und Ihre Gruppe zu, wie unter beschrieben. [Schritt 4: Fügen Sie Ihrer Transfer Family Family-Web-App einen Benutzer hinzu](#)
5. Um zu vermeiden, dass Ihre Benutzer MFA verwenden müssen, wenn sie sich bei Ihrer Web-App anmelden, führen Sie die folgenden Schritte in Okta durch.
 - a. Rufen Sie in der Okta-Administrationskonsole [Anwendungen] — [Anwendungen] auf und wählen Sie die Anwendung aus. AWS IAM Identity Center
 - b. Wählen Sie auf der Registerkarte Anmelden die Option [Benutzerauthentifizierung] — Bearbeiten aus.
 - c. Wählen Sie Nur Passwort aus.

Nachdem Sie alle anderen Schritte für das Tutorial ausgeführt haben, sollte Ihr Benutzer in der Lage sein, auf Ihre Transfer Family Family-Web-App zuzugreifen, indem er in einem Webbrowser zum Zugriffsendpunkt der Web-App navigiert.

Tutorial: AWS Transfer Family Web-App mit selektivem Multi-Bucket-Zugriff einrichten

Dieses Tutorial führt Sie durch die Konfiguration einer Transfer Family Family-Web-App mit bestimmten Amazon S3 S3-Bucket-Berechtigungen für einen einzelnen Benutzer. Sie erfahren, wie Sie eine Lösung einrichten, mit der Benutzer aus einem Bucket herunterladen und in einen anderen hochladen können, ohne dabei die Sicherheit zu gefährden. Dies ist ein Tutorial für Fortgeschrittene, das auf den im Basis-Tutorial behandelten Konzepten aufbaut. Wenn Sie mit AWS Transfer Family Web-Apps noch nicht vertraut sind, sollten Sie mit beginnen [Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#).

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, brauchen Sie Folgendes:

- IAM Identity Center ist in derselben Region wie Ihre AWS Transfer Family Web-App konfiguriert. Beachten Sie, dass nur eine Instanz von IAM Identity Center pro AWS Konto für alle Regionen AWS zulässig ist.
- Mindestens ein Benutzer ist in IAM Identity Center konfiguriert.
- Zwei S3-Buckets: einer für Downloads und einer für Uploads.

 Note

Dieses Tutorial hat viele Voraussetzungen mit dem grundlegenden Web-App-Tutorial gemeinsam. Weitere Informationen zum Einrichten von IAM Identity Center und zum Erstellen von Benutzern finden Sie unter [Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#).

Schritt 1: Erstellen Sie eine Transfer Family Family-Web-App

So erstellen Sie eine Transfer Family Family-Web-App

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Web-Apps aus.
3. Wählen Sie Web-App erstellen aus.

Beachten Sie beim Authentifizierungszugriff, dass der Dienst die AWS IAM Identity Center Instanz, die Sie als Voraussetzung eingerichtet haben, automatisch findet.

4. Wählen Sie im Bereich Berechtigungstyp die Option Neue Servicerolle erstellen und verwenden aus. Der Dienst erstellt die Rolle des Identitätsträgers für Sie. Eine Identitätsträgerrolle umfasst die Identität eines authentifizierten Benutzers in seinen Sitzungen.
5. Akzeptieren Sie im Bereich Web-App-Einheiten den Standardwert 1, oder passen Sie ihn bei Bedarf auf einen höheren Wert an.
6. Fügen Sie ein Tag hinzu, um Ihre Web-Apps zu organisieren. Geben Sie für das Tutorial Name für den Schlüssel und Tutorial web app als Wert ein.

 Tip

Sie können den Namen der Web-App direkt auf der Listenseite der Web-Apps bearbeiten, nachdem Sie sie erstellt haben.

7. Wählen Sie Weiter, um die Seite Web-App entwerfen zu öffnen. Geben Sie auf diesem Bildschirm die folgenden Informationen ein.

Sie können optional einen Titel für Ihre Web-App angeben. Sie können auch Bilddateien für Ihr Logo und Favicon hochladen.

- Passen Sie für den Seitentitel den Titel für den Browser-Tab an, den Ihre Benutzer sehen, wenn sie eine Verbindung zur Web-App herstellen. Wenn Sie nichts für den Seitentitel eingeben, wird standardmäßig Transfer Web App verwendet.
- Laden Sie für das Logo eine Bilddatei hoch. Die maximale Dateigröße für Ihr Logobild beträgt 50 KB.
- Laden Sie für das Favicon eine Bilddatei hoch. Die maximale Dateigröße für Ihr Favicon beträgt 20 KB.

8. Wählen Sie Weiter und anschließend Web-App erstellen.

Schritt 2: Konfigurieren Sie IAM-Rollen für den S3-Zugriff

Sie müssen zwei IAM-Rollen erstellen: eine mit reinem Download-Zugriff auf den ersten Bucket und eine weitere mit reinem Upload-Zugriff auf den zweiten Bucket.

Vertrauensrichtlinie für beide Rollen

Verwenden Sie die folgende Vertrauensrichtlinie für beide IAM-Rollen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessGrantsTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:SetContext"
      ]
    }
  ]
}
```

IAM-Richtlinie für den Download-Bucket

Erstellen Sie eine IAM-Rolle mit der folgenden Richtlinie für den schreibgeschützten Zugriff auf Ihren Download-Bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket1"
      ]
    }
  ]
}
```

Important

Ersetzen Sie `amzn-s3-demo-bucket1` durch den tatsächlichen Namen Ihres Download-Buckets.

IAM-Richtlinie für den Upload-Bucket

Erstellen Sie eine weitere IAM-Rolle mit der folgenden Richtlinie für den Schreibzugriff auf Ihren Upload-Bucket:

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:AbortMultipartUpload",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket2/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2"
    ]
  }
]
```

Important

Ersetzen Sie amzn-s3-demo-bucket2 durch den tatsächlichen Namen Ihres Upload-Buckets.

Schritt 3: Richten Sie S3 Access Grants ein

1. Öffnen Sie die S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im Navigationsbereich Access Grants aus.
3. Klicken Sie auf S3 Access Grants-Instanz erstellen.
4. Wählen Sie die Option IAM Identity Center-Instanz hinzufügen und geben Sie den ARN der Identity Center-Instanz ein.
5. Klicken Sie auf Weiter und dann auf Abbrechen, um die Erstellung der S3 Access Grants-Instanz abzuschließen, ohne mit weiteren Schritten fortzufahren.

In diesem Schritt wird die S3 Access Grants-Instanz erstellt. Sie registrieren jetzt Standorte und erstellen Zugriffsberechtigungen.

Schritt 4: Registrieren Sie S3-Bucket-Standorte

Registrieren Sie beide S3-Buckets als Standorte mit S3 Access Grants:

1. Navigieren Sie in der S3 Access Grants-Konsole zu Standorte und klicken Sie auf Standort registrieren.
2. Wählen Sie unter Standortbereich den spezifischen S3-Bucket für Downloads aus (amzn-s3-demo-bucket1).
3. Wenn Sie aufgefordert werden, eine IAM-Rolle auszuwählen, wählen Sie die Download-IAM-Rolle aus, die Sie zuvor erstellt haben.
4. Schließen Sie den Registrierungsprozess ab.
5. Wiederholen Sie den Vorgang, um den Upload-Bucket (amzn-s3-demo-bucket2) zu registrieren, und wählen Sie die Upload-IAM-Rolle aus, wenn Sie dazu aufgefordert werden.

Schritt 5: Zugriffsberechtigungen erstellen

Erstellen Sie zwei Zuschüsse, eine für jeden registrierten Standort:

1. Navigieren Sie in der S3 Access Grants-Konsole zu Grants und klicken Sie auf Create Grants.
2. Klicken Sie unter Standort auf Speicherort durchsuchen und wählen Sie den Download-Bucket-Speicherort aus (amzn-s3-demo-bucket1).
3. Geben Sie im Feld Unterpräfix (optional) ein, ob Sie Zugriff auf den gesamten Bucket gewähren möchten, oder geben Sie * einen Pfad an, um den Zugriff auf ein bestimmtes Präfix zu beschränken. `folder1/folder2/*`

Mit dieser * Option wird der Geltungsbereich der Gewährung auf festgelegt `3://bucket-name/*`, sodass der Zugriff auf den gesamten Bucket möglich ist. Um den Zugriff nur auf ein bestimmtes Präfix zu ermöglichen, geben Sie einen Pfad wie ein `folder1/folder2/*`, wodurch der Geltungsbereich der Gewährung auf festgelegt wird `3://bucket-name/folder1/folder2/*`.

4. Wählen Sie unter Berechtigungen und Zugriff die Option Lesen für den Download-Bucket aus.
5. Wählen Sie im Feld Grantee-Typ die Option Verzeichnisidentität aus IAM Identity Center aus.

6. Wählen Sie als IAM-Prinzipaltyp die Option Benutzer aus und geben Sie die Benutzer-ID Ihres IAM Identity Center-Benutzers ein.
7. Schließen Sie den Prozess zur Erstellung des Zuschusses ab.
8. Wiederholen Sie den Vorgang, um einen Grant für den Upload-Bucket (amzn-s3-demo-bucket2) zu erstellen, wählen Sie jedoch die Berechtigungen aus. Read-write

Schritt 6: Konfigurieren Sie die CORS-Richtlinie für S3-Buckets

Konfigurieren Sie eine CORS-Richtlinie für beide S3-Buckets, um den Zugriff über Folgendes zu ermöglichen: AWS Transfer Family WebApp

1. Öffnen Sie die S3-Konsole und navigieren Sie zu Ihrem Download-Bucket (amzn-s3-demo-bucket1).
2. Wählen Sie den Tab Berechtigungen aus.
3. Scrollen Sie nach unten zum Abschnitt Cross-origin Resource Sharing (CORS) und klicken Sie auf Bearbeiten.
4. Fügen Sie die folgende CORS-Konfiguration hinzu und *WebAppEndpoint* ersetzen Sie sie durch Ihre tatsächliche WebApp Endpunkt-URL:

Sie finden die URL Ihres Web-App-Endpunkts in der AWS Transfer Family Konsole unter WebApps. Sie wird ähnlich wie `https://webapp-*****.transfer-webapp.us-west-2.on.aws` aussehen.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
  },
]
```

```
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

5. Klicken Sie auf Änderungen speichern.
6. Wiederholen Sie den Vorgang für Ihren Upload-Bucket (amzn-s3-demo-bucket2).

Schritt 7: Testen Sie die Konfiguration

1. Öffnen Sie die URL Ihrer AWS Transfer Family Web-App. Sie finden diese URL in der AWS Transfer Family Konsole unter dem WebApps Feld Zugriffsendpunkt.
2. Melden Sie sich mit den IAM Identity Center-Benutzeranmeldedaten an, die Sie mit Zugriffsberechtigungen konfiguriert haben.
3. Nach der Anmeldung sollten Sie beide S3-Standorte auf der Startseite sehen.
4. Navigieren Sie zum Download-Bucket (amzn-s3-demo-bucket1) und stellen Sie sicher, dass Sie Dateien herunterladen, aber nicht hochladen können.
5. Navigieren Sie zum Upload-Bucket (amzn-s3-demo-bucket2) und vergewissern Sie sich, dass Sie Dateien hochladen können.

Schlussfolgerung

Sie haben erfolgreich den selektiven S3-Bucket-Zugriff für einen einzelnen Benutzer konfiguriert AWS Transfer Family WebApp . Dieses Setup ermöglicht es dem Benutzer, Daten von einem Bucket herunterzuladen und in einen anderen hochzuladen, während gleichzeitig die Sicherheit durch IAM-Rollen und S3-Zugriffsberechtigungen gewahrt bleibt.

Dieser Ansatz kann auf mehrere Benutzer ausgedehnt werden, indem zusätzliche Grants in S3 Access Grants für jeden Benutzer erstellt werden, was eine detaillierte Steuerung der Bucket-Zugriffsberechtigungen ermöglicht. Informationen zur grundlegenden Einrichtung der Web-App finden Sie unter [Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#).

Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts

Dieses Thema enthält Einzelheiten zum Erstellen und Verwenden von AWS Transfer Family Serverendpunkten, die eines oder mehrere der Protokolle SFTP, FTPS und FTP verwenden.

Themen

- [Optionen für den Identitätsanbieter](#)
- [AWS Transfer Family Endpunkt-Typmatrix](#)
- [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#)
- [Überlegungen zum FTP- und FTPS-Network Load Balancer](#)
- [Übertragung von Dateien über einen Serverendpunkt mit einem Client](#)
- [Benutzer für Serverendpunkte verwalten](#)
- [Verwendung logischer Verzeichnisse zur Vereinfachung Ihrer Transfer Family Family-Verzeichnisstrukturen](#)
- [Greifen Sie mit Transfer Family auf Ihre FSx for NetApp ONTAP-Dateisysteme zu](#)

Optionen für den Identitätsanbieter

AWS Transfer Family bietet verschiedene Methoden zur Authentifizierung und Verwaltung von Benutzern. In der folgenden Tabelle werden die verfügbaren Identitätsanbieter verglichen, die Sie mit Transfer Family verwenden können.

Action	AWS Transfer Family Dienst verwaltet	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Unterstützte Protokolle	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based authentication	Ja	Nein	Ja	Ja

Action	AWS Transfer Family Dienst verwaltet	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Passwortauthentifizierung	Nein	Ja	Ja	Ja
AWS Identity and Access Management (IAM) und POSIX	Ja	Ja	Ja	Ja
Logisches Home-Verzeichnis	Ja	Ja	Ja	Ja
Parametrisierter Zugriff (benutzer namenbasiert)	Ja	Ja	Ja	Ja
Ad-hoc-Zugriffsstruktur	Ja	Nein	Ja	Ja
AWS WAF	Nein	Nein	Ja	Nein

Hinweise:

- IAM wird verwendet, um den Zugriff auf den Amazon S3 S3-Backing-Speicher zu kontrollieren, und POSIX wird für Amazon EFS verwendet.
- Ad-Hoc bezieht sich auf die Möglichkeit, das Benutzerprofil zur Laufzeit zu senden. Sie können beispielsweise Benutzer in ihren Home-Verzeichnissen landen lassen, indem Sie den Benutzernamen als Variable übergeben.
- Einzelheiten dazu finden AWS WAF Sie unter [Fügen Sie eine Firewall für Webanwendungen hinzu](#).
- In einem Blogbeitrag wird die Verwendung einer in Microsoft Entra ID (ehemals Azure AD) integrierten Lambda-Funktion als Identitätsanbieter für Transfer Family beschrieben. Einzelheiten

finden Sie unter [Authentifizierung AWS Transfer Family mit Azure Active Directory](#) und. AWS Lambda

- Wir bieten verschiedene CloudFormation Vorlagen, mit denen Sie schnell einen Transfer Family Family-Server bereitstellen können, der einen benutzerdefinierten Identitätsanbieter verwendet. Details hierzu finden Sie unter [Lambda-Funktionsvorlagen](#).

Mit den folgenden Verfahren können Sie einen SFTP-enabled Server, FTPS-enabled Server, FTP-enabled Server oder AS2-enabled Server erstellen.

Nächster Schritt

- [Erstellen Sie einen SFTP-enabled Server](#)
- [Einen FTPS-enabled Server erstellen](#)
- [Erstellen Sie einen FTP-enabled Server](#)
- [AS2 konfigurieren](#)

AWS Transfer Family Endpunkt-Typmatrix

Wenn Sie einen Transfer Family Family-Server erstellen, wählen Sie den zu verwendenden Endpunkttyp aus. In der folgenden Tabelle werden die Merkmale der einzelnen Endpunkttypen beschrieben.

Matrix der Endpunkttypen

Merkmal	Öffentlich	VPC - Internet	VPC — Intern	VPC_Endpoint (veraltet)
Unterstützte Protokolle	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
Access	Über das Internet. Für diesen Endpunkttyp ist keine spezielle Konfiguration	Über das Internet und innerhalb von VPC und VPC-connected Umgebungen, z. B. einem lokalen	Innerhalb von VPC und VPC-connected Umgebungen, z. B. einem lokalen Rechenzentrum über Direct	Innerhalb von VPC und VPC-connected Umgebungen, z. B. einem lokalen Rechenzentrum über Direct

Merkmal	Öffentlich	VPC - Internet	VPC — Intern	VPC_Endpoint (veraltet)
	in Ihrer VPC erforderlich.	Rechenzentrum über Direct Connect oder VPN.	Connect oder VPN.	Connect oder VPN.
Statische IP-Adresse	Sie können keine statische IP-Adresse anhängen. AWS stellt IP-Adressen bereit, die sich ändern können.	Sie können Elastic IP-Adressen an den Endpunkt anhängen. Dies können AWS eigene IP-Adressen oder Ihre eigenen IP-Adressen sein (Bringen Sie Ihre eigenen IP-Adressen mit). Elastische IP-Adressen, die an den Endpunkt angehängt sind, ändern sich nicht. Private IP-Adressen, die an den Server angeschlossen sind, ändern sich ebenfalls nicht.	Private IP-Adressen, die an den Endpunkt angeschlossen sind, ändern sich nicht.	Private IP-Adressen, die an den Endpunkt angeschlossen sind, ändern sich nicht.

Merkmal	Öffentlich	VPC - Internet	VPC — Intern	VPC_Endpoint (veraltet)
Liste der zugelassenen Quell-IP-Adressen	Dieser Endpunkttyp unterstützt keine Zulassungslisten nach Quell-IP-Adressen. Der Endpunkt ist öffentlich zugänglich und überwacht den Datenverkehr über Port 22.  Note Für VPC-hosted Endgeräte können Server der SFTP Transfer Family über Port 22 (Standard), 2222, 2223 oder 22000	Um den Zugriff über die Quell-IP-Adresse zu ermöglichen, können Sie Sicherheitsgruppen verwenden, die an die Serverendpunkte angehängt sind, und Netzwerk-ACLs, die an das Subnetz angeschlossen sind, in dem sich der Endpunkt befindet.	Um den Zugriff über die Quell-IP-Adresse zu ermöglichen, können Sie Sicherheitsgruppen verwenden, die an die Serverendpunkte angehängt sind, und Netzwerkzugriffskontrolllisten (Netzwerk-ACLs), die an das Subnetz angehängt sind, in dem sich der Endpunkt befindet.	Um den Zugriff über die Quell-IP-Adresse zu ermöglichen, können Sie Sicherheitsgruppen verwenden, die an die Serverendpunkte angehängt sind, und Netzwerk-ACLs, die an das Subnetz angeschlossen sind, in dem sich der Endpunkt befindet.

Merkmal	Öffentlich	VPC - Internet	VPC — Intern	VPC_Endpoint (veraltet)
	betrieben werden.			
Liste der zugelassenen Client-Firewalls	Sie müssen den DNS-Namen des Servers zulassen. Da sich IP-Adressen ändern können, sollten Sie es vermeiden, IP-Adressen für Ihre Client-Firewall-Zulassungsliste zu verwenden.	Sie können den DNS-Namen des Servers oder die mit dem Server verbundenen Elastic IP-Adressen zulassen.	Sie können die privaten IP-Adressen oder den DNS-Namen der Endpoints zulassen.	Sie können die privaten IP-Adressen oder den DNS-Namen der Endpunkte zulassen.
IP-Adresstyp	IPv4 (Standard) oder Dual-Stack (IPv4 und IPv6)	Nur IPv4 (Dual-Stack wird nicht unterstützt)	IPv4 (Standard) oder Dual-Stack (IPv4 und IPv6)	Nur IPv4 (Dual-Stack wird nicht unterstützt)

Note

Der VPC_ENDPOINT Endpunkttyp ist jetzt veraltet und kann nicht zum Erstellen neuer Server verwendet werden. Verwenden Sie statt dessen den VPC-Endpunkttyp (EndpointType=VPC), den Sie entweder als Intern - oder Internetanschluss verwenden können, wie in der vorherigen Tabelle beschrieben. EndpointType=VPC_ENDPOINT

- Einzelheiten zu dieser veralteten Version finden Sie unter: [Einstellung der Verwendung von VPC_ENDPOINT](#)
- Informationen zur Verwaltung von VPC-Endpunktberechtigungen finden Sie unter [Beschränkung des VPC-Endpunktzugriffs für Transfer Family Family-Server](#).

Ziehen Sie die folgenden Optionen in Betracht, um die Sicherheit Ihres AWS Transfer Family Servers zu verbessern:

- Verwenden Sie einen VPC-Endpunkt mit internem Zugriff, sodass der Server nur für Clients innerhalb Ihrer VPC oder VPC-connected Umgebungen wie ein lokales Rechenzentrum über Direct Connect oder VPN zugänglich ist.
- Verwenden Sie einen VPC-Endpunkt mit Internetzugriff, um Clients den Zugriff auf den Endpunkt über das Internet zu ermöglichen und Ihren Server zu schützen. Ändern Sie anschließend die Sicherheitsgruppen der VPC so, dass nur Datenverkehr von bestimmten IP-Adressen zugelassen wird, auf denen die Clients Ihrer Benutzer gehostet werden.
- Wenn Sie eine kennwortbasierte Authentifizierung benötigen und einen benutzerdefinierten Identitätsanbieter für Ihren Server verwenden, ist es eine bewährte Methode, dass Ihre Passwortrichtlinie verhindert, dass Benutzer schwache Passwörter erstellen, und dass die Anzahl fehlgeschlagener Anmeldeversuche begrenzt wird.
- AWS Transfer Family ist ein verwalteter Dienst und bietet daher keinen Shell-Zugriff. Sie können nicht direkt auf den zugrunde liegenden SFTP-Server zugreifen, um betriebssystemeigene Befehle auf Transfer Family Family-Servern auszuführen.
- Verwenden Sie einen Network Load Balancer vor einem VPC-Endpunkt mit internem Zugriff. Ändern Sie den Listener-Port auf dem Load Balancer von Port 22 auf einen anderen Port. Dadurch kann das Risiko, dass Portscanner und Bots Ihren Server untersuchen, verringern, aber nicht ausschließen, da Port 22 am häufigsten zum Scannen verwendet wird. Einzelheiten finden Sie im Blogbeitrag [Network Load Balancers now support Security Groups](#).

 Note

Wenn Sie einen Network Load Balancer verwenden, zeigen die AWS Transfer Family CloudWatch Protokolle die IP-Adresse für den NLB und nicht die tatsächliche Client-IP-Adresse.

Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts

Mithilfe des Dienstes können Sie einen Dateiübertragungsserver erstellen. AWS Transfer Family Die folgenden Dateiübertragungsprotokolle sind verfügbar:

- Secure Shell (SSH) File Transfer Protocol (SFTP) — Dateiübertragung über SSH. Details hierzu finden Sie unter [the section called “Erstellen Sie einen SFTP-enabled Server”](#).

 Note

Wir bieten ein AWS CDK Beispiel für die Erstellung eines SFTP Transfer Family Family-Servers. Das Beispiel verwendet TypeScript und ist GitHub [hier verfügbar](#).

- File Transfer Protocol Secure (FTPS) — Dateiübertragung mit TLS-Verschlüsselung. Details hierzu finden Sie unter [the section called “Erstellen Sie einen FTPS-enabled Server”](#).
- File Transfer Protocol (FTP) — Unverschlüsselte Dateiübertragung. Details hierzu finden Sie unter [the section called “Erstellen Sie einen FTP-enabled Server”](#).
- Applicability Statement 2 (AS2) — Dateiübertragung für den Transport strukturierter Business-to-Business-Daten. Details hierzu finden Sie unter [the section called “AS2 konfigurieren”](#). Für AS2 können Sie schnell einen Stack zu Demonstrationszwecken erstellen CloudFormation . Dieses Verfahren wird unter beschrieben. [Verwenden Sie eine Vorlage, um einen Demo-Stack der Transfer Family AS2 zu erstellen](#)

Sie können einen Server mit mehreren Protokollen erstellen.

 Note

Wenn Sie mehrere Protokolle für denselben Serverendpunkt aktiviert haben und den Zugriff über mehrere Protokolle mit demselben Benutzernamen ermöglichen möchten, können Sie dies tun, sofern die für das Protokoll spezifischen Anmeldeinformationen in Ihrem Identitätsanbieter eingerichtet wurden. Für FTP empfehlen wir, separate Anmeldeinformationen von SFTP und FTPS zu verwenden. Dies liegt daran, dass FTP im Gegensatz zu SFTP und FTPS Anmeldeinformationen im Klartext überträgt. Durch die Isolierung von FTP-Anmeldeinformationen von SFTP oder FTPS bleiben Ihre Workloads, die SFTP oder FTPS verwenden, sicher, wenn FTP-Anmeldeinformationen geteilt oder offengelegt werden.

Wenn Sie einen Server erstellen, wählen Sie einen bestimmten Server aus, AWS-Region um die Dateioptionsanforderungen von Benutzern auszuführen, die diesem Server zugewiesen sind. Sie weisen dem Server nicht nur ein oder mehrere Protokolle zu, sondern weisen auch einen der folgenden Identitätsanbieterstypen zu:

- Dienst, der mithilfe von SSH-Schlüsseln verwaltet wird. Details hierzu finden Sie unter [Arbeiten mit Benutzern, die vom Dienst verwaltet werden](#).
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Mit dieser Methode können Sie Ihre Microsoft Active Directory-Gruppen integrieren, um Zugriff auf Ihre Transfer Family Family-Server zu gewähren. Details hierzu finden Sie unter [Verwenden des AWS Directory Service für Microsoft Active Directory](#).
- Ein benutzerdefinierter Identitätsanbieter. Transfer Family bietet mehrere Optionen für die Verwendung eines benutzerdefinierten Identitätsanbieters, wie im [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#) Thema beschrieben.

Sie weisen dem Server auch einen Endpunkttyp (öffentlich zugänglich oder von VPC gehostet) und einen Hostnamen zu, indem Sie den Standard-Serverendpunkt oder einen benutzerdefinierten Hostnamen verwenden, indem Sie den Amazon Route 53-Service oder einen Domain Name System (DNS) -Service Ihrer Wahl verwenden. Ein Server-Hostname muss in dem Ort, an AWS-Region dem er erstellt wurde, eindeutig sein.

Darüber hinaus können Sie eine CloudWatch Amazon-Protokollierungsrolle zuweisen, um Ereignisse in Ihre CloudWatch Protokolle zu übertragen, eine Sicherheitsrichtlinie wählen, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind, und dem Server Metadaten in Form von Tags hinzufügen, die Schlüssel-Wert-Paare sind.

 Important

Es fallen Kosten für instanziierte Server und für die Datenübertragung an. Preisinformationen und Informationen zur Schätzung der Kosten für die Nutzung von Transfer Family finden Sie unter [AWS Transfer Family Preise](#). AWS Pricing Calculator

Erstellen Sie einen SFTP-enabled Server

Das Secure Shell (SSH) File Transfer Protocol (SFTP) ist ein Netzwerkprotokoll, das für die sichere Übertragung von Daten über das Internet verwendet wird. Das Protokoll unterstützt die volle Sicherheits- und Authentifizierungsfunktionalität von SSH. Es wird häufig für den Austausch von Daten, einschließlich sensibler Informationen, zwischen Geschäftspartnern in einer Vielzahl von Branchen wie Finanzdienstleistungen, Gesundheitswesen, Einzelhandel und Werbung verwendet.

Beachten Sie Folgendes

- SFTP-Server für Transfer Family arbeiten über Port 22. Für VPC-hosted Endgeräte können Server der SFTP Transfer Family auch über Port 2222, 2223 oder 22000 betrieben werden. Details hierzu finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).
- Öffentliche Endpunkte können den Verkehr nicht über Sicherheitsgruppen einschränken. Um Sicherheitsgruppen mit Ihrem Transfer Family Family-Server zu verwenden, müssen Sie den Endpunkt Ihres Servers in einer Virtual Private Cloud (VPC) hosten, wie unter beschrieben. [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#)

Informationen finden Sie auch unter:

- Wir bieten ein AWS CDK Beispiel für die Erstellung eines SFTP Transfer Family Family-Servers. Das Beispiel verwendet TypeScript und ist GitHub [hier verfügbar](#).
- Eine exemplarische Vorgehensweise zur Bereitstellung eines Transfer Family Family-Servers in einer VPC finden Sie unter [Verwenden Sie die IP-Zulassungsliste, um Ihre AWS Transfer Family Server zu sichern](#).

So erstellen Sie einen Server SFTP-enabled

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie im Navigationsbereich Server und anschließend Server erstellen aus.
2. Wählen Sie unter Protokolle auswählen die Option SFTP und dann Weiter aus.
3. Wählen Sie unter Wählen Sie einen Identitätsanbieter aus den Identitätsanbieter aus, den Sie für die Verwaltung des Benutzerzugriffs verwenden möchten. Ihnen stehen folgende Optionen zur Verfügung:
 - Service verwaltet — Sie speichern Benutzeridentitäten und Schlüssel in AWS Transfer Family.
 - AWS Directory Service for Microsoft Active Directory— Sie stellen ein Directory Service Verzeichnis für den Zugriff auf den Endpunkt bereit. Auf diese Weise können Sie die in Ihrem Active Directory gespeicherten Anmeldeinformationen verwenden, um Ihre Benutzer zu authentifizieren. Weitere Informationen zur Arbeit mit AWS Managed Microsoft AD Identitätsanbietern finden Sie unter [Verwenden des AWS Directory Service für Microsoft Active Directory](#).

 Note

- Cross-Account und Geteilte Verzeichnisse werden nicht unterstützt für AWS Managed Microsoft AD.
- Um einen Server mit Directory Service als Identitätsanbieter einzurichten, müssen Sie einige Directory Service Berechtigungen hinzufügen. Details hierzu finden Sie unter [Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory](#).

- Benutzerdefinierter Identitätsanbieter — Wählen Sie eine der folgenden Optionen:
 - Verwenden Sie AWS Lambda , um Ihren Identitätsanbieter zu verbinden — Sie können einen vorhandenen Identitätsanbieter verwenden, der von einer Lambda-Funktion unterstützt wird. Sie geben den Namen der Lambda-Funktion an. Weitere Informationen finden Sie unter [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet](#).
 - Verwenden Sie Amazon API Gateway, um Ihren Identitätsanbieter zu verbinden — Sie können eine API Gateway Gateway-Methode erstellen, die von einer Lambda-Funktion unterstützt wird, um sie als Identitätsanbieter zu verwenden. Sie geben eine Amazon API Gateway Gateway-URL und eine Aufrufrolle an. Weitere Informationen finden Sie unter [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☒ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ **Password OR public key**

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel Previous Next

4. Wählen Sie Weiter aus.
5. Gehen Sie unter Endpunkt auswählen wie folgt vor:
 - a. Wählen Sie als Endpunkttyp den Typ Öffentlich zugänglicher Endpunkt aus. Informationen zu einem VPC-gehosteten Endpunkt finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).
 - b. Wählen Sie als IP-Adresstyp IPv4 (Standard) aus Gründen der Abwärtskompatibilität oder Dual-stackum sowohl IPv4- als auch IPv6-Verbindungen zu Ihrem Endpunkt zu aktivieren.

 Note

Dual-stack Im Modus kann Ihr Transfer Family Family-Endpunkt sowohl mit IPv4- als auch mit IPv6-fähigen Clients kommunizieren. Auf diese Weise können Sie schrittweise von IPv4- zu IPv6-basierten Systemen wechseln, ohne alle auf einmal wechseln zu müssen.

- c. (Optional) Wählen Sie für Benutzerdefinierter Hostname die Option Keine aus.

Sie erhalten einen Server-Hostnamen, der von bereitgestellt wird.

AWS Transfer Family Der Server-Host-Name hat das Format

serverId.server.transfer.*regionId*.amazonaws.com.

Für einen benutzerdefinierten Hostnamen geben Sie einen benutzerdefinierten Alias für Ihren Serverendpunkt an. Weitere Informationen zum Arbeiten mit benutzerdefinierten Hostnamen finden Sie unter [Mit benutzerdefinierten Hostnamen arbeiten](#)

- d. (Optional) Aktivieren Sie für FIPS Enabled das Kontrollkästchen FIPS-fähiger Endpunkt, um sicherzustellen, dass der Endpunkt den Federal Information Processing Standards (FIPS) entspricht.

 Note

FIPS-enabled Endpunkte sind nur in nordamerikanischen Regionen verfügbar. AWS Informationen zu den verfügbaren Regionen finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Weitere Informationen zu FIPS finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

- e. Wählen Sie Weiter aus.

6. Wählen Sie auf der Seite Domain auswählen den AWS Speicherdienst aus, den Sie zum Speichern und Zugreifen auf Ihre Daten über das ausgewählte Protokoll verwenden möchten:

- Wählen Sie Amazon S3, um Ihre Dateien als Objekte über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.
- Wählen Sie Amazon EFS, um Ihre Dateien in Ihrem Amazon EFS-Dateisystem über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.

Wählen Sie Weiter aus.

7. Gehen Sie unter Zusätzliche Details konfigurieren wie folgt vor:

- a. Geben Sie für die Protokollierung eine bestehende Protokollgruppe an oder erstellen Sie eine neue (Standardoption). Wenn Sie eine bestehende Protokollgruppe wählen, müssen Sie eine auswählen, die mit Ihrer verknüpft ist AWS-Konto.

The screenshot shows the AWS Transfer Family console interface for creating a server. The breadcrumb trail at the top reads "Transfer Family > Servers > Create server". On the left, a sidebar lists six steps: "Step 1: Choose protocols", "Step 2: Choose an identity provider", "Step 3: Choose an endpoint", "Step 4: Choose a domain", "Step 5: Configure additional details" (which is highlighted), and "Step 6: Review and create". The main content area is titled "Configure additional details" and contains a "Logging" section. Under "Log group", it says "Choose the CloudWatch log group where your events will be delivered in a structured JSON format". There are two radio buttons: "Create a new log group" (unselected) and "Choose an existing log group" (selected). Below the radio buttons is a text input field containing "/aws/transfer/" followed by a dropdown arrow, a refresh button, and a "Create log group" button with an external link icon. Under "Logging role", it says "Choose the IAM role that will be used to deliver events to your CloudWatch logs". There are two radio buttons: "Create a new role" (unselected) and "Choose an existing role" (unselected). At the bottom, a blue information box states: "Logging role is only required when selecting a workflow in the Managed workflows section below."

Wenn Sie „Protokollgruppe erstellen“ wählen, wird in der CloudWatch Konsole (<https://console.aws.amazon.com/cloudwatch/>) die Seite „Protokollgruppe erstellen“ geöffnet. Einzelheiten finden Sie unter [Protokollgruppe erstellen in CloudWatch Logs](#).

- b. (Optional) Wählen Sie für verwaltete Workflows Workflow-IDs (und eine entsprechende Rolle) aus, die Transfer Family bei der Ausführung des Workflows annehmen soll. Sie können einen Workflow auswählen, der bei einem vollständigen Upload ausgeführt wird, und einen anderen, der bei einem teilweisen Upload ausgeführt werden soll. Weitere Informationen zur Verarbeitung Ihrer Dateien mithilfe verwalteter Workflows finden Sie unter [AWS Transfer Family verwaltete Workflows](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [redacted] ▼ [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [redacted] ▼ [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[redacted] ▼

- c. Wählen Sie unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind. Unsere neueste Sicherheitsrichtlinie ist die Standardeinstellung: Einzelheiten finden Sie unter: [Sicherheitsrichtlinien für Server AWS Transfer Family](#)
- d. (Optional) Geben Sie für Server Host Key einen privaten RSA-, ED25519- oder ECDSA-Schlüssel ein, der zur Identifizierung Ihres Servers verwendet wird, wenn Clients über SFTP eine Verbindung zu ihm herstellen. Sie können auch eine Beschreibung hinzufügen, um zwischen mehreren Hostschlüsseln zu unterscheiden.

Nachdem Sie Ihren Server erstellt haben, können Sie weitere Hostschlüssel hinzufügen. Mehrere Hostschlüssel sind nützlich, wenn Sie Schlüssel rotieren möchten oder wenn Sie verschiedene Schlüsseltypen verwenden möchten, z. B. einen RSA-Schlüssel und auch einen ECDSA-Schlüssel.

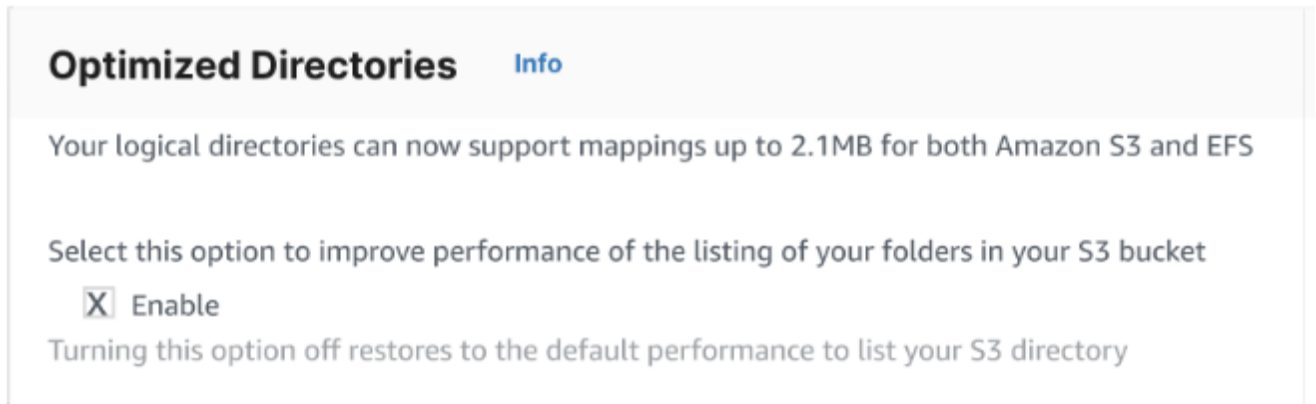
Note

Der Abschnitt Server-Host-Schlüssel wird nur für die Migration von Benutzern von einem vorhandenen Server verwendet. SFTP-enabled

- e. (Optional) Geben Sie für Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie dann Tag hinzufügen aus.
- f. Wählen Sie Weiter aus.
- g. Sie können die Leistung Ihrer Amazon S3 S3-Verzeichnisse optimieren. Nehmen wir zum Beispiel an, Sie gehen in Ihr Home-Verzeichnis und haben 10.000 Unterverzeichnisse. Mit anderen Worten, Ihr Amazon S3 S3-Bucket hat 10.000 Ordner. Wenn Sie in diesem

Szenario den Befehl `ls` (list) ausführen, dauert der Listenvorgang zwischen sechs und acht Minuten. Wenn Sie Ihre Verzeichnisse optimieren, dauert dieser Vorgang jedoch nur wenige Sekunden.

Wenn Sie Ihren Server mit der Konsole erstellen, sind optimierte Verzeichnisse standardmäßig aktiviert. Wenn Sie Ihren Server mithilfe der API erstellen, ist dieses Verhalten standardmäßig nicht aktiviert.



- h. (Optional) Konfigurieren Sie AWS Transfer Family Server so, dass Ihren Endbenutzern benutzerdefinierte Nachrichten wie Unternehmensrichtlinien oder Nutzungsbedingungen angezeigt werden. Geben Sie für Banner Pre-authentication anzeigen in das Textfeld Banner anzeigen die Textnachricht ein, die Sie Ihren Benutzern vor der Authentifizierung anzeigen möchten.
- i. (Optional) Sie können die folgenden zusätzlichen Optionen konfigurieren.
 - SetStat Option: Aktivieren Sie diese Option, um den Fehler zu ignorieren, der generiert wird, wenn ein Client versucht, eine Datei SETSTAT zu verwenden, die Sie in einen Amazon S3 S3-Bucket hochladen. Weitere Informationen finden Sie in der SetStatOption Dokumentation im [ProtocolDetails](#).
 - Wiederaufnahme der TLS-Sitzung: Diese Option ist nur verfügbar, wenn Sie FTPS als eines der Protokolle für diesen Server aktiviert haben.
 - Passive IP: Diese Option ist nur verfügbar, wenn Sie FTPS oder FTP als eines der Protokolle für diesen Server aktiviert haben.

Additional configuration

SetStat option - *optional* [Info](#)

Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - *optional* [Info](#)

Choose how you want your server to process TLS session resumption requests

☒ Enforce

☐ Enable

☐ Disable

 To enable TLS session resumption, enable FTPS as one of the protocols selected in Step 1

Passive IP - *optional* [Info](#)

Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

 To enable Passive IP, enable FTP or FTPS as one of the protocols selected in Step 1

8. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl.

- Wenn Sie eine davon bearbeiten möchten, wählen Sie neben dem Schritt Bearbeiten aus.

Note

Sie müssen jeden Schritt nach dem Schritt überprüfen, den Sie bearbeiten möchten.

- Wenn Sie keine Änderungen vorgenommen haben, wählen Sie Server erstellen, um Ihren Server zu erstellen. Sie gelangen zur Seite Servers (Server) (siehe unten), auf der der neue Server aufgelistet ist.

Es kann einige Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Zu diesem Zeitpunkt kann Ihr Server Dateioperationen ausführen, aber Sie müssen zuerst einen Benutzer erstellen. Einzelheiten zum Erstellen von Benutzern finden Sie unter [Benutzer für Serverendpunkte verwalten](#).

Einen FTPS-enabled Server erstellen

Das File Transfer Protocol over SSL (FTPS) ist eine Erweiterung von FTP. Es verwendet die kryptografischen Protokolle Transport Layer Security (TLS) und Secure Sockets Layer (SSL) zur Verschlüsselung des Datenverkehrs. FTPS ermöglicht die gleichzeitige oder unabhängige Verschlüsselung sowohl der Kontroll- als auch der Datenkanalverbindungen.

Note

Wichtige Überlegungen zu Network Load Balancers finden Sie unter [Vermeiden Sie es, AWS Transfer Family NLBs und NATs vor Servern zu platzieren](#)

So erstellen Sie einen Server FTPS-enabled

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie im Navigationsbereich Server und anschließend Server erstellen aus.
2. Wählen Sie unter Protokolle auswählen die Option FTPS aus.

Wählen Sie unter Serverzertifikat ein in AWS Certificate Manager (ACM) gespeichertes Zertifikat aus, das zur Identifizierung Ihres Servers verwendet wird, wenn Clients über FTPS eine Verbindung zu ihm herstellen, und wählen Sie dann Weiter aus.

Informationen zum Anfordern eines neuen öffentlichen Zertifikats finden Sie unter [Anfordern eines öffentlichen Zertifikats](#) im AWS Certificate Manager Benutzerhandbuch.

Informationen zum Importieren eines vorhandenen Zertifikats in ACM finden Sie unter [Zertifikate in ACM importieren](#) im AWS Certificate Manager Benutzerhandbuch.

Informationen zum Anfordern eines privaten Zertifikats für die Verwendung von FTPS über private IP-Adressen finden Sie unter [Anfordern eines privaten Zertifikats](#) im AWS Certificate Manager Benutzerhandbuch.

Zertifikate mit den folgenden kryptografischen Algorithmen und Schlüsselgrößen werden unterstützt:

- 2048-Bit-RSA (RSA_2048)
- 4096-Bit-RSA (RSA_4096)
- Elliptic Prime Curve 256-Bit (EC_prime256v1)
- Elliptic Prime Curve 384-Bit (EC_secp384r1)
- Elliptic Prime Curve 521-Bit (EC_secp521r1)

 Note

Das Zertifikat muss ein gültiges Zertifikat der SSL/TLS X.509 Version 3 mit angegebenem FQDN oder IP-Adresse sein und Informationen über den Aussteller enthalten.

3. Wählen Sie unter Identitätsanbieter auswählen den Identitätsanbieter aus, den Sie für die Verwaltung des Benutzerzugriffs verwenden möchten. Ihnen stehen folgende Optionen zur Verfügung:

- AWS Directory Service for Microsoft Active Directory— Sie stellen ein Directory Service Verzeichnis für den Zugriff auf den Endpunkt bereit. Auf diese Weise können Sie die in Ihrem Active Directory gespeicherten Anmeldeinformationen verwenden, um Ihre Benutzer zu authentifizieren. Weitere Informationen zur Arbeit mit AWS Managed Microsoft AD Identitätsanbietern finden Sie unter [Verwenden des AWS Directory Service für Microsoft Active Directory](#).

 Note

- Cross-Account und Geteilte Verzeichnisse werden nicht unterstützt für AWS Managed Microsoft AD.
- Um einen Server mit Directory Service als Identitätsanbieter einzurichten, müssen Sie einige Directory Service Berechtigungen hinzufügen. Details hierzu finden Sie unter [Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory](#).

- Benutzerdefinierter Identitätsanbieter — Wählen Sie eine der folgenden Optionen:

- Verwenden Sie AWS Lambda , um Ihren Identitätsanbieter zu verbinden — Sie können einen vorhandenen Identitätsanbieter verwenden, der von einer Lambda-Funktion unterstützt wird. Sie geben den Namen der Lambda-Funktion an. Weitere Informationen finden Sie unter [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet.](#)
- Verwenden Sie Amazon API Gateway, um Ihren Identitätsanbieter zu verbinden — Sie können eine API Gateway Gateway-Methode erstellen, die von einer Lambda-Funktion unterstützt wird, um sie als Identitätsanbieter zu verwenden. Sie geben eine Amazon API Gateway Gateway-URL und eine Aufrufrolle an. Weitere Informationen finden Sie unter [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters.](#)

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

- ☐ Service managed
Create and manage users within the service
- ☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

- ☒ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization
- ☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

- ☒ Password OR public key
- ☐ Password ONLY
- ☐ Public Key ONLY
- ☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Wählen Sie Weiter aus.

5. Gehen Sie unter Endpunkt auswählen wie folgt vor:

 Note

FTPS-Server für Transfer Family arbeiten über Port 21 (Control Channel) und Port Range 8192—8200 (Datenkanal).

- a. Wählen Sie als Endpunkttyp den VPC-gehosteten Endpunkttyp aus, um den Endpunkt Ihres Servers zu hosten. Informationen zur Einrichtung Ihres VPC-gehosteten Endpunkts finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).

 Note

Öffentlich zugängliche Endpunkte werden nicht unterstützt.

- b. (Optional) Aktivieren Sie für FIPS Enabled das Kontrollkästchen FIPS-fähiger Endpunkt, um sicherzustellen, dass der Endpunkt den Federal Information Processing Standards (FIPS) entspricht.

 Note

FIPS-enabled Endpunkte sind nur in nordamerikanischen Regionen verfügbar. AWS Informationen zu den verfügbaren Regionen finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Weitere Informationen zu FIPS finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

- c. Wählen Sie Weiter aus.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

6. Wählen Sie auf der Seite „Domain auswählen“ den AWS Speicherdienst aus, den Sie zum Speichern und Zugreifen auf Ihre Daten über das ausgewählte Protokoll verwenden möchten:

- Wählen Sie Amazon S3, um Ihre Dateien als Objekte über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.
- Wählen Sie Amazon EFS, um Ihre Dateien in Ihrem Amazon EFS-Dateisystem über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.

Wählen Sie Weiter aus.

7. Gehen Sie unter Zusätzliche Details konfigurieren wie folgt vor:

- a. Geben Sie für die Protokollierung eine bestehende Protokollgruppe an oder erstellen Sie eine neue (Standardoption).

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', it instructs to 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. There are two radio buttons: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below the radio buttons is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. Under 'Logging role', it instructs to 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. There are two radio buttons: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Wenn Sie „Protokollgruppe erstellen“ wählen, wird in der CloudWatch Konsole (<https://console.aws.amazon.com/cloudwatch/>) die Seite „Protokollgruppe erstellen“ geöffnet. Einzelheiten finden Sie unter [Protokollgruppe erstellen in CloudWatch Logs](#).

- b. (Optional) Wählen Sie für verwaltete Workflows Workflow-IDs (und eine entsprechende Rolle) aus, die Transfer Family bei der Ausführung des Workflows annehmen soll. Sie können einen Workflow auswählen, der bei einem vollständigen Upload ausgeführt wird, und einen anderen, der bei einem teilweisen Upload ausgeführt werden soll. Weitere Informationen zur Verarbeitung Ihrer Dateien mithilfe verwalteter Workflows finden Sie unter [AWS Transfer Family verwaltete Workflows](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

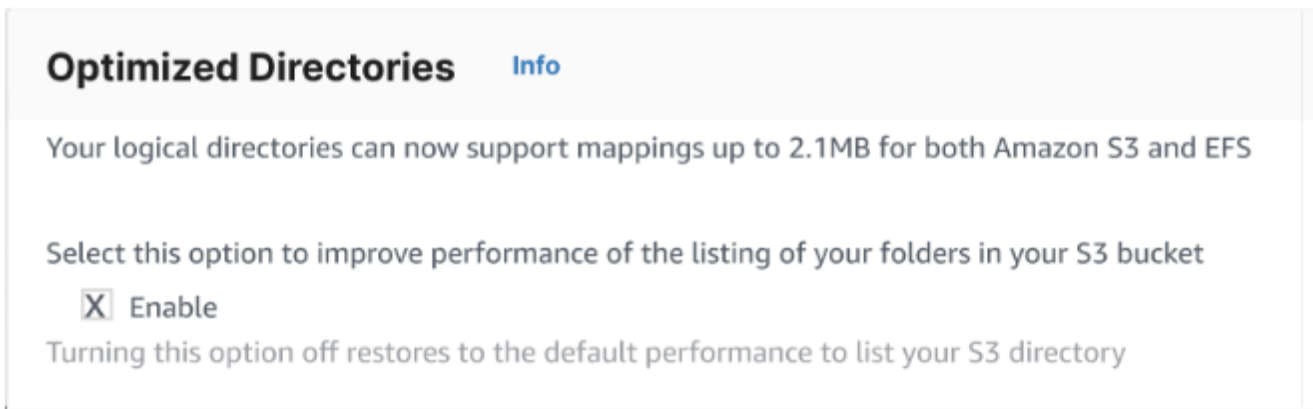
w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

- c. Wählen Sie unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind. Unsere neueste Sicherheitsrichtlinie ist die Standardeinstellung: Einzelheiten finden Sie unter: [Sicherheitsrichtlinien für Server AWS Transfer Family](#)
- d. Lassen Sie das Feld Server-Host-Schlüssel leer.
- e. (Optional) Geben Sie für Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie dann Tag hinzufügen aus.
- f. Sie können die Leistung Ihrer Amazon S3 S3-Verzeichnisse optimieren. Nehmen wir zum Beispiel an, Sie gehen in Ihr Home-Verzeichnis und haben 10.000 Unterverzeichnisse. Mit anderen Worten, Ihr Amazon S3 S3-Bucket hat 10.000 Ordner. Wenn Sie in diesem Szenario den Befehl `ls` (list) ausführen, dauert der Listenvorgang zwischen sechs und acht Minuten. Wenn Sie Ihre Verzeichnisse optimieren, dauert dieser Vorgang jedoch nur wenige Sekunden.

Wenn Sie Ihren Server mit der Konsole erstellen, sind optimierte Verzeichnisse standardmäßig aktiviert. Wenn Sie Ihren Server mithilfe der API erstellen, ist dieses Verhalten standardmäßig nicht aktiviert.



- g. Wählen Sie Weiter aus.
- h. (Optional) Sie können AWS Transfer Family Server so konfigurieren, dass Ihren Endbenutzern benutzerdefinierte Nachrichten wie Unternehmensrichtlinien oder Nutzungsbedingungen angezeigt werden. Sie können Benutzern, die sich erfolgreich authentifiziert haben, auch benutzerdefinierte Message of The Day (MOTD) anzeigen.

Geben Sie für Banner Pre-authentication anzeigen in das Textfeld Banner anzeigen die Textnachricht ein, die Sie Ihren Benutzern vor der Authentifizierung anzeigen möchten, und geben Sie in das Textfeld Banner Post-authentication anzeigen den Text ein, den Sie Ihren Benutzern nach erfolgreicher Authentifizierung anzeigen möchten.

- i. (Optional) Sie können die folgenden zusätzlichen Optionen konfigurieren.
- **SetStat Option:** Aktivieren Sie diese Option, um den Fehler zu ignorieren, der generiert wird, wenn ein Client versucht, eine Datei SETSTAT zu verwenden, die Sie in einen Amazon S3 S3-Bucket hochladen. Weitere Informationen finden Sie in der `SetStatOption` Dokumentation im [ProtocolDetails](#) Thema.
 - **Wiederaufnahme der TLS-Sitzung:** bietet einen Mechanismus zur Wiederaufnahme oder gemeinsamen Nutzung eines ausgehandelten geheimen Schlüssels zwischen der Kontroll- und Datenverbindung für eine FTPS-Sitzung. Weitere Informationen finden Sie in der `TlsSessionResumptionMode` Dokumentation zum Thema. [ProtocolDetails](#)
 - **Passive IP:** steht für den passiven Modus für FTP- und FTPS-Protokolle. Geben Sie eine einzelne IPv4-Adresse ein, z. B. die öffentliche IP-Adresse einer Firewall, eines Routers oder eines Load Balancers. Weitere Informationen finden Sie in der `PassiveIp` Dokumentation zum [ProtocolDetails](#) Thema.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl.

- Wenn Sie eine davon bearbeiten möchten, wählen Sie neben dem Schritt Bearbeiten aus.

 Note

Sie müssen jeden Schritt nach dem Schritt überprüfen, den Sie bearbeiten möchten.

- Wenn Sie keine Änderungen vorgenommen haben, wählen Sie Server erstellen, um Ihren Server zu erstellen. Sie gelangen zur Seite Servers (Server) (siehe unten), auf der der neue Server aufgelistet ist.

Es kann einige Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Ab diesem Zeitpunkt kann der Server Dateioperationen für die Benutzer ausführen.

Nächste Schritte: Fahren Sie im nächsten Schritt mit [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#) So richten Sie Benutzer ein.

Erstellen Sie einen FTP-enabled Server

Das File Transfer Protocol (FTP) ist ein Netzwerkprotokoll, das für die Übertragung von Daten verwendet wird. FTP verwendet einen separaten Kanal für Steuerung und Datenübertragungen. Der Steuerkanal ist geöffnet, bis er beendet wird oder ein Timeout bei Inaktivität eintritt. Der Datenkanal ist für die Dauer der Übertragung aktiv. FTP verwendet Klartext und unterstützt keine Verschlüsselung des Datenverkehrs.

Note

Wenn Sie FTP aktivieren, müssen Sie die interne Zugriffsoption für den VPC-hosted Endpunkt auswählen. Wenn Sie möchten, dass Ihr Server Daten über das öffentliche Netzwerk überträgt, müssen Sie sichere Protokolle wie SFTP oder FTPS verwenden.

Note

Wichtige Überlegungen zu Network Load Balancers finden Sie unter [Vermeiden Sie es, AWS Transfer Family NLBs und NATs vor Servern zu platzieren](#)

So erstellen Sie einen Server FTP-enabled

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie im Navigationsbereich Server und anschließend Server erstellen aus.
2. Wählen Sie unter Protokolle auswählen die Option FTP und dann Weiter aus.
3. Wählen Sie unter Wählen Sie einen Identitätsanbieter aus den Identitätsanbieter aus, den Sie für die Verwaltung des Benutzerzugriffs verwenden möchten. Ihnen stehen folgende Optionen zur Verfügung:
 - AWS Directory Service for Microsoft Active Directory— Sie stellen ein Directory Service Verzeichnis für den Zugriff auf den Endpunkt bereit. Auf diese Weise können Sie die in Ihrem Active Directory gespeicherten Anmeldeinformationen verwenden, um Ihre Benutzer zu authentifizieren. Weitere Informationen zur Arbeit mit AWS Managed Microsoft AD Identitätsanbietern finden Sie unter [Verwenden des AWS Directory Service für Microsoft Active Directory](#).

 Note

- Cross-Account und Geteilte Verzeichnisse werden nicht unterstützt für AWS Managed Microsoft AD.
- Um einen Server mit Directory Service als Identitätsanbieter einzurichten, müssen Sie einige Directory Service Berechtigungen hinzufügen. Details hierzu finden Sie unter [Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory](#).

- Benutzerdefinierter Identitätsanbieter — Wählen Sie eine der folgenden Optionen:
 - Verwenden Sie AWS Lambda , um Ihren Identitätsanbieter zu verbinden — Sie können einen vorhandenen Identitätsanbieter verwenden, der von einer Lambda-Funktion unterstützt wird. Sie geben den Namen der Lambda-Funktion an. Weitere Informationen finden Sie unter [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet](#).
 - Verwenden Sie Amazon API Gateway, um Ihren Identitätsanbieter zu verbinden — Sie können eine API Gateway Gateway-Methode erstellen, die von einer Lambda-Funktion unterstützt wird, um sie als Identitätsanbieter zu verwenden. Sie geben eine Amazon API Gateway Gateway-URL und eine Aufrufrolle an. Weitere Informationen finden Sie unter [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

- ☐ **Service managed**
Create and manage users within the service
- ☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

- ☒ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization
- ☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

- ☒ Password OR public key
- ☐ Password ONLY
- ☐ Public Key ONLY
- ☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

- Wählen Sie Weiter aus.
- Gehen Sie unter Endpunkt auswählen wie folgt vor:

[i](#) Note

FTP-Server für Transfer Family arbeiten über Port 21 (Steuerkanal) und Portbereich 8192—8200 (Datenkanal).

- a. Wählen Sie als Endpunkttyp die Option VPC hostet, um den Endpunkt Ihres Servers zu hosten. Informationen zur Einrichtung Ihres VPC-gehosteten Endpunkts finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).

 Note

Öffentlich zugängliche Endpunkte werden nicht unterstützt.

- b. Lassen Sie für FIPS Enabled das Kontrollkästchen FIPS-fähiger Endpunkt deaktiviert.

 Note

FIPS-enabled Endpunkte werden für FTP-Server nicht unterstützt.

- c. Wählen Sie Weiter aus.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

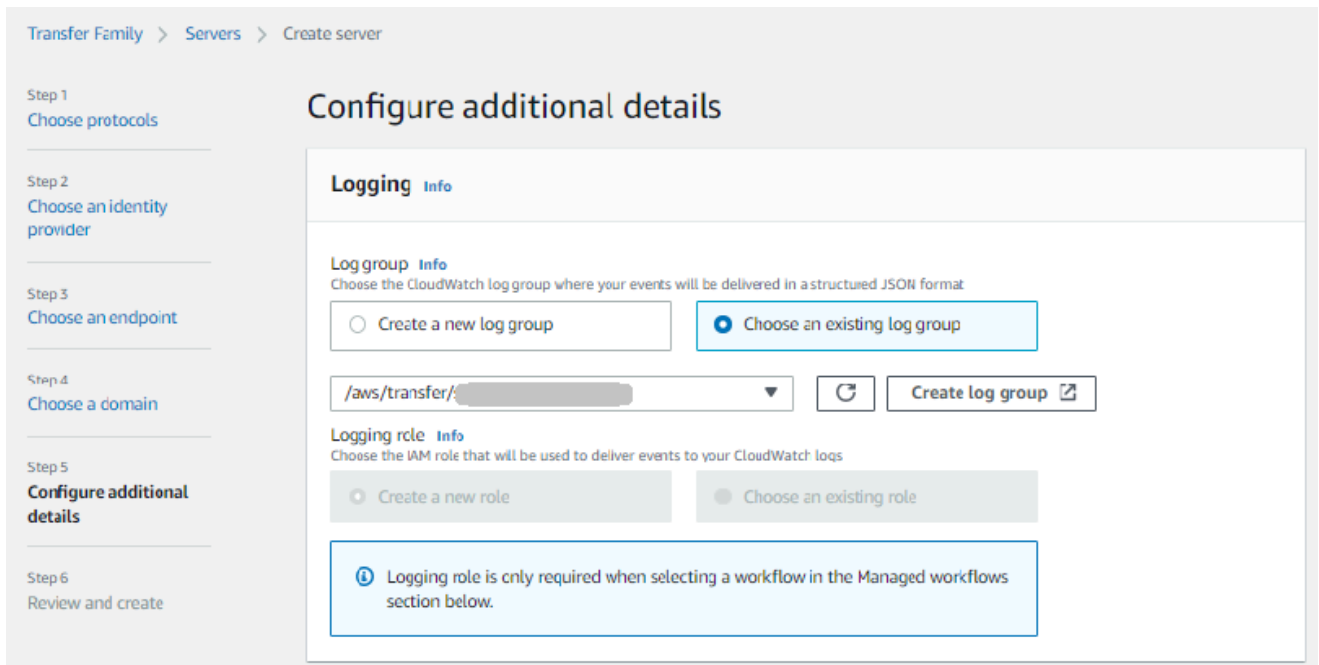
[Cancel](#) [Previous](#) [Next](#)

6. Wählen Sie auf der Seite „Domain auswählen“ den AWS Speicherdienst aus, den Sie zum Speichern und Zugreifen auf Ihre Daten über das ausgewählte Protokoll verwenden möchten.
 - Wählen Sie Amazon S3, um Ihre Dateien als Objekte über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.
 - Wählen Sie Amazon EFS, um Ihre Dateien in Ihrem Amazon EFS-Dateisystem über das ausgewählte Protokoll zu speichern und darauf zuzugreifen.

Wählen Sie Weiter aus.

7. Gehen Sie unter Zusätzliche Details konfigurieren wie folgt vor:

- a. Geben Sie für die Protokollierung eine bestehende Protokollgruppe an oder erstellen Sie eine neue (Standardoption).



Wenn Sie „Protokollgruppe erstellen“ wählen, wird in der CloudWatch Konsole (<https://console.aws.amazon.com/cloudwatch/>) die Seite „Protokollgruppe erstellen“ geöffnet. Einzelheiten finden Sie unter [Protokollgruppe erstellen in CloudWatch Logs](#).

- b. (Optional) Wählen Sie für verwaltete Workflows Workflow-IDs (und eine entsprechende Rolle) aus, die Transfer Family bei der Ausführung des Workflows annehmen soll. Sie können einen Workflow auswählen, der bei einem vollständigen Upload ausgeführt wird, und einen anderen, der bei einem teilweisen Upload ausgeführt werden soll. Weitere Informationen zur Verarbeitung Ihrer Dateien mithilfe verwalteter Workflows finden Sie unter [AWS Transfer Family verwaltete Workflows](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

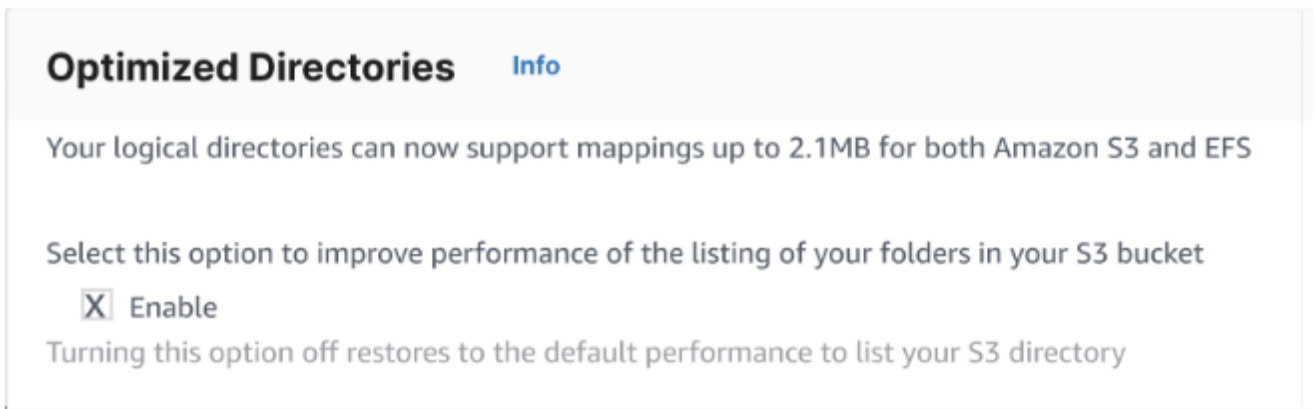
- c. Wählen Sie unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind.

Note

Transfer Family weist Ihrem FTP-Server die neueste Sicherheitsrichtlinie zu. Da das FTP-Protokoll jedoch keine Verschlüsselung verwendet, verwenden FTP-Server keinen der Sicherheitsrichtlinien-Algorithmen. Sofern Ihr Server nicht auch das FTPS- oder SFTP-Protokoll verwendet, bleibt die Sicherheitsrichtlinie ungenutzt.

- d. Lassen Sie das Feld Server-Hostschlüssel leer.
- e. (Optional) Geben Sie für Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie dann Tag hinzufügen aus.
- f. Sie können die Leistung Ihrer Amazon S3 S3-Verzeichnisse optimieren. Nehmen wir zum Beispiel an, Sie gehen in Ihr Home-Verzeichnis und haben 10.000 Unterverzeichnisse. Mit anderen Worten, Ihr Amazon S3 S3-Bucket hat 10.000 Ordner. Wenn Sie in diesem Szenario den Befehl `ls` (list) ausführen, dauert der Listenvorgang zwischen sechs und acht Minuten. Wenn Sie Ihre Verzeichnisse optimieren, dauert dieser Vorgang jedoch nur wenige Sekunden.

Wenn Sie Ihren Server mit der Konsole erstellen, sind optimierte Verzeichnisse standardmäßig aktiviert. Wenn Sie Ihren Server mithilfe der API erstellen, ist dieses Verhalten standardmäßig nicht aktiviert.



- g. Wählen Sie Weiter aus.
- h. (Optional) Sie können AWS Transfer Family Server so konfigurieren, dass Ihren Endbenutzern benutzerdefinierte Nachrichten wie Unternehmensrichtlinien oder Nutzungsbedingungen angezeigt werden. Sie können Benutzern, die sich erfolgreich authentifiziert haben, auch benutzerdefinierte Message of The Day (MOTD) anzeigen.

Geben Sie für Banner Pre-authentication anzeigen in das Textfeld Banner anzeigen die Textnachricht ein, die Sie Ihren Benutzern vor der Authentifizierung anzeigen möchten, und geben Sie in das Textfeld Banner Post-authentication anzeigen den Text ein, den Sie Ihren Benutzern nach erfolgreicher Authentifizierung anzeigen möchten.

- i. (Optional) Sie können die folgenden zusätzlichen Optionen konfigurieren.
- **SetStat Option:** Aktivieren Sie diese Option, um den Fehler zu ignorieren, der generiert wird, wenn ein Client versucht, eine Datei SETSTAT zu verwenden, die Sie in einen Amazon S3 S3-Bucket hochladen. Weitere Informationen finden Sie in der `SetStatOption` Dokumentation im [ProtocolDetails](#) Thema.
 - **Wiederaufnahme der TLS-Sitzung:** bietet einen Mechanismus zur Wiederaufnahme oder gemeinsamen Nutzung eines ausgehandelten geheimen Schlüssels zwischen der Kontroll- und Datenverbindung für eine FTPS-Sitzung. Weitere Informationen finden Sie in der `TlsSessionResumptionMode` Dokumentation zum Thema. [ProtocolDetails](#)
 - **Passive IP:** steht für den passiven Modus für FTP- und FTPS-Protokolle. Geben Sie eine einzelne IPv4-Adresse ein, z. B. die öffentliche IP-Adresse einer Firewall, eines Routers oder eines Load Balancers. Weitere Informationen finden Sie in der `PassiveIp` Dokumentation zum [ProtocolDetails](#) Thema.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl.

- Wenn Sie eine davon bearbeiten möchten, wählen Sie neben dem Schritt Bearbeiten aus.

 Note

Sie müssen jeden Schritt nach dem Schritt überprüfen, den Sie bearbeiten möchten.

- Wenn Sie keine Änderungen vorgenommen haben, wählen Sie Server erstellen, um Ihren Server zu erstellen. Sie gelangen zur Seite Servers (Server) (siehe unten), auf der der neue Server aufgelistet ist.

Es kann einige Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Ab diesem Zeitpunkt kann der Server Dateioperationen für die Benutzer ausführen.

Nächste Schritte — Fahren Sie im nächsten Schritt mit [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#) So richten Sie Benutzer ein.

Erstellen Sie einen Server in einer virtuellen privaten Cloud

Sie können den Endpunkt Ihres Servers in einer Virtual Private Cloud (VPC) hosten, um Daten zu und von einem Amazon S3-Bucket oder Amazon EFS-Dateisystem zu übertragen, ohne das öffentliche Internet nutzen zu müssen.

Note

Nach dem 19. Mai 2021 können Sie mit `EndpointType=VPC_ENDPOINT` Ihrem Konto keinen Server mehr erstellen, wenn Ihr AWS Konto dies nicht bereits vor dem 19. Mai 2021 getan hat. Wenn du am oder vor dem 21. Februar 2021 bereits Server mit `EndpointType=VPC_ENDPOINT` deinem AWS Konto erstellt hast, bist du davon nicht betroffen. Verwenden Sie nach diesem Datum `EndpointType =VPC`. Weitere Informationen finden Sie unter [the section called “Einstellung der Verwendung von VPC_ENDPOINT”](#).

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine private Verbindung zwischen Ihrer VPC und einem Server herstellen. Sie können diesen Server dann verwenden, um Daten über Ihren Client zu und von Ihrem Amazon S3 S3-Bucket zu übertragen, ohne öffentliche IP-Adressen zu verwenden oder ein Internet-Gateway zu benötigen.

Mit Amazon VPC können Sie AWS Ressourcen in einem benutzerdefinierten virtuellen Netzwerk starten. Mit einer VPC können Sie Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways, steuern. Weitere Informationen zu VPCs finden Sie unter [Was ist Amazon VPC?](#) im Amazon VPC-Benutzerhandbuch.

In den nächsten Abschnitten finden Sie Anweisungen zum Erstellen und Verbinden Ihrer VPC mit einem Server. Im Überblick gehen Sie dazu wie folgt vor:

1. Richten Sie einen Server mit einem VPC-Endpunkt ein.
2. Connect Sie mithilfe eines Clients, der sich in Ihrer VPC befindet, über den VPC-Endpunkt eine Verbindung zu Ihrem Server her. Auf diese Weise können Sie Daten, die in Ihrem Amazon S3 S3-Bucket gespeichert sind, mithilfe von über Ihren Client übertragen AWS Transfer Family. Sie können diese Übertragung durchführen, obwohl das Netzwerk vom öffentlichen Internet getrennt ist.
3. Wenn Sie sich dafür entscheiden, den Endpunkt Ihres Servers mit dem Internet zu verbinden, können Sie Ihrem Endpunkt außerdem Elastic IP-Adressen zuordnen. Auf diese Weise können

Clients außerhalb Ihrer VPC eine Verbindung zu Ihrem Server herstellen. Sie können VPC-Sicherheitsgruppen verwenden, um den Zugriff auf authentifizierte Benutzer zu kontrollieren, deren Anfragen nur von zulässigen Adressen stammen.

 Note

AWS Transfer Family unterstützt Dual-Stack-Endpunkte, sodass Ihr Server sowohl über IPv4 als auch über IPv6 kommunizieren kann. Um die Dual-Stack-Unterstützung zu aktivieren, wählen Sie bei der Erstellung Ihres VPC-Endpunkts die Option DNS-Dual-Stack-Endpunkt aktivieren aus. Beachten Sie, dass sowohl Ihre VPC als auch Ihre Subnetze so konfiguriert sein müssen, dass sie IPv6 unterstützen, bevor Sie diese Funktion verwenden können. Dual-stack Unterstützung ist besonders nützlich, wenn Sie Clients haben, die über eines der Protokolle eine Verbindung herstellen müssen.

Hinweise zu Dual-Stack-Serverendpunkten (IPv4 und IPv6) finden Sie unter. [IPv6-Unterstützung für Transfer Family Family-Server](#)

Themen

- [Erstellen Sie einen Serverendpunkt, auf den nur innerhalb Ihrer VPC zugegriffen werden kann](#)
- [Erstellen Sie einen mit dem Internet verbundenen Endpunkt für Ihren Server](#)
- [Ändern Sie den Endpunkttyp für Ihren Server](#)
- [Einstellung der Verwendung von VPC_ENDPOINT](#)
- [Beschränkung des VPC-Endpunktzugriffs für Transfer Family Family-Server](#)
- [Zusätzliche Netzwerkfunktionen](#)
- [Aktualisierung des AWS Transfer Family Serverendpunkttyps von VPC_ENDPOINT auf VPC](#)

Erstellen Sie einen Serverendpunkt, auf den nur innerhalb Ihrer VPC zugegriffen werden kann

Im folgenden Verfahren erstellen Sie einen Serverendpunkt, auf den nur Ressourcen innerhalb Ihrer VPC zugreifen können.

So erstellen Sie einen Serverendpunkt in einer VPC

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>

2. Wählen Sie im Navigationsbereich Server und anschließend Server erstellen aus.
3. Wählen Sie unter Protokolle auswählen ein oder mehrere Protokolle aus, und klicken Sie dann auf Weiter. Weitere Informationen zu Protokollen finden Sie unter [Schritt 2: Einen SFTP-enabled Server erstellen](#).
4. Wählen Sie unter Einen Identitätsanbieter auswählen die Option Dienst verwaltet, um Benutzeridentitäten und Schlüssel zu speichern AWS Transfer Family, und klicken Sie dann auf Weiter.

Bei diesem Verfahren wird die vom Dienst verwaltete Option verwendet. Wenn Sie Benutzerdefiniert wählen, geben Sie einen Amazon API Gateway Gateway-Endpunkt und eine AWS Identity and Access Management (IAM) -Rolle für den Zugriff auf den Endpunkt an. Auf diese Weise können Sie Ihren Verzeichnisdienst integrieren, um Ihre Benutzer zu authentifizieren und zu autorisieren. Weitere Informationen zur Verwendung benutzerdefinierter Identitätsanbieter siehe [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#).

5. Gehen Sie unter Endpunkt auswählen wie folgt vor:
 - a. Wählen Sie als Endpunkttyp den VPC-gehosteten Endpunkttyp aus, um den Endpunkt Ihres Servers zu hosten.
 - b. Wählen Sie für Zugriff die Option Intern aus, um Ihren Endpunkt nur für Clients zugänglich zu machen, die die privaten IP-Adressen des Endpunkts verwenden.

Einzelheiten zur Option „Internetzugriff“ finden Sie unter [Erstellen Sie einen mit dem Internet verbundenen Endpunkt für Ihren Server](#). Ein Server, der in einer VPC nur für den internen Zugriff erstellt wurde, unterstützt keine benutzerdefinierten Hostnamen.

- c. Wählen Sie für VPC eine vorhandene VPC-ID oder wählen Sie Create a VPC, um eine neue VPC zu erstellen.
 - d. Wählen Sie im Abschnitt Availability Zones bis zu drei Availability Zones und zugehörige Subnetze aus.
 - e. Wählen Sie im Abschnitt Sicherheitsgruppen eine oder mehrere vorhandene Sicherheitsgruppen-IDs aus, oder wählen Sie Sicherheitsgruppe erstellen, um eine neue Sicherheitsgruppe zu erstellen. Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Sicherheitsgruppen für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch. Informationen zum Erstellen einer Sicherheitsgruppe finden Sie unter [Erstellen einer Sicherheitsgruppe](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

 Note

Ihre VPC verfügt automatisch über eine Standardsicherheitsgruppe. Wenn Sie beim Starten des Servers keine andere Sicherheitsgruppe oder Gruppen angeben, ordnen wir Ihrem Server die Standardsicherheitsgruppe zu.

- Für die eingehenden Regeln für die Sicherheitsgruppe können Sie den SSH-Verkehr so konfigurieren, dass er Port 22, 2222, 22000 oder eine beliebige Kombination verwendet. Port 22 ist standardmäßig konfiguriert. Um Port 2222 oder Port 22000 zu verwenden, fügen Sie Ihrer Sicherheitsgruppe eine Regel für eingehenden Datenverkehr hinzu. Wählen Sie für den Typ Benutzerdefiniertes TCP aus, geben Sie dann entweder **2222** oder **22000** als Portbereich ein und geben Sie für die Quelle denselben CIDR-Bereich ein, den Sie für Ihre SSH-Port-22-Regel haben.
- Konfigurieren Sie für die eingehenden Regeln für die Sicherheitsgruppe FTP- und FTPS-Verkehr so, dass der Portbereich **21** für den Steuerkanal und **8192-8200** für den Datenkanal verwendet wird.

 Note

Sie können Port 2223 auch für Clients verwenden, die TCP-"Piggy-Back" -ACKs oder die Fähigkeit benötigen, dass das letzte Ack des TCP-3-Wege-Handshakes auch Daten enthält.

Manche Client-Software ist möglicherweise nicht mit Port 2223 kompatibel, z. B. ein Client, bei dem der Server die SFTP-Identifikationszeichenfolge senden muss, bevor der Client dies tut.

[VPC](#) > [Security Groups](#) > [sg-\[REDACTED\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[REDACTED]	HTTP
sg-[REDACTED]	RDP
sg-[REDACTED]	HTTPS
sg-[REDACTED]	Custom TCP
sg-[REDACTED]	SSH

[Add rule](#)

- f. (Optional) Aktivieren Sie für FIPS Enabled das Kontrollkästchen FIPS-fähiger Endpunkt, um sicherzustellen, dass der Endpunkt den Federal Information Processing Standards (FIPS) entspricht.

 Note

FIPS-enabled Endpunkte sind nur in nordamerikanischen Regionen verfügbar. AWS Informationen zu den verfügbaren Regionen finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Weitere Informationen zu FIPS finden Sie unter [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- g. Wählen Sie Weiter aus.
6. Gehen Sie unter Zusätzliche Details konfigurieren wie folgt vor:
- a. Wählen Sie für die CloudWatch Protokollierung eine der folgenden Optionen, um die CloudWatch Amazon-Protokollierung Ihrer Benutzeraktivitäten zu aktivieren:
- Erstellen Sie eine neue Rolle, damit Transfer Family die IAM-Rolle automatisch erstellen kann, sofern Sie über die erforderlichen Berechtigungen zum Erstellen einer neuen Rolle verfügen. Die erstellte IAM-Rolle wird aufgerufen. `AWSTransferLoggingAccess`
 - Wählen Sie eine vorhandene Rolle aus, um eine bestehende IAM-Rolle aus Ihrem Konto auszuwählen. Wählen Sie unter Logging-Rolle die Rolle aus. Diese IAM-Rolle sollte eine Vertrauensrichtlinie mit der Einstellung Service auf `transfer.amazonaws.com` enthalten.

Weitere Informationen zur CloudWatch Protokollierung finden Sie unter [Konfigurieren Sie die CloudWatch Protokollierungsrolle](#).

 Note

- Sie können keine Endbenutzeraktivitäten in anzeigen, CloudWatch wenn Sie keine Protokollierungsrolle angeben.
- Wenn Sie keine CloudWatch Protokollierungsrolle einrichten möchten, wählen Sie Bestehende Rolle auswählen, aber wählen Sie keine Protokollierungsrolle aus.

- b. Wählen Sie unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind.

 Note

Standardmäßig ist die `TransferSecurityPolicy-2024-01` Sicherheitsrichtlinie an Ihren Server angehängt, sofern Sie keine andere auswählen.

Weitere Informationen zu Sicherheitsrichtlinien finden Sie unter [Sicherheitsrichtlinien für Server AWS Transfer Family](#).

- c. (Optional: Dieser Abschnitt ist nur für die Migration von Benutzern von einem vorhandenen SFTP-enabled Server vorgesehen.) Geben Sie als Server-Hostschlüssel einen privaten RSA-, ED25519- oder ECDSA-Schlüssel ein, der zur Identifizierung Ihres Servers verwendet wird, wenn Clients über SFTP eine Verbindung zu ihm herstellen.
 - d. (Optional) Geben Sie für Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie dann Tag hinzufügen aus.
 - e. Wählen Sie Weiter aus.
7. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl. Wenn Sie:
- Wenn Sie eine davon bearbeiten möchten, wählen Sie neben dem Schritt Bearbeiten aus.

 Note

Sie müssen jeden Schritt nach dem Schritt, den Sie bearbeiten möchten, erneut überprüfen.

- Haben Sie keine Änderungen vorgenommen, wählen Sie Server erstellen, um Ihren Server zu erstellen. Sie gelangen zur Seite Servers (Server) (siehe unten), auf der der neue Server aufgelistet ist.

Es kann einige Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Zu diesem Zeitpunkt kann Ihr Server Dateioperationen ausführen, aber Sie müssen zuerst einen Benutzer erstellen. Einzelheiten zum Erstellen von Benutzern finden Sie unter [Benutzer für Serverendpunkte verwalten](#).

Erstellen Sie einen mit dem Internet verbundenen Endpunkt für Ihren Server

Im folgenden Verfahren erstellen Sie einen Serverendpunkt. Auf diesen Endpunkt können nur Clients über das Internet zugreifen, deren Quell-IP-Adressen in der Standardsicherheitsgruppe Ihrer VPC zulässig sind. Indem Sie Elastic IP-Adressen verwenden, um Ihren Endpunkt mit dem Internet zu verbinden, können Ihre Kunden die Elastic IP-Adresse außerdem verwenden, um den Zugriff auf Ihren Endpunkt in ihren Firewalls zu ermöglichen.

Note

Nur SFTP und FTPS können auf einem mit dem Internet verbundenen VPC-gehosteten Endpunkt verwendet werden.

Um einen mit dem Internet verbundenen Endpunkt zu erstellen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im Navigationsbereich Server und anschließend Server erstellen aus.
3. Wählen Sie unter Protokolle auswählen ein oder mehrere Protokolle aus, und klicken Sie dann auf Weiter. Weitere Informationen zu Protokollen finden Sie unter [Schritt 2: Einen SFTP-enabled Server erstellen](#).
4. Wählen Sie unter Einen Identitätsanbieter auswählen die Option Dienst verwaltet, um Benutzeridentitäten und Schlüssel zu speichern AWS Transfer Family, und klicken Sie dann auf Weiter.

Bei diesem Verfahren wird die vom Dienst verwaltete Option verwendet. Wenn Sie Benutzerdefiniert wählen, geben Sie einen Amazon API Gateway Gateway-Endpunkt und eine AWS Identity and Access Management (IAM) -Rolle für den Zugriff auf den Endpunkt an. Auf diese Weise können Sie Ihren Verzeichnisdienst integrieren, um Ihre Benutzer zu authentifizieren und zu autorisieren. Weitere Informationen zur Verwendung benutzerdefinierter Identitätsanbieter siehe [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#).

5. Gehen Sie unter Endpunkt auswählen wie folgt vor:
 - a. Wählen Sie als Endpunkttyp den VPC-gehosteten Endpunkttyp aus, um den Endpunkt Ihres Servers zu hosten.
 - b. Wählen Sie für Access die Option Internet Facing aus, um Ihren Endpunkt für Kunden über das Internet zugänglich zu machen.

 Note

Wenn Sie sich für Internet Facing entscheiden, können Sie in jedem Subnetz oder Subnetzen eine bestehende Elastic IP-Adresse auswählen. Oder Sie können die VPC-Konsole (<https://console.aws.amazon.com/vpc/>) aufrufen, um eine oder mehrere neue Elastic IP-Adressen zuzuweisen. Diese Adressen können entweder Ihnen AWS oder Ihnen gehören. Sie können Elastic IP-Adressen, die bereits verwendet werden, nicht mit Ihrem Endpunkt verknüpfen.

- c. (Optional) Wählen Sie für Benutzerdefinierter Hostname eine der folgenden Optionen:

 Note

Kunden, die eine direkte Verbindung über die Elastic IP-Adresse herstellen oder einen Hostnamen-Datensatz in Commercial Route 53 erstellen AWS GovCloud (US) müssen, der auf ihre EIP verweist. Weitere Informationen zur Verwendung von Route 53 für GovCloud Endgeräte finden Sie unter [Einrichten von Amazon Route 53 mit Ihren AWS GovCloud \(US\) Ressourcen](#) im AWS GovCloud (US) Benutzerhandbuch.

- Amazon Route 53 DNS-Alias — wenn der Hostname, den Sie verwenden möchten, bei Route 53 registriert ist. Sie können dann den Hostnamen eingeben.
- Anderes DNS — wenn der Hostname, den Sie verwenden möchten, bei einem anderen DNS-Anbieter registriert ist. Sie können dann den Hostnamen eingeben.
- Keine — um den Endpunkt des Servers zu verwenden und keinen benutzerdefinierten Hostnamen zu verwenden. Der Server-Host-Name hat das Format *server-id.server.transfer.region.amazonaws.com*.

 Note

Für Kunden in AWS GovCloud (US) wird durch die Auswahl von None kein Hostname in diesem Format erstellt.

Weitere Informationen zum Arbeiten mit benutzerdefinierten Hostnamen finden Sie unter. [Mit benutzerdefinierten Hostnamen arbeiten](#)

- d. Wählen Sie für VPC eine vorhandene VPC-ID oder wählen Sie Create a VPC, um eine neue VPC zu erstellen.
- e. Wählen Sie im Abschnitt Availability Zones bis zu drei Availability Zones und zugehörige Subnetze aus. Wählen Sie für IPv4-Adressen eine Elastic IP-Adresse für jedes Subnetz aus. Dies ist die IP-Adresse, die Ihre Clients verwenden können, um den Zugriff auf Ihren Endpunkt in ihren Firewalls zu ermöglichen.

Tipp: Sie müssen ein öffentliches Subnetz für Ihre Availability Zones verwenden oder zuerst ein Internet-Gateway einrichten, wenn Sie ein privates Subnetz verwenden möchten.

- f. Wählen Sie im Abschnitt Sicherheitsgruppen eine oder mehrere vorhandene Sicherheitsgruppen-IDs aus, oder wählen Sie Sicherheitsgruppe erstellen, um eine neue Sicherheitsgruppe zu erstellen. Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Sicherheitsgruppen für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch. Informationen zum Erstellen einer Sicherheitsgruppe finden Sie unter [Erstellen einer Sicherheitsgruppe](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

 Note

Ihre VPC verfügt automatisch über eine Standardsicherheitsgruppe. Wenn Sie beim Starten des Servers keine andere Sicherheitsgruppe oder Gruppen angeben, ordnen wir Ihrem Server die Standardsicherheitsgruppe zu.

- Für die eingehenden Regeln für die Sicherheitsgruppe können Sie den SSH-Verkehr so konfigurieren, dass er Port 22, 2222, 22000 oder eine beliebige Kombination verwendet. Port 22 ist standardmäßig konfiguriert. Um Port 2222 oder Port 22000 zu verwenden, fügen Sie Ihrer Sicherheitsgruppe eine Regel für eingehenden Datenverkehr hinzu. Wählen Sie für den Typ Benutzerdefiniertes TCP aus, geben Sie dann entweder **2222** oder **22000** als Portbereich ein und geben Sie für die Quelle denselben CIDR-Bereich ein, den Sie für Ihre SSH-Port-22-Regel haben.

- Konfigurieren Sie für die eingehenden Regeln für die Sicherheitsgruppe den FTPS-Verkehr so, dass der Portbereich **21** für den Steuerkanal und **8192-8200** für den Datenkanal verwendet wird.

 Note

Sie können Port 2223 auch für Clients verwenden, die TCP-Huckepack-ACKs oder die Möglichkeit benötigen, dass das letzte Ack des TCP-3-Wege-Handshakes auch Daten enthält.

Manche Client-Software ist möglicherweise nicht mit Port 2223 kompatibel, z. B. ein Client, bei dem der Server die SFTP-Identifikationszeichenfolge senden muss, bevor der Client dies tut.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- g. (Optional) Aktivieren Sie für FIPS Enabled das Kontrollkästchen FIPS-fähiger Endpunkt, um sicherzustellen, dass der Endpunkt den Federal Information Processing Standards (FIPS) entspricht.

 Note

FIPS-enabled Endpunkte sind nur in nordamerikanischen Regionen verfügbar. AWS Informationen zu den verfügbaren Regionen finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz Weitere Informationen zu FIPS finden Sie unter [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- h. Wählen Sie Weiter aus.
6. Gehen Sie unter Zusätzliche Details konfigurieren wie folgt vor:
- a. Wählen Sie für die CloudWatch Protokollierung eine der folgenden Optionen, um die CloudWatch Amazon-Protokollierung Ihrer Benutzeraktivitäten zu aktivieren:
- Erstellen Sie eine neue Rolle, damit Transfer Family die IAM-Rolle automatisch erstellen kann, sofern Sie über die erforderlichen Berechtigungen zum Erstellen einer neuen Rolle verfügen. Die erstellte IAM-Rolle wird aufgerufen. `AWSTransferLoggingAccess`
 - Wählen Sie eine vorhandene Rolle aus, um eine bestehende IAM-Rolle aus Ihrem Konto auszuwählen. Wählen Sie unter Logging-Rolle die Rolle aus. Diese IAM-Rolle sollte eine Vertrauensrichtlinie mit der Einstellung Service auf `transfer.amazonaws.com` enthalten.

Weitere Informationen zur CloudWatch Protokollierung finden Sie unter [Konfigurieren Sie die CloudWatch Protokollierungsrolle](#).

 Note

- Sie können keine Endbenutzeraktivitäten in anzeigen, CloudWatch wenn Sie keine Protokollierungsrolle angeben.
- Wenn Sie keine CloudWatch Protokollierungsrolle einrichten möchten, wählen Sie Bestehende Rolle auswählen, aber wählen Sie keine Protokollierungsrolle aus.

- b. Wählen Sie unter Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind.

Note

Standardmäßig ist die `TransferSecurityPolicy-2024-01` Sicherheitsrichtlinie an Ihren Server angehängt, sofern Sie keine andere auswählen.

Weitere Informationen zu Sicherheitsrichtlinien finden Sie unter [Sicherheitsrichtlinien für Server AWS Transfer Family](#).

- c. (Optional: Dieser Abschnitt ist nur für die Migration von Benutzern von einem vorhandenen SFTP-enabled Server vorgesehen.) Geben Sie als Server-Hostschlüssel einen privaten RSA-, ED25519- oder ECDSA-Schlüssel ein, der zur Identifizierung Ihres Servers verwendet wird, wenn Clients über SFTP eine Verbindung zu ihm herstellen.
- d. (Optional) Geben Sie für Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie dann Tag hinzufügen aus.
- e. Wählen Sie Weiter aus.
- f. (Optional) Wählen Sie für verwaltete Workflows Workflow-IDs (und eine entsprechende Rolle) aus, die Transfer Family bei der Ausführung des Workflows annehmen soll. Sie können einen Workflow auswählen, der bei einem vollständigen Upload ausgeführt wird, und einen anderen, der bei einem teilweisen Upload ausgeführt werden soll. Weitere Informationen zur Verarbeitung Ihrer Dateien mithilfe verwalteter Workflows finden Sie unter [AWS Transfer Family verwaltete Workflows](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

7. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl. Wenn Sie:

- Wenn Sie eine davon bearbeiten möchten, wählen Sie neben dem Schritt Bearbeiten aus.

 Note

Sie müssen jeden Schritt nach dem Schritt, den Sie bearbeiten möchten, erneut überprüfen.

- Haben Sie keine Änderungen vorgenommen, wählen Sie **Server erstellen**, um Ihren Server zu erstellen. Sie gelangen zur Seite **Servers (Server)** (siehe unten), auf der der neue Server aufgelistet ist.

Sie können die Server-ID auswählen, um die detaillierten Einstellungen des Servers zu sehen, den Sie gerade erstellt haben. Nachdem die Spalte **Öffentliche IPv4-Adresse** gefüllt wurde, wurden die von Ihnen angegebenen Elastic IP-Adressen erfolgreich mit dem Endpunkt Ihres Servers verknüpft.

 Note

Wenn Ihr Server in einer VPC online ist, können nur die Subnetze geändert werden, und zwar nur über die [UpdateServer](#) API. Sie müssen [den Server anhalten](#), um die Elastic-IP-Adressen des Serverendpunkts hinzuzufügen oder zu ändern.

Ändern Sie den Endpunkttyp für Ihren Server

Wenn Sie bereits über einen Server verfügen, auf den über das Internet zugegriffen werden kann (d. h. einen öffentlichen Endpunkttyp hat), können Sie seinen Endpunkt in einen VPC-Endpunkt ändern.

 Note

Wenn Sie einen vorhandenen Server in einer VPC als angezeigt haben, empfehlen wir Ihnen `VPC_ENDPOINT`, ihn auf den neuen VPC-Endpunkttyp zu ändern. Mit diesem neuen Endpunkttyp müssen Sie keinen Network Load Balancer (NLB) mehr verwenden, um Elastic IP-Adressen mit dem Endpunkt Ihres Servers zu verknüpfen. Sie können auch VPC-Sicherheitsgruppen verwenden, um den Zugriff auf den Endpunkt Ihres Servers einzuschränken. Sie können den `VPC_ENDPOINT` Endpunkttyp jedoch weiterhin nach Bedarf verwenden.

Beim folgenden Verfahren wird davon ausgegangen, dass Sie über einen Server verfügen, der entweder den aktuellen öffentlichen Endpunkttyp oder den älteren VPC_ENDPOINT Typ verwendet.

Um den Endpunkttyp für Ihren Server zu ändern

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Aktivieren Sie das Kontrollkästchen des Servers, für den Sie den Endpunkttyp ändern möchten.

 Important

Sie müssen den Server anhalten, bevor Sie dessen Endpunkttyp ändern können.

4. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp).
5. Wählen Sie im daraufhin angezeigten Bestätigungsdialogfeld die Option Stopp aus, um zu bestätigen, dass Sie den Server beenden möchten.

 Note

Bevor Sie mit dem nächsten Schritt fortfahren, warten Sie unter Endpunktdetails, bis sich der Status des Servers in Offline ändert. Dies kann einige Minuten dauern. Möglicherweise müssen Sie auf der Seite Server die Option Aktualisieren auswählen, um die Statusänderung zu sehen.

Sie können keine Änderungen vornehmen, bis der Server offline ist.

6. Wählen Sie unter Endpunktdetails die Option Bearbeiten aus.
7. Gehen Sie unter Endpunktkonfiguration bearbeiten wie folgt vor:
 - a. Wählen Sie für Endpunkttyp bearbeiten die Option VPC hosted aus.
 - b. Wählen Sie für Access eine der folgenden Optionen aus:
 - Intern, um Ihren Endpunkt nur für Clients zugänglich zu machen, die die privaten IP-Adressen des Endpunkts verwenden.
 - Internet Facing, um Ihren Endpunkt für Kunden über das öffentliche Internet zugänglich zu machen.

 Note

Wenn Sie sich für Internet Facing entscheiden, können Sie in jedem Subnetz oder Subnetzen eine bestehende Elastic IP-Adresse auswählen. Oder Sie können die VPC-Konsole (<https://console.aws.amazon.com/vpc/>) aufrufen, um eine oder mehrere neue Elastic IP-Adressen zuzuweisen. Diese Adressen können entweder Ihnen AWS oder Ihnen gehören. Sie können Elastic IP-Adressen, die bereits verwendet werden, nicht mit Ihrem Endpunkt verknüpfen.

- c. (Optional nur für Internetzugriff) Wählen Sie für Benutzerdefinierter Hostname eine der folgenden Optionen:
- Amazon Route 53 DNS-Alias — wenn der Hostname, den Sie verwenden möchten, bei Route 53 registriert ist. Sie können dann den Hostnamen eingeben.
 - Anderes DNS — wenn der Hostname, den Sie verwenden möchten, bei einem anderen DNS-Anbieter registriert ist. Sie können dann den Hostnamen eingeben.
 - Keine — um den Endpunkt des Servers zu verwenden und keinen benutzerdefinierten Hostnamen zu verwenden. Der Server-Host-Name hat das Format `serverId.server.transfer.regionId.amazonaws.com`.
- Weitere Informationen zum Arbeiten mit benutzerdefinierten Hostnamen finden Sie unter [Mit benutzerdefinierten Hostnamen arbeiten](#).
- d. Wählen Sie für VPC eine vorhandene VPC-ID aus, oder wählen Sie Create a VPC, um eine neue VPC zu erstellen.
- e. Wählen Sie im Abschnitt Availability Zones bis zu drei Availability Zones und zugehörige Subnetze aus. Wenn Internet Facing ausgewählt ist, wählen Sie auch eine Elastic IP-Adresse für jedes Subnetz aus.

 Note

Wenn Sie maximal drei Availability Zones wünschen, aber nicht genügend verfügbar sind, erstellen Sie sie in der VPC-Konsole (<https://console.aws.amazon.com/vpc/>). Wenn Sie die Subnetze oder Elastic IP-Adressen ändern, dauert die Aktualisierung des Servers einige Minuten. Sie können Ihre Änderungen erst speichern, wenn das Server-Update abgeschlossen ist.

- f. Wählen Sie Speichern.
8. Wählen Sie unter Aktionen die Option Start und warten Sie, bis sich der Status des Servers auf Online ändert. Dies kann einige Minuten dauern.

 Note

Wenn Sie einen öffentlichen Endpunkttyp in einen VPC-Endpunkttyp geändert haben, beachten Sie, dass der Endpunkttyp für Ihren Server in VPC geändert wurde.

Die Standardsicherheitsgruppe ist an den Endpunkt angehängt. Informationen zum Ändern oder Hinzufügen zusätzlicher Sicherheitsgruppen finden Sie unter [Sicherheitsgruppen erstellen](#).

Einstellung der Verwendung von VPC_ENDPOINT

AWS Transfer Family hat die Möglichkeit, Server `EndpointType=VPC_ENDPOINT` für neue AWS Konten zu erstellen, eingestellt. Ab dem 19. Mai 2021 können AWS Konten, die keine AWS Transfer Family Server mit dem Endpunkttyp von `VPC_ENDPOINT` besitzen, keine neuen Server mit `createEndpointType=VPC_ENDPOINT` erstellen. Wenn Sie bereits Server besitzen, die den `VPC_ENDPOINT` Endpunkttyp verwenden, empfehlen wir Ihnen, `EndpointType=VPC` so bald wie möglich mit der Nutzung zu beginnen. Einzelheiten finden Sie unter [Aktualisieren Sie Ihren AWS Transfer Family Serverendpunkttyp von VPC_ENDPOINT auf VPC](#).

Wir haben den neuen VPC Endpunkttyp Anfang 2020 eingeführt. Weitere Informationen finden Sie unter [AWS Transfer Family Für SFTP werden VPC-Sicherheitsgruppen und Elastic IP-Adressen unterstützt](#). Dieser neue Endpunkt bietet mehr Funktionen und ist kostengünstiger und es fallen keine PrivateLink Gebühren an. Weitere Informationen finden Sie unter [AWS PrivateLink Preise](#).

Dieser Endpunkttyp entspricht funktionell dem vorherigen Endpunkttyp (`VPC_ENDPOINT`). Sie können Elastic IP-Adressen direkt an den Endpunkt anhängen, um ihn mit dem Internet zu verbinden, und Sicherheitsgruppen für die Quell-IP-Filterung verwenden. Weitere Informationen finden Sie im Blogbeitrag [Use IP Allow List to secure your AWS Transfer Family for SFTP servers](#).

Sie können diesen Endpunkt auch in einer gemeinsam genutzten VPC-Umgebung hosten. Weitere Informationen finden Sie unter [Unterstützt AWS Transfer Family jetzt Shared Services-VPC-Umgebungen](#).

Zusätzlich zu SFTP können Sie die VPC verwenden, um FTPS und FTP `EndpointType` zu aktivieren. Wir haben nicht vor, diese Funktionen und FTPS/FTP diese Unterstützung hinzuzufügen.

EndpointType=VPC_ENDPOINT Wir haben diesen Endpunkttyp auch als Option aus der AWS Transfer Family Konsole entfernt.

Sie können den Endpunkttyp für Ihren Server mithilfe der Transfer Family Family-Konsole AWS CLI, API, SDKs oder CloudFormation ändern. Informationen zum Ändern des Endpunkt-Typs Ihres Servers finden Sie unter [Aktualisierung des AWS Transfer Family Serverendpunkttyps von VPC_ENDPOINT auf VPC](#).

Wenn Sie Fragen haben, wenden Sie sich an AWS Support Ihr AWS Account-Team.

 Note

Wir haben nicht vor, diese Funktionen und FTPS- oder FTP-Unterstützung zu EndpointType =VPC_ENDPOINT hinzuzufügen. Wir bieten es nicht mehr als Option auf der Konsole an.
AWS Transfer Family

Wenn du weitere Fragen hast, kannst du uns über AWS Support oder dein Account-Team kontaktieren.

Beschränkung des VPC-Endpunktzugriffs für Transfer Family Family-Server

Wenn Sie einen AWS Transfer Family Server mit VPC-Endpunkttyp erstellen, benötigen Ihre IAM-Benutzer und -Prinzipale Berechtigungen zum Erstellen und Löschen von VPC-Endpoints. Die Sicherheitsrichtlinien Ihrer Organisation können diese Berechtigungen jedoch einschränken. Sie können IAM-Richtlinien verwenden, um das Erstellen und Löschen von VPC-Endpunkten speziell für Transfer Family zu ermöglichen und gleichzeitig Einschränkungen für andere Dienste beizubehalten.

 Important

Die folgende IAM-Richtlinie ermöglicht es Benutzern, VPC-Endpunkte nur für Transfer Family Family-Server zu erstellen und zu löschen, während diese Vorgänge für andere Dienste verweigert werden:

```
{  
  "Effect": "Deny",  
  "Action": [
```

```

        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
    ],
    "Resource": ["*"],
    "Condition": {
        "ForAnyValue:StringNotLike": {
            "ec2:VpceServiceName": [
                "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
            ]
        },
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
            ]
        }
    }
}

```

INPUT-YOUR-REGION Ersetzen Sie es durch Ihre AWS Region (z. B. **us-east-1**) und *INPUT-YOUR-ROLE* durch die IAM-Rolle, der Sie diese Berechtigungen gewähren möchten.

Zusätzliche Netzwerkfunktionen

AWS Transfer Family bietet mehrere erweiterte Netzwerkfunktionen, die die Sicherheit und Flexibilität bei der Verwendung von VPC-Konfigurationen verbessern:

- Unterstützung für gemeinsam genutzte VPC-Umgebungen — Sie können Ihren Transfer Family Family-Serverendpunkt in einer gemeinsam genutzten VPC-Umgebung hosten. Weitere Informationen finden Sie unter [Verwenden von VPC-gehosteten Endpunkten in gemeinsam genutzten VPCs](#) mit AWS Transfer Family
- Authentifizierung und Sicherheit — Sie können eine AWS Web Application Firewall verwenden, um Ihren Amazon API Gateway Gateway-Endpunkt zu schützen. Weitere Informationen finden Sie unter [Absichern AWS Transfer Family mit AWS Web Application Firewall und Amazon API Gateway](#).

Aktualisierung des AWS Transfer Family Serverendpunkttyps von VPC_ENDPOINT auf VPC

Sie können die AWS-Managementkonsole CloudFormation, oder die Transfer Family Family-API verwenden, um die Daten EndpointType von bis eines Servers VPC_ENDPOINT zu

aktualisieren VPC. In den folgenden Abschnitten finden Sie detaillierte Verfahren und Beispiele für die Verwendung jeder dieser Methoden zur Aktualisierung eines Serverendpunkttyps. Wenn Sie Server in mehreren AWS Regionen und in mehreren AWS Konten haben, können Sie das Beispielskript im folgenden Abschnitt mit Änderungen verwenden, um Server zu identifizieren, die den VPC_ENDPOINT Typ verwenden, den Sie aktualisieren müssen.

Themen

- [Identifizieren von Servern anhand des VPC_ENDPOINT Endpunkttyps](#)
- [Aktualisierung des Serverendpunkt-Typs mit dem AWS-Managementkonsole](#)
- [Aktualisieren Sie den Serverendpunkttyp mit CloudFormation](#)
- [Den Server EndpointType mithilfe der API aktualisieren](#)

Identifizieren von Servern anhand des **VPC_ENDPOINT** Endpunkttyps

Mithilfe von können Sie feststellen, welche Server das VPC_ENDPOINT verwenden AWS-Managementkonsole.

Um Server zu identifizieren, die den **VPC_ENDPOINT** Endpunkttyp mithilfe der Konsole verwenden

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im Navigationsbereich Server aus, um die Liste der Server in Ihrem Konto in dieser Region anzuzeigen.
3. Sortieren Sie die Liste der Server nach dem Endpunkttyp, um zu sehen, dass alle Server diese verwenden VPC_ENDPOINT.

Um Server zu identifizieren, die mehrere **VPC_ENDPOINT** AWS Regionen und Konten verwenden

Wenn Sie Server in mehreren AWS Regionen und in mehreren AWS Konten haben, können Sie das folgende Beispielskript mit Änderungen verwenden, um Server zu identifizieren, die den VPC_ENDPOINT Endpunkttyp verwenden. Das Beispielskript verwendet die [ListServers](#) API-Operationen Amazon EC2 [DescribeRegions](#) und Transfer Family. Wenn Sie viele AWS Konten haben, können Sie Ihre Konten mithilfe einer IAM-Rolle mit schreibgeschütztem Auditor-Zugriff durchgehen, wenn Sie sich mithilfe von Sitzungsprofilen bei Ihrem Identitätsanbieter authentifizieren.

1. Im Folgenden finden Sie ein einfaches Beispiel.

```
import boto3
```



```
profile = input("Enter the name of the AWS account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()

for region in regions['Regions']:
    region_name = region['RegionName']
    if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
        continue
    transfer = session.client("transfer", region_name=region_name)
    servers = transfer.list_servers()
    for server in servers['Servers']:
        if server['EndpointType']=='VPC_ENDPOINT':
            print(server['ServerId'], region_name)
```

2. Nachdem Sie die Liste der zu aktualisierenden Server erstellt haben, können Sie eine der in den folgenden Abschnitten beschriebenen Methoden verwenden, um den Server EndpointType zu aktualisierenVPC.

Aktualisierung des Serverendpoint-Typs mit dem AWS-Managementkonsole

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Aktivieren Sie das Kontrollkästchen des Servers, für den Sie den Endpunktyp ändern möchten.

Important

Sie müssen den Server anhalten, bevor Sie dessen Endpunktyp ändern können.

4. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp).
5. Wählen Sie im daraufhin angezeigten Bestätigungsdiaologfeld die Option Stopp aus, um zu bestätigen, dass Sie den Server beenden möchten.

Note

Bevor Sie mit dem nächsten Schritt fortfahren, warten Sie, bis sich der Status des Servers auf Offline ändert. Dies kann einige Minuten dauern. Möglicherweise müssen

Sie auf der Seite Server die Option Aktualisieren auswählen, um die Statusänderung zu sehen.

6. Nachdem sich der Status auf Offline geändert hat, wählen Sie den Server aus, auf dem die Serverdetailseite angezeigt werden soll.
7. Wählen Sie im Abschnitt Endpunktdetails die Option Bearbeiten aus.
8. Wählen Sie VPC Hosted für den Endpoint-Typ aus.
9. Wählen Sie Speichern aus.
10. Wählen Sie für Aktionen die Option Start und warten Sie, bis sich der Status des Servers auf Online ändert. Dies kann einige Minuten dauern.

Aktualisieren Sie den Serverendpunkttyp mit CloudFormation

In diesem Abschnitt wird beschrieben, wie CloudFormation Sie das auf einem Server aktualisieren EndpointType könnenVPC. Verwenden Sie dieses Verfahren für Transfer Family Family-Server, mit denen Sie bereitgestellt haben CloudFormation. In diesem Beispiel wird die ursprüngliche CloudFormation Vorlage, die für die Bereitstellung des Transfer Family Family-Servers verwendet wurde, wie folgt dargestellt:

```
AWS::TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
```

```

VPCEndpoint:
  Type: AWS::EC2::VPCEndpoint
  Properties:
    ServiceName: com.amazonaws.us-east-1.transfer.server
    SecurityGroupIds:
      - !Ref SecurityGroupId
    SubnetIds:
      - !Select [0, !Ref SubnetIds]
      - !Select [1, !Ref SubnetIds]
      - !Select [2, !Ref SubnetIds]
    VpcEndpointType: Interface
    VpcId: !Ref VpcId

```

Die Vorlage wurde mit den folgenden Änderungen aktualisiert:

- Das EndpointType wurde geändert in VPC.
- Die AWS::EC2::VPCEndpoint Ressource wurde entfernt.
- Die SecurityGroupIdSubnetIds, und VpcId wurden in den EndpointDetails Abschnitt der AWS::Transfer::Server Ressource verschoben,
- Die VpcEndpointId Eigenschaft von EndpointDetails wurde entfernt.

Die aktualisierte Vorlage sieht wie folgt aus:

```

AWS::TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:

```

```
- !Select [0, !Ref SubnetIds]
- !Select [1, !Ref SubnetIds]
- !Select [2, !Ref SubnetIds]
VpcId: !Ref VpcId
EndpointType: VPC
IdentityProviderType: SERVICE_MANAGED
Protocols:
  - SFTP
```

Um den Endpunkttyp von Transfer Family Family-Servern zu aktualisieren, die bereitgestellt werden mit CloudFormation

1. Stoppen Sie den Server, den Sie aktualisieren möchten, indem Sie die folgenden Schritte ausführen.
 - a. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
 - b. Klicken Sie im Navigationsbereich auf Servers (Server).
 - c. Aktivieren Sie das Kontrollkästchen des Servers, für den Sie den Endpunkttyp ändern möchten.

 Important

Sie müssen den Server anhalten, bevor Sie dessen Endpunkttyp ändern können.

- d. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp).
- e. Wählen Sie im daraufhin angezeigten Bestätigungsdialogfeld die Option Stopp aus, um zu bestätigen, dass Sie den Server beenden möchten.

 Note

Bevor Sie mit dem nächsten Schritt fortfahren, warten Sie, bis sich der Status des Servers auf Offline ändert. Dies kann einige Minuten dauern. Möglicherweise müssen Sie auf der Seite Server die Option Aktualisieren auswählen, um die Statusänderung zu sehen.

2. Aktualisieren Sie den CloudFormation Stack

- a. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
- b. Wählen Sie den Stack aus, der zur Erstellung des Transfer Family Family-Servers verwendet wurde.
- c. Wählen Sie Aktualisieren aus.
- d. Wählen Sie Aktuelle Vorlage ersetzen
- e. Laden Sie die neue Vorlage hoch. CloudFormation Mithilfe von Änderungssätzen können Sie verstehen, wie sich Vorlagenänderungen auf laufende Ressourcen auswirken, bevor Sie sie implementieren. In diesem Beispiel wird die Transfer-Serverressource geändert und die VPCEndpoint-Ressource wird entfernt. Der VPC-Endpunktserver erstellt in Ihrem Namen einen VPC-Endpunkt und ersetzt die ursprüngliche VPCEndpoint Ressource.

Nach dem Hochladen der neuen Vorlage sieht der Änderungssatz etwa wie folgt aus:

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 🔗	AWS::EC2::VPCEndpoint	-

- f. Aktualisieren Sie den Stack.
3. Sobald das Stack-Update abgeschlossen ist, navigieren Sie zur Transfer Family Family-Verwaltungskontrolle unter <https://console.aws.amazon.com/transfer/>.
 4. Starten Sie den Server neu. Wählen Sie den Server aus, auf dem Sie aktualisiert haben CloudFormation, und wählen Sie dann im Menü Aktionen die Option Start.

Den Server EndpointType mithilfe der API aktualisieren

Sie können den Befehl [describe-server](#) oder den AWS CLI [UpdateServer](#) API-Befehl verwenden. Das folgende Beispielskript stoppt den Transfer Family Family-Server, aktualisiert den EndpointType, entfernt den VPC_ENDPOINT und startet den Server.

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
    ['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
            group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
```

```
delete_vpc_endpoint =  
ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
```

Mit benutzerdefinierten Hostnamen arbeiten

Ihr Server-Hostname ist der Hostname, den Ihre Benutzer in ihren Clients eingeben, wenn sie eine Verbindung zu Ihrem Server herstellen. Sie können eine benutzerdefinierte Domain verwenden, die Sie für Ihren Server-Hostnamen registriert haben, wenn Sie damit arbeiten. AWS Transfer Family Sie könnten beispielsweise einen benutzerdefinierten Hostnamen wie verwenden. `mysftpserver.mysubdomain.domain.com`

Um Traffic von Ihrer registrierten benutzerdefinierten Domain zu Ihrem Serverendpunkt umzuleiten, können Sie Amazon Route 53 oder einen beliebigen Domain Name System (DNS) -Anbieter verwenden. Route 53 ist der DNS-Dienst, der AWS Transfer Family nativ unterstützt wird.

Themen

- [Verwenden Sie Amazon Route 53 als Ihren DNS-Anbieter](#)
- [Verwenden Sie andere DNS-Anbieter](#)
- [Benutzerdefinierte Hostnamen für Server, die nicht von der Konsole erstellt wurden](#)

Auf der Konsole können Sie eine der folgenden Optionen für die Einrichtung eines benutzerdefinierten Hostnamens wählen:

- Amazon Route 53 DNS-Alias — wenn der Hostname, den Sie verwenden möchten, bei Route 53 registriert ist. Sie können dann den Hostnamen eingeben.
- Anderes DNS — wenn der Hostname, den Sie verwenden möchten, bei einem anderen DNS-Anbieter registriert ist. Sie können dann den Hostnamen eingeben.
- Keine — um den Endpunkt des Servers zu verwenden und keinen benutzerdefinierten Hostnamen zu verwenden.

Sie legen diese Option fest, wenn Sie einen neuen Server erstellen oder die Konfiguration eines vorhandenen Servers bearbeiten. Weitere Hinweise zum Erstellen eines neuen Servers finden Sie unter [Schritt 2: Einen SFTP-enabled Server erstellen](#). Weitere Hinweise zum Bearbeiten der Konfiguration eines vorhandenen Servers finden Sie unter [Serverdetails bearbeiten](#).

Weitere Informationen zur Verwendung Ihrer eigenen Domain für den Server-Hostnamen und zur Verwendung AWS Transfer Family von Route 53 finden Sie in den folgenden Abschnitten.

Verwenden Sie Amazon Route 53 als Ihren DNS-Anbieter

Wenn Sie einen Server erstellen, können Sie Amazon Route 53 als Ihren DNS-Anbieter verwenden. Bevor Sie eine Domain mit Route 53 verwenden, registrieren Sie die Domain. Weitere Informationen finden Sie unter [So funktioniert die Domainregistrierung](#) im Amazon Route 53-Entwicklerhandbuch.

Wenn Sie Route 53 verwenden, um DNS-Routing für Ihren Server bereitzustellen, AWS Transfer Family verwendet es den benutzerdefinierten Hostnamen, den Sie eingegeben haben, um die Hosting-Zone zu extrahieren. Beim AWS Transfer Family Extrahieren einer Hosting-Zone können drei Dinge passieren:

1. Wenn Route 53 neu für Sie ist und Sie noch keine Hosting-Zone haben, AWS Transfer Family fügt Sie eine neue Hosting-Zone und einen CNAME Datensatz hinzu. Der Wert dieses CNAME Datensatzes ist der Endpunkt-Hostname für Ihren Server. Ein CNAME ist ein alternativer Domänenname.
2. Wenn Sie eine gehostete Zone in Route 53 ohne CNAME Datensätze haben, AWS Transfer Family fügt der Hosting-Zone einen CNAME Datensatz hinzu.
3. Wenn der Service erkennt, dass bereits ein CNAME-Datensatz in der gehosteten Zone vorhanden ist, wird Ihnen eine Fehlermeldung angezeigt, der angibt, dass bereits ein CNAME-Datensatz vorhanden ist. Ändern Sie in diesem Fall den Wert des CNAME Datensatzes in den Hostnamen Ihres Servers.

Weitere Informationen zu gehosteten Zonen in Route 53 finden Sie unter [Gehostete Zone](#) im Amazon Route 53 Developer Guide.

Verwenden Sie andere DNS-Anbieter

Wenn Sie einen Server erstellen, können Sie auch andere DNS-Anbieter als Amazon Route 53 verwenden. Wenn Sie einen alternativen DNS-Anbieter verwenden, müssen Sie sicherstellen, dass der Datenverkehr aus Ihrer Domäne zum -Server-Endpunkt geleitet wird.

Stellen Sie dazu Ihre Domain auf den Endpunkt-Hostnamen für den Server ein.

- Für IPv4-Endpunkte sieht der Hostname in der Konsole wie folgt aus:

`serverid.server.transfer.region.amazonaws.com`

- Für Dual-Stack-Endpunkte sieht der Hostname in der Konsole wie folgt aus:

`serverid.transfer-server.region.on.aws`

 Note

Wenn Ihr Server über einen VPC-Endpunkt verfügt, unterscheidet sich das Format für den Hostnamen von den oben beschriebenen. Um Ihren VPC-Endpunkt zu finden, wählen Sie die VPC auf der Detailseite des Servers und dann die VPC-Endpunkt-ID im VPC-Dashboard aus. Der Endpunkt ist der erste DNS-Name der aufgelisteten Namen.

Benutzerdefinierte Hostnamen für Server, die nicht von der Konsole erstellt wurden

Wenn Sie einen Server mit AWS Cloud Development Kit (AWS CDK) CloudFormation, oder über die CLI erstellen, müssen Sie ein Tag hinzufügen, wenn dieser Server einen benutzerdefinierten Hostnamen haben soll. Wenn Sie mithilfe der Konsole einen Transfer Family Family-Server erstellen, erfolgt das Tagging automatisch.

 Note

Sie müssen auch einen DNS-Eintrag erstellen, um den Verkehr von Ihrer Domain zu Ihrem Serverendpunkt umzuleiten. Einzelheiten finden Sie unter [Arbeiten mit Datensätzen](#) im Amazon Route 53-Entwicklerhandbuch.

Verwenden Sie die folgenden Schlüssel für Ihren benutzerdefinierten Hostnamen:

- Fügen Sie `hinzutransfer:customHostname`, um den benutzerdefinierten Hostnamen in der Konsole anzuzeigen.
- Wenn Sie Route 53 als Ihren DNS-Anbieter verwenden, fügen Sie `hinzutransfer:route53HostedZoneId`. Dieses Tag verknüpft den benutzerdefinierten Hostnamen mit Ihrer Route 53 Hosted Zone ID.

Geben Sie den folgenden CLI-Befehl ein, um den benutzerdefinierten Hostnamen hinzuzufügen.

```
aws transfer tag-resource --arn arn:aws:transfer:region:AWS-Konto:server/server-ID --  
tags Key=transfer:customHostname,Value="custom-host-name"
```

Beispiel:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Wenn Sie Route 53 verwenden, geben Sie den folgenden Befehl ein, um Ihren benutzerdefinierten Hostnamen mit Ihrer Route 53 Hosted Zone ID zu verknüpfen.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

Beispiel:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

Gehen Sie von den Beispielwerten aus dem vorherigen Befehl aus und führen Sie den folgenden Befehl aus, um Ihre Tags anzuzeigen:

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-
east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [
  {
    "Key": "transfer:route53HostedZoneId",
    "Value": "/hostedzone/ABCDE1111222233334444"
  },
  {
    "Key": "transfer:customHostname",
    "Value": "abc.example.com"
  }
]
```

 Note

Ihre öffentlichen, gehosteten Zonen und ihre IDs sind auf Amazon Route 53 verfügbar. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter <https://console.aws.amazon.com/route53/>.

Überlegungen zum FTP- und FTPS-Network Load Balancer

Wir empfehlen zwar, Network Load Balancer vor AWS Transfer Family Servern zu vermeiden, aber wenn Ihre FTP- oder FTPS-Implementierung eine NLB- oder NAT-Verbindung in der Kommunikationsroute vom Client erfordert, sollten Sie die folgenden Empfehlungen beachten:

- Verwenden Sie für einen NLB Port 21 für Integritätsprüfungen anstelle der Ports 8192-8200.
- Aktivieren Sie für den AWS Transfer Family Server die Wiederaufnahme der TLS-Sitzung durch Einstellung. `TlsSessionResumptionMode = ENFORCED`

Note

Dies ist der empfohlene Modus, da er erhöhte Sicherheit bietet:

- Erfordert, dass Clients die TLS-Sitzungswiederaufnahme für nachfolgende Verbindungen verwenden.
 - Bietet stärkere Sicherheitsgarantien, indem konsistente Verschlüsselungsparameter gewährleistet werden.
 - Hilft, potenzielle Downgrade-Angriffe zu verhindern.
 - Sorgt für die Einhaltung der Sicherheitsstandards und optimiert gleichzeitig die Leistung.
- Wenn möglich, sollten Sie auf die Verwendung eines NLB verzichten, um die AWS Transfer Family Leistungs- und Verbindungslimits voll auszunutzen.

Wenn Sie weitere Informationen zu NLB-Alternativen benötigen, wenden Sie sich über den AWS Support an das AWS Transfer Family Produktmanagementteam. Weitere Informationen zur Verbesserung Ihres Sicherheitsstatus finden Sie im Blogbeitrag [Sechs Tipps zur Verbesserung der Sicherheit Ihres AWS Transfer Family Servers](#).

Sicherheitsrichtlinien für NLBs finden Sie unter. [Vermeiden Sie es, AWS Transfer Family NLBs und NATs vor Servern zu platzieren](#)

Übertragung von Dateien über einen Serverendpunkt mit einem Client

Sie übertragen Dateien über den AWS Transfer Family Dienst, indem Sie den Übertragungsvorgang in einem Client angeben. AWS Transfer Family unterstützt die folgenden Clients:

- Wir unterstützen Version 3 des SFTP-Protokolls.
- OpenSSH (macOS und Linux)

 Note

Dieser Client funktioniert nur mit Servern, die für Secure Shell (SSH) File Transfer Protocol (SFTP) aktiviert sind.

- WinSCP (nur Microsoft Windows)
- Cyberduck (Windows, macOS und Linux)
- FileZilla (Windows, macOS und Linux)

Die folgenden Einschränkungen gelten für jeden Client:

- Das SCP-Protokoll wird nicht unterstützt, da es als unsicher gilt. Sie können den scp OpenSSH-Befehl wie unter beschrieben verwenden. [Verwenden Sie den Befehl scp](#)
- Die maximale Anzahl gleichzeitiger, gemultiplexer SFTP-Sitzungen pro Verbindung beträgt 10.
- Bei Verbindungen im Leerlauf beträgt der Timeout-Wert 1800 Sekunden (30 Minuten) für alle Protokolle (). SFTP/FTP/FTPS Wenn nach diesem Zeitraum keine Aktivität mehr stattfindet, wird die Verbindung zum Client möglicherweise unterbrochen. Bei Verbindungen, die nicht reagieren:
 - SFTP hat einen Timeout von 300 Sekunden (5 Minuten), wenn ein Client überhaupt nicht reagiert.
 - FTPS und FTP haben ein Zeitlimit von etwa 10 Minuten, das von der zugrunde liegenden Bibliothek verarbeitet wird.
- Amazon S3 und Amazon EFS (aufgrund des NFSv4-Protokolls) erfordern, dass Dateinamen verschlüsselt sind. UTF-8 Die Verwendung einer anderen Kodierung kann zu unerwarteten Ergebnissen führen. Informationen zu Amazon S3 finden Sie unter [Richtlinien zur Benennung von Objektschlüsseln](#).
- Für das File Transfer Protocol over SSL (FTPS) wird nur der Modus Explizit unterstützt. Der implizite Modus wird nicht unterstützt.
- Für File Transfer Protocol (FTP) und FTPS wird nur der passive Modus unterstützt.
- Für FTP und FTPS wird nur der STREAM-Modus unterstützt.
- Für FTP und FTPS wird nur der Image/Binary Modus unterstützt.

- Für FTP und FTPS ist TLS — PROT C (ungeschützt) TLS für die Datenverbindung die Standardeinstellung, aber PROT C wird im FTPS-Protokoll nicht unterstützt. AWS Transfer Family Für FTPS müssen Sie also PROT P ausgeben, damit Ihr Datenvorgang akzeptiert wird.
- Wenn Sie Amazon S3 für den Speicher Ihres Servers verwenden und Ihr Client die Option enthält, mehrere Verbindungen für eine einzelne Übertragung zu verwenden, stellen Sie sicher, dass Sie die Option deaktivieren. Andernfalls können große Datei-Uploads auf unvorhersehbare Weise fehlschlagen. Beachten Sie, dass EFS mehrere Verbindungen für eine einzige Übertragung unterstützt, wenn Sie Amazon EFS als Speicher-Backend verwenden.

Im Folgenden finden Sie eine Liste der verfügbaren Befehle für FTP und FTPS:

Verfügbare Befehle					
ARBEIT	KUNSTSTÜCK	AM MEISTEN	PASS	RETR	GESCHICHTE
AUTHENTIFIZIEREN	LANG	MKD	PASV	RMD	STOU
CUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	HAFEN	ENTO	SYSTEM
DELE	MFMT	NEIN	PWD	SIZE	TYPE
EPSV	MLSD	WÄHLT	QUIT	STAT	USER

Note

APPE wird nicht unterstützt.

Für SFTP werden die folgenden Operationen derzeit nicht für Benutzer unterstützt, die das logische Home-Verzeichnis auf Servern verwenden, die Amazon Elastic File System (Amazon EFS) verwenden.

SFTP-Befehle werden nicht unterstützt

SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT, wenn die angeforderte Datei ein Symlink ist	SSH_FXP_R EALPATH, wenn der angeforderte Pfad irgendeine Symlink-Komponente n enthält

Generieren Sie ein öffentlich-privates key pair

Bevor Sie eine Datei übertragen können, müssen Sie über ein öffentlich-privates key pair verfügen. Wenn Sie noch kein key pair generiert haben, finden Sie weitere Informationen unter [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).

Themen

- [Verfügbare SFTP/FTPS/FTP Befehle](#)
- [Finden Sie Ihren Amazon VPC-Endpunkt](#)
- [Vermeiden Sie Fehler setstat](#)
- [OpenSSH verwenden](#)
- [Verwenden Sie WinSCP](#)
- [Verwenden Sie Cyberduck](#)
- [Verwenden Sie FileZilla](#)
- [Verwenden Sie einen Perl-Client](#)
- [Verwenden Sie LFTP](#)
- [Verarbeitung nach dem Upload](#)
- [SFTP-Nachrichten](#)

Verfügbare SFTP/FTPS/FTP Befehle

In der folgenden Tabelle werden die verfügbaren Befehle für AWS Transfer Family die Protokolle SFTP, FTPS und FTP beschrieben.

Note

In der Tabelle werden Dateien und Verzeichnisse für Amazon S3 aufgeführt, das nur Buckets und Objekte unterstützt: Es gibt keine Hierarchie. Sie können jedoch Präfixe in Objektschlüsselnamen verwenden, um eine Hierarchie zu implizieren und Ihre Daten ähnlich wie Ordner zu organisieren. Dieses Verhalten wird unter [Arbeiten mit Objektmetadaten](#) im Amazon Simple Storage Service-Benutzerhandbuch beschrieben.

SFTP/FTPS/FTP Befehle

Befehl	Amazon S3	Amazon EFS
cd	Unterstützt	Unterstützt
chgrp	Nicht unterstützt	Unterstützt (root oder owner nur)
chmod	Nicht unterstützt	Wird unterstützt (root nur)
chmtime	Nicht unterstützt	Unterstützt
chown	Nicht unterstützt	Wird unterstützt (root nur)
get	Unterstützt	Unterstützt (einschließlich der Auflösung symbolischer Links)
ln -s	Nicht unterstützt	Unterstützt
ls/dir	Unterstützt	Unterstützt
mkdir	Unterstützt	Unterstützt
put	Unterstützt	Unterstützt
pwd	Unterstützt	Unterstützt
rename	Wird nur für Dateien unterstützt	Unterstützt

Befehl	Amazon S3	Amazon EFS
	 Note Ein Umbenennen, das eine bestehende Datei überschreiben würde, wird nicht unterstützt.	 Note Ein Umbenennen, das eine bestehende Datei oder ein vorhandenes Verzeichnis überschreiben würde, wird nicht unterstützt.
<code>rm</code>	Unterstützt	Unterstützt
<code>rmdir</code>	Unterstützt (nur leere Verzeichnisse)	Unterstützt
<code>version</code>	Unterstützt	Unterstützt

Finden Sie Ihren Amazon VPC-Endpunkt

Wenn der Endpunkttyp für Ihren Transfer Family Family-Server VPC ist, ist es nicht einfach, den Endpunkt zu identifizieren, der für die Übertragung von Dateien verwendet werden soll. Gehen Sie in diesem Fall wie folgt vor, um Ihren Amazon VPC-Endpunkt zu finden.

So finden Sie Ihren Amazon VPC-Endpunkt

1. Navigieren Sie zur Detailseite Ihres Servers.
2. Wählen Sie im Bereich Endpunktdetails die VPC aus.

Endpoint details

Edit

Status	Online	Custom hostname	-
Endpoint type	VPC (vpce- [redacted] [link icon])	Endpoint	-
VPC	vpc- [redacted]	Access	Info
FIPS Enabled	No	Internal	

3. Wählen Sie im Amazon VPC-Dashboard die VPC-Endpoint-ID aus.
4. In der Liste der DNS-Namen ist Ihr Serverendpoint der erste, der aufgeführt ist.

VPC > Endpoints > vpce-[redacted]

vpce-[redacted] Actions ▼

Details

Endpoint ID	Status	Creation time	Endpoint type
vpce-[redacted]	Available	Monday, April 4, 2022 at 10:51:31 EDT	Interface
VPC ID	Status message	Service name	Private DNS names enabled
vpc-515e1d14 (no-name-specified)	-	com.amazonaws.us-east-2.transfer.server.c-0002	No
DNS record IP type	IP address type	DNS names	
ipv4	ipv4	vpce-[redacted] [redacted] [redacted].us-east-2 [redacted] [redacted] [redacted].us-east-	

Vermeiden Sie Fehler **setstat**

Einige SFTP-Dateiübertragungsclients können versuchen, die Attribute von Remotedateien, einschließlich Zeitstempel und Berechtigungen, mithilfe von Befehlen wie SETSTAT beim Hochladen der Datei zu ändern. Diese Befehle sind jedoch nicht mit Objekt-Speichersystemen wie Amazon S3 kompatibel. Aufgrund dieser Inkompatibilität können Datei-Uploads von diesen Clients zu Fehlern führen, selbst wenn die Datei anderweitig erfolgreich hochgeladen wurde.

- Verwenden Sie beim Aufrufen der UpdateServer API CreateServer oder die ProtocolDetails Option, um den Fehler SetStatOption zu ignorieren, der generiert wird, wenn der Client versucht, SETSTAT für eine Datei zu verwenden, die Sie in einen S3-Bucket hochladen.
- Setzen Sie den Wert auf ENABLE_NO_OP, damit der Transfer-Family-Server den SETSTAT-Befehl ignoriert und Dateien hochlädt, ohne Änderungen an Ihrem SFTP-Client vornehmen zu müssen.
- Beachten Sie, dass die SetStatOption ENABLE_NO_OP Einstellung zwar den Fehler ignoriert, aber einen Protokolleintrag in CloudWatch Logs generiert, sodass Sie feststellen können, wann der Client einen SETSTAT-Aufruf durchführt.

Die API-Details für diese Option finden Sie unter [ProtocolDetails](#)

OpenSSH verwenden

Dieser Abschnitt enthält Anweisungen zum Übertragen von Dateien über die Befehlszeile mit OpenSSH.

Note

Dieser Client funktioniert nur mit einem SFTP-enabled Server.

Themen

- [Verwenden von OpenSSH](#)
- [Verwenden Sie den Befehl scp](#)

Verwenden von OpenSSH

Um Dateien AWS Transfer Family mit dem OpenSSH-Befehlszeilenprogramm zu übertragen

1. Öffnen Sie unter Linux, macOS oder Windows ein Befehlsterminal.
2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
sftp -i transfer-key sftp_user@service_endpoint
```

Im vorherigen Befehl *sftp_user* ist dies der Benutzername und *transfer-key* der private SSH-Schlüssel. Hier *service_endpoint* ist der Endpunkt des Servers, wie er in der AWS Transfer Family Konsole für den ausgewählten Server angezeigt wird.

Note

Dieser Befehl verwendet Einstellungen, die in der `ssh_config` Standarddatei enthalten sind. Sofern Sie diese Datei nicht zuvor bearbeitet haben, verwendet SFTP Port 22. Sie können einen anderen Port angeben (z. B. 2222), indem Sie dem Befehl wie folgt ein **-P** Flag hinzufügen.

```
sftp -P 2222 -i transfer-key sftp_user@service_endpoint
```

Wenn Sie immer Port 2222 oder Port 22000 verwenden möchten, können Sie alternativ Ihren Standardport in Ihrer Datei aktualisieren. `ssh_config`

Eine `sftp`-Eingabeaufforderung sollte angezeigt werden.

3. (Optional) Um das Home-Verzeichnis des Benutzers anzuzeigen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `sftp`

```
pwd
```

4. Verwenden Sie den `put` Befehl, um eine Datei von Ihrem Dateisystem auf den Transfer Family Family-Server hochzuladen. Um beispielsweise einen Upload durchzuführen `hello.txt` (vorausgesetzt, die Datei befindet sich in Ihrem aktuellen Verzeichnis auf Ihrem Dateisystem), führen Sie an der `sftp` Eingabeaufforderung den folgenden Befehl aus:

```
put hello.txt
```

Eine Meldung ähnlich der folgenden wird angezeigt, die darauf hinweist, dass die Dateiübertragung im Gange ist oder abgeschlossen ist.

```
Uploading hello.txt to /amzn-s3-demo-bucket/home/sftp_user/hello.txt  
hello.txt 100% 127 0.1KB/s 00:00
```

Note

Nachdem Ihr Server erstellt wurde, kann es einige Minuten dauern, bis der Hostname des Serverendpunkts vom DNS-Dienst in Ihrer Umgebung aufgelöst werden kann.

Verwenden Sie den Befehl **scp**

Transfer Family unterstützt das SCP-Protokoll nicht. Sie können jedoch den scp OpenSSH-Befehl verwenden, wenn Sie diese Funktionalität benötigen.

Die Empfehlung für die Verwendung von SCP über SFTP ist die Verwendung von OpenSSH Version 9.0 oder höher. In OpenSSH Version 9 und höher verwendet der scp Befehl standardmäßig das SFTP-Protokoll für Dateiübertragungen anstelle des alten SCP-Protokolls.

Important

Stellen Sie sicher, dass Ihr Transfer Family Family-Server für den S3-optimierten Verzeichniszugriff konfiguriert wurde.

Verwenden Sie WinSCP

Unten wird beschrieben, wie Dateien in der Befehlszeile mit WinSCP übertragen werden.

Note

Wenn Sie WinSCP 5.19 verwenden, können Sie mit Ihren AWS Anmeldeinformationen und Dateien direkt eine Verbindung zu Amazon S3 herstellen. `upload/download` Weitere Informationen finden Sie unter [Verbindung zum Amazon S3 S3-Service](#) herstellen.

Um Dateien AWS Transfer Family mit WinSCP zu übertragen

1. Öffnen Sie den WinSCP-Client.
2. Wählen Sie im Anmeldedialogfeld für Dateiprotokoll ein Protokoll aus: SFTP oder FTP.

Wenn Sie FTP für Verschlüsselung ausgewählt haben, wählen Sie eine der folgenden Optionen:

- Keine Verschlüsselung für FTP
 - TLS/SSL Explizite Verschlüsselung für FTPS
3. Geben Sie in das Feld Host name (Host-Name) den Server-Endpunkt ein. Der Serverendpunkt befindet sich auf der Seite mit den Serverdetails. Weitere Informationen finden Sie unter [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#).

Wenn Ihr Server einen VPC-Endpunkt verwendet, finden Sie weitere Informationen unter [Finden Sie Ihren Amazon VPC-Endpunkt](#).

4. Geben Sie als Portnummer Folgendes ein:
 - **22** für SFTP
 - **21** für FTP/FTPS
5. Geben Sie unter Benutzername den Namen für den Benutzer ein, den Sie für Ihren spezifischen Identity Provider erstellt haben.

Tipp: Der Benutzername sollte einer der Benutzer sein, die Sie für Ihren Identitätsanbieter erstellt oder konfiguriert haben. AWS Transfer Family bietet die folgenden Identitätsanbieter:

- [Arbeiten mit Benutzern, die vom Dienst verwaltet werden](#)
 - [Verwenden des AWS Directory Service für Microsoft Active Directory](#)
 - [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#)
6. Wählen Sie „Erweitert“, um das Dialogfeld „Erweiterte Seiteneinstellungen“ zu öffnen. Wählen Sie im Abschnitt SSH die Option Authentifizierung aus.
 7. Suchen Sie unter Datei mit privatem Schlüssel nach der privaten SSH-Schlüsseldatei aus Ihrem Dateisystem und wählen Sie sie aus.

Wenn WinSCP anbietet, Ihren privaten SSH-Schlüssel in das PPK-Format zu konvertieren, wählen Sie OK.

8. Wählen Sie OK aus, um zum Dialogfeld Login (Anmelden) zurückzukehren. Wählen Sie dann Save (Speichern) aus.

9. Wählen Sie im Dialogfeld Sitzung als Site speichern die Option OK, um die Verbindungseinrichtung abzuschließen.
10. Wählen Sie im Anmeldedialogfeld die Option Tools und anschließend Einstellungen aus.
11. Wählen Sie im Dialogfeld „Einstellungen“ für „Übertragung“ die Option „Endurance“.

Wählen Sie für die Option Übertragung resume/transfer an temporären Dateinamen aktivieren die Option Deaktivieren.

 Important

Wenn Sie diese Option aktiviert lassen, erhöht dies die Upload-Kosten und verringert die Upload-Leistung erheblich. Dies kann auch dazu führen, dass das Hochladen großer Dateien fehlschlägt.

12. Wählen Sie für Übertragung die Option Hintergrund und deaktivieren Sie das Kontrollkästchen Mehrere Verbindungen für eine einzige Übertragung verwenden.

Tipp: Wenn Sie diese Option aktiviert lassen, können große Datei-Uploads auf unvorhersehbare Weise fehlschlagen. Beispielsweise können verwaiste mehrteilige Uploads erstellt werden, für die Amazon S3 S3-Gebühren anfallen. Es kann auch zu einer unbemerkten Beschädigung von Daten kommen.

13. Führen Sie Ihre Dateiübertragung durch.

Sie können Drag-and-Drop-Methoden verwenden, um Dateien zwischen dem Ziel- und dem Quellfenster zu kopieren. Sie können die Symbolleisten Symbole verwenden, um die Eigenschaften von Dateien in WinSCP hochzuladen, herunterzuladen, zu löschen, zu bearbeiten oder zu ändern.

 Note

Dieser Hinweis gilt nicht, wenn Sie Amazon EFS als Speicher verwenden. Befehle, die versuchen, Attribute von Remote-Dateien, einschließlich Zeitstempeln, zu ändern, sind nicht mit Objektspeichersystemen wie Amazon S3 kompatibel. Wenn Sie Amazon S3 als Speicher verwenden, stellen Sie daher sicher, dass Sie die WinSCP-Zeitstempелеinstellungen deaktivieren (oder `SetStatOption` wie unter beschrieben verwenden [Vermeiden Sie Fehler `setstat`](#)), bevor Sie Dateiübertragungen durchführen.

Deaktivieren Sie dazu im Dialogfeld mit den WinSCP-Übertragungseinstellungen die Upload-Option Berechtigungen festlegen und die allgemeine Option Zeitstempel beibehalten.

Verwenden Sie Cyberduck

Unten wird beschrieben, wie Dateien in der Befehlszeile mit Cyberduck übertragen werden.

Um Dateien AWS Transfer Family mit Cyberduck zu übertragen

1. Öffnen Sie den [Cyberduck-Client](#).
2. Wählen Sie Verbindung öffnen.
3. Wählen Sie im Dialogfeld „Verbindung öffnen“ ein Protokoll aus: SFTP (SSH File Transfer Protocol), FTP-SSL(Explicit AUTH TLS) oder FTP (File Transfer Protocol).
4. Geben Sie unter Server Ihren Serverendpunkt ein. Der Serverendpunkt befindet sich auf der Seite mit den Serverdetails. Weitere Informationen finden Sie unter [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#).

Wenn Ihr Server einen VPC-Endpunkt verwendet, finden Sie weitere Informationen unter [Finden Sie Ihren Amazon VPC-Endpunkt](#).

5. Geben Sie als Portnummer Folgendes ein:
 - **22** für SFTP
 - **21** für FTP/FTPS
6. Geben Sie in das Feld Username (Benutzername) den Namen des Benutzers ein, den Sie in [Benutzer für Serverendpunkte verwalten](#) erstellt haben.
7. Wenn SFTP ausgewählt ist, wählen Sie für SSH Private Key den privaten SSH-Schlüssel aus oder geben Sie ihn ein.
8. Wählen Sie Connect aus.
9. Führen Sie Ihre Dateiübertragung durch.

Führen Sie nun – abhängig von der Position der Dateien – einen der folgenden Schritte durch:

- Wählen Sie in Ihrem lokalen Verzeichnis (der Quelle) die Dateien aus, die Sie übertragen möchten, und ziehen Sie sie per Drag & Drop in das Amazon S3 S3-Verzeichnis (das Ziel).
- Wählen Sie im Amazon S3 S3-Verzeichnis (der Quelle) die Dateien aus, die Sie übertragen möchten, und ziehen Sie sie per Drag & Drop in Ihr lokales Verzeichnis (das Ziel).

Verwenden Sie FileZilla

Verwenden Sie die folgenden Anweisungen, um Dateien mit zu übertragen FileZilla.

So richten Sie FileZilla eine Dateiübertragung ein

1. Öffnen Sie den FileZilla Client.
2. Wählen Sie „Datei“ und anschließend „Site-Manager“.
3. Wählen Sie im Dialogfeld „Site-Manager“ die Option „Neue Site“ aus.
4. Wählen Sie auf der Registerkarte Allgemein für Protokoll ein Protokoll aus: SFTP oder FTP.

Wenn Sie FTP für Verschlüsselung ausgewählt haben, wählen Sie eine der folgenden Optionen:

- Verwenden Sie nur einfaches FTP (unsicher) — für FTP
 - Verwenden Sie explizites FTP über TLS, falls verfügbar — für FTPS
5. Geben Sie als Hostname das Protokoll ein, das Sie verwenden, gefolgt von Ihrem Serverendpunkt. Der Serverendpunkt befindet sich auf der Seite mit den Serverdetails. Weitere Informationen finden Sie unter [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#).
 - Wenn Sie SFTP verwenden, geben Sie Folgendes ein: `sftp://hostname`
 - Wenn Sie FTPS verwenden, geben Sie Folgendes ein: `ftps://hostname`

Stellen Sie sicher, dass Sie es *hostname* durch Ihren tatsächlichen Serverendpunkt ersetzen.

Wenn Ihr Server einen VPC-Endpunkt verwendet, finden Sie weitere Informationen unter [Finden Sie Ihren Amazon VPC-Endpunkt](#).

6. Geben Sie als Portnummer Folgendes ein:
 - **22** für SFTP
 - **21** für FTP/FTPS
7. Wenn SFTP ausgewählt ist, wählen Sie als Anmeldetyp die Option Schlüsseldatei aus.

Wählen Sie unter Schlüsseldatei den privaten SSH-Schlüssel aus, oder geben Sie ihn ein.

8. Geben Sie unter Benutzer den Namen des Benutzers ein, den Sie erstellt haben. [Benutzer für Serverendpunkte verwalten](#)
9. Wählen Sie Connect aus.

10. Führen Sie Ihre Dateiübertragung durch.

Note

Wenn Sie eine laufende Dateiübertragung unterbrechen, wird AWS Transfer Family möglicherweise ein Teilobjekt in Ihren Amazon S3 S3-Bucket geschrieben. Wenn Sie einen Upload unterbrechen, überprüfen Sie, ob die Dateigröße im Amazon S3 S3-Bucket der Dateigröße des Quellobjekts entspricht, bevor Sie fortfahren.

Verwenden Sie einen Perl-Client

Wenn Sie den `Net::SFTP::Foreign` Perl-Client verwenden, müssen Sie den `queue_size` Wert auf setzen. 1 Beispiel:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

Note

[Diese Problemumgehung ist für Versionen Net::SFTP::Foreign vor 1.92.02 erforderlich.](#)

Verwenden Sie LFTP

LFTP ist ein kostenloser FTP-Client, mit dem Benutzer Dateiübertragungen über die Befehlszeilenschnittstelle von den meisten Linux-Computern aus durchführen können.

Bei großen Dateidownloads gibt es bei LFTP ein bekanntes Problem mit Paketen, die nicht in der richtigen Reihenfolge sind, wodurch die Dateiübertragung fehlschlägt.

Verarbeitung nach dem Upload

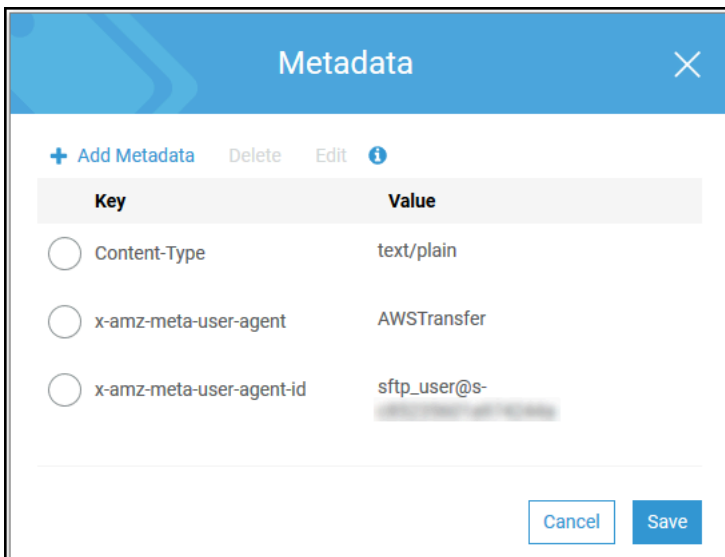
Sie können Verarbeitungsinformationen nach dem Upload anzeigen, einschließlich Amazon S3 S3-Objektmetadaten und Ereignisbenachrichtigungen.

Themen

- [Amazon S3 S3-Objektmetadaten](#)
- [Amazon-S3-Ereignis-Benachrichtigungen](#)

Amazon S3 S3-Objektmetadaten

Als Teil der Metadaten Ihres Objekts sehen Sie einen Schlüssel namens `x-amz-meta-user-agent` Wessen Wert ist `AWSTransfer` und `x-amz-meta-user-agent-id` Wessen Wert ist `username@server-id`. Der `username` ist der Transfer Family Family-Benutzer, der die Datei hochgeladen hat, und `server-id` ist der Server, der für den Upload verwendet wurde. Auf diese Informationen kann mithilfe der [HeadObject](#) Operation für das S3-Objekt in Ihrer Lambda-Funktion zugegriffen werden.



The screenshot shows the 'Metadata' window in the Amazon S3 console. It has a blue header with the title 'Metadata' and a close button. Below the header are three buttons: '+ Add Metadata', 'Delete', and 'Edit', followed by an information icon. A table displays the metadata for an object. The table has two columns: 'Key' and 'Value'. There are three rows of metadata, each with a radio button in the 'Key' column. The first row shows 'Content-Type' with the value 'text/plain'. The second row shows 'x-amz-meta-user-agent' with the value 'AWSTransfer'. The third row shows 'x-amz-meta-user-agent-id' with the value 'sftp_user@s-'. At the bottom right of the window are 'Cancel' and 'Save' buttons.

Key	Value
☐ Content-Type	text/plain
☐ x-amz-meta-user-agent	AWSTransfer
☐ x-amz-meta-user-agent-id	sftp_user@s-

Amazon-S3-Ereignis-Benachrichtigungen

Wenn ein Objekt mit Transfer Family in Ihren S3-Bucket hochgeladen wird, ist es im Feld `Requester` in der [S3-Ereignisbenachrichtigungsstruktur](#) als `[AWS:Role Unique Identifier]/username.sessionid@server-id` enthalten. Im Folgenden finden Sie beispielsweise den Inhalt eines Beispielfeldes „Requester“ aus einem S3-Zugriffsprotokoll für eine Datei, die in den S3-Bucket kopiert wurde.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

Im obigen Feld `Requester` wird die aufgerufene IAM-Rolle angezeigt. `IamRoleName` Weitere Informationen zur Konfiguration von S3-Ereignisbenachrichtigungen finden Sie unter [Konfiguration von Amazon S3 S3-Ereignisbenachrichtigungen](#) im Amazon Simple Storage Service Developer Guide. Weitere Informationen zu eindeutigen AWS Identity and Access Management (IAM-) Rollenbezeichnern finden Sie unter [Eindeutige Identifikatoren](#) im AWS Identity and Access Management Benutzerhandbuch.

SFTP-Nachrichten

In diesem Abschnitt werden clientseitige Nachrichten beschrieben, die Sie während oder nach Ihren SFTP-Dateiübertragungen erhalten können, wenn Sie einen Transfer Family Family-Server verwenden. Weitere Informationen zu allen SFTP-Ereignissen finden Sie in den Protokollen Ihres SFTP-Clients. Sie können diese Informationen verwenden, um Fehler zu beheben, oder diese Informationen an Ihr Netzwerkteam weiterleiten, um Hilfe bei der Identifizierung des Problems zu erhalten.

Clientseitige SFTP-Nachrichten

Aktivität	Description
AUTH_FAILURE	Der Benutzer hat die Authentifizierung nicht bestanden. Dabei kann es sich um jede Art von Fehler handeln, die von einem benutzerdefinierten Identitätsanbieter oder einem vom Dienst verwalteten Benutzer verursacht wurden. Die Einzelheiten des Ereignisses helfen dabei, die Ursache des Fehlers zu klären.
CLOSE	Zeigt an, dass eine geöffnete Datei oder ein geöffnetes Verzeichnis erfolgreich geschlossen wurde.
CONNECTED/DISCONNECTED	Zeigt einen normalen Verbindungserfolg und Verbindungsabbrüche an.
CREATE_SYMLINK	Ein symbolischer Link wurde erstellt (erfolgreich oder erfolglos).
DELETE	Eine Datei wurde gelöscht (erfolgreich oder erfolglos).
ERROR	Ein allgemeiner, unerwarteter Fehler. Die zugehörige Beschreibung enthält Informationen, die Ihnen oder Ihren Netzwerkadministratoren helfen, das Problem zu beheben.

Aktivität	Description
	toren helfen können, das spezifische Problem zu identifizieren.
EXIT_REASON	Wird ausgelöst, wenn ein unerwarteter Fehler zur Beendigung Ihrer SFTP-Sitzung führte. Die dem Ereignis zugeordnete Nachricht beschreibt die Ursache.
MKDIR	Ein Verzeichnis wurde erstellt (erfolgreich oder erfolglos).
OPEN	Eine Datei wurde zum Lesen oder Schreiben geöffnet (erfolgreich oder erfolglos)
PARTIAL_CLOSE	Der Client hat die Verbindung zum Server getrennt, während eine Datei noch geöffnet war, ohne dass eine CLOSE-Meldung empfangen wurde. Transfer Family speichert den empfangenen Teil der Datei (bei dem es sich tatsächlich um die vollständige Datei handeln könnte) und gibt das Ereignis PARTIAL_CLOSE aus, um den Kunden über das Problem zu informieren. Die Workflow-Integration empfängt außerdem ein <code>onPartialClose</code> Ereignis, um die Datei entsprechend zu behandeln.
RENAME	Eine Datei wurde umbenannt (erfolgreich oder erfolglos)
RMDIR	Ein Verzeichnis wurde gelöscht (erfolgreich oder erfolglos)

Aktivität	Description
SETSTAT	Die Attribute einer Datei werden geändert (erfolgreich oder erfolglos).  Note Transfer Family unterstützt SETSTAT nicht, wenn Sie Amazon S3 als Speicher verwenden. Vermeiden Sie Fehler setstat In diesem Abschnitt erfahren Sie, wie Sie SetStat Fehler vermeiden können, indem Sie die Einstellung ausschalten. Dadurch wird vermieden, dass Sie die folgende Meldung erhalten <code>fail unsupported error</code> : Sie erhalten stattdessen <code>success but do nothing</code> eine Nachricht.
TLS_RESUME_FAILURE	Der Server ist so konfiguriert, dass er die Wiederaufnahme der TLS-Sitzung erzwingt, und der Client unterstützt dies nicht.

Benutzer für Serverendpunkte verwalten

In den folgenden Abschnitten finden Sie Informationen zum Hinzufügen von Benutzern mithilfe AWS Transfer Family eines benutzerdefinierten Identitätsanbieters. AWS Directory Service for Microsoft Active Directory

Sie speichern außerdem in den Eigenschaften der Benutzer den öffentlichen Secure Shell (SSH)-Schlüssel des jeweiligen Benutzers. Dies ist für die schlüsselbasierte Authentifizierung erforderlich. Der private Schlüssel wird lokal auf dem Computer Ihres Benutzers gespeichert. Wenn Ihr Benutzer mithilfe eines Clients eine Authentifizierungsanfrage an Ihren Server sendet, bestätigt Ihr Server zunächst, dass der Benutzer Zugriff auf den zugehörigen privaten SSH-Schlüssel hat. Der Server authentifiziert den Benutzer dann erfolgreich.

 Note

Informationen zur automatisierten Bereitstellung und Verwaltung von Benutzern mit mehreren SSH-Schlüsseln finden Sie unter: [Terraform-Module der Transfer Family](#)

Darüber hinaus geben Sie das Home-Verzeichnis oder das Landing-Verzeichnis eines Benutzers an und weisen dem Benutzer eine AWS Identity and Access Management (IAM-) Rolle zu. Optional können Sie eine Sitzungsrichtlinie angeben, um den Benutzerzugriff nur auf das Home-Verzeichnis Ihres Amazon S3 S3-Buckets zu beschränken.

 Important

AWS Transfer Family verhindert, dass sich Benutzernamen, die 1 oder 2 Zeichen lang sind, bei SFTP-Servern authentifizieren. Darüber hinaus blockieren wir auch den `root` Benutzernamen.

Der Grund dafür liegt in der großen Anzahl böswilliger Anmeldeversuche durch Passwortscanner.

Amazon EFS im Vergleich zu Amazon S3

Eigenschaften der einzelnen Speicheroptionen:

- Um den Zugriff zu beschränken: Amazon S3 unterstützt Sitzungsrichtlinien; Amazon EFS unterstützt POSIX-Benutzer-, Gruppen- und sekundäre Gruppen-IDs
- Beide unterstützen Schlüssel `public/private`
- Beide unterstützen Home-Verzeichnisse
- Beide unterstützen logische Verzeichnisse

 Note

Für Amazon S3 erfolgt der Großteil der Unterstützung für logische Verzeichnisse über API/CLI. Sie können das Kontrollkästchen `Eingeschränkt` in der Konsole verwenden, um einen Benutzer auf sein Home-Verzeichnis zu sperren, aber Sie können keine virtuelle Verzeichnisstruktur angeben.

Logische Verzeichnisse

Wenn Sie logische Verzeichniswerte für Ihren Benutzer angeben, hängt der verwendete Parameter vom Benutzertyp ab.

- Geben Sie für vom Dienst verwaltete Benutzer logische Verzeichniswerte in `HomeDirectoryMappings` ein.
- Geben Sie für Benutzer eines benutzerdefinierten Identitätsanbieters logische Verzeichniswerte in `anHomeDirectoryDetails`.

AWS Transfer Family unterstützt die Angabe eines `HomeDirectory` Werts bei Verwendung von `LOGICAL HomeDirectoryType`. Dies gilt für vom Service verwaltete Benutzer, Active Directory-Zugriff und benutzerdefinierte Identity Provider-Implementierungen, bei denen sie in der Antwort angegeben `HomeDirectoryDetails` werden.

Important

Wenn Sie a `HomeDirectory` mit `LOGICAL` angeben `HomeDirectoryType`, muss der Wert einer Ihrer logischen Verzeichniszuordnungen zugeordnet werden. Der Dienst überprüft dies sowohl bei der Benutzererstellung als auch bei Aktualisierungen, um Konfigurationen zu verhindern, die nicht funktionieren würden.

Standardverhalten

Wenn nichts angegeben wird, `HomeDirectory` ist der standardmäßig auf „/“ für den LOGISCHEN Modus gesetzt. Dieses Verhalten ist unverändert und bleibt mit bestehenden Benutzerdefinitionen kompatibel.

- Stellen Sie sicher, dass `HomeDirectory` Sie Ihrem Eintrag und nicht einem Ziel zuordnen. Weitere Details finden Sie unter [Regeln für die Verwendung logischer Verzeichnisse](#).
- Einzelheiten zur Struktur eines virtuellen Verzeichnisses finden Sie unter [Struktur des virtuellen Verzeichnisses](#).

Überlegungen zum benutzerdefinierten Identitätsanbieter

Wenn Sie einen benutzerdefinierten Identitätsanbieter verwenden, können Sie jetzt HomeDirectory in der Antwort a angeben, während Sie LOGICAL verwenden HomeDirectoryType. Der TestIdentityProvider API-Aufruf führt zu korrekten Ergebnissen, wenn der benutzerdefinierte IDP HomeDirectory im LOGICAL-Modus a angibt.

Beispiel für eine benutzerdefinierte IDP-Antwort mit HomeDirectory und LOGICAL:
HomeDirectoryType

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"\\\\\\\\\", \"Target\":\"\\\\\\\\/bucket/home\\\\\\\\\"}, {\"Entry\":\"\\\\\\\\/marketing\\\\\\\\\", \"Target\":\"\\\\\\\\/marketing-bucket/campaigns\\\\\\\\\"}]"
}
```

Active Directory-Gruppenkontingente

AWS Transfer Family hat ein Standardlimit von 100 Active Directory-Gruppen pro Server. Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Dieses Limit gilt für Server, die die folgenden Identitätsanbieter verwenden:

- AWS Directory Service für Microsoft Active Directory
- AWS Directory Service für Entra ID Domain Services

Wenn Sie eine Erhöhung des Servicelimits beantragen müssen, finden Sie Informationen zu den [AWS-Service Kontingenten](#) in der Allgemeine AWS-Referenz. Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Informationen zur Problembehandlung im Zusammenhang mit Active Directory-Gruppenlimits finden Sie unter [Die Active Directory-Gruppenlimits wurden überschritten](#).

Themen

- [Arbeiten mit Benutzern, die vom Dienst verwaltet werden](#)
- [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#)
- [Verwenden des AWS Directory Service für Microsoft Active Directory](#)
- [Verwenden des AWS Directory Service für Entra ID Domain Services](#)

Arbeiten mit Benutzern, die vom Dienst verwaltet werden

Sie können Ihrem Server entweder vom Service verwaltete Amazon S3- oder Amazon EFS-Benutzer hinzufügen, abhängig von der Domain-Einstellung des Servers. Weitere Informationen finden Sie unter [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#).

Wenn Sie einen vom Dienst verwalteten Identitätstyp verwenden, fügen Sie Benutzer zu Ihrem Server hinzu, auf dem das File Transfer Protocol aktiviert ist. Dabei muss jeder Benutzername auf Ihrem Server einzigartig sein.

Informationen zum programmgesteuerten Hinzufügen eines vom Service verwalteten Benutzers finden Sie im [Beispiel für die API. CreateUser](#)

Note

Für Benutzer, die vom Dienst verwaltet werden, gilt eine Obergrenze von 2.000 logischen Verzeichniseinträgen. Hinweise zur Verwendung logischer Verzeichnisse finden Sie unter [Verwendung logischer Verzeichnisse zur Vereinfachung Ihrer Transfer Family Family-Verzeichnisstrukturen](#).

Themen

- [Hinzufügen von vom Service verwalteten Amazon S3-Benutzern](#)
- [Hinzufügen von vom Service verwalteten Amazon EFS-Benutzern](#)
- [Verwaltung von Benutzern, die vom Service verwaltet werden](#)

Hinzufügen von vom Service verwalteten Amazon S3-Benutzern

Note

Wenn Sie einen kontoübergreifenden Amazon S3 S3-Bucket konfigurieren möchten, folgen Sie den Schritten in diesem Knowledge Center-Artikel: [Wie konfiguriere ich meinen AWS Transfer Family Server für die Verwendung eines Amazon Simple Storage Service-Buckets, der sich in einem anderen AWS Konto befindet?](#) .

So fügen Sie Ihrem Server einen vom Service verwalteten Amazon S3 S3-Benutzer hinzu

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie dann im Navigationsbereich Server aus.
2. Aktivieren Sie auf der Seite Server das Kontrollkästchen des Servers, zu dem Sie einen Benutzer hinzufügen möchten.
3. Wählen Sie Benutzer hinzufügen.
4. Geben Sie im Abschnitt Benutzerkonfiguration für Benutzername den Benutzernamen ein. Dieser Benutzername muss mindestens 3 und maximal 100 Zeichen lang sein. Sie können die folgenden Zeichen im Benutzernamen verwenden: a—z, 0—9 A-Z, Unterstrich '_', Bindestrich '-', Punkt '.' und das Zeichen '@'. Der Benutzername darf nicht mit einem Bindestrich '-', einem Punkt '.' oder einem Zeichen '@' beginnen.
5. Wählen Sie für Access die IAM-Rolle aus, die Sie zuvor erstellt haben und die Zugriff auf Ihren Amazon S3 S3-Bucket bietet.

Sie haben diese IAM-Rolle in der Prozedur [Erstellen Sie eine IAM-Rolle und -Richtlinie](#) erstellt. Diese IAM-Rolle beinhaltet eine IAM-Richtlinie, die den Zugriff auf Ihren Amazon S3 S3-Bucket ermöglicht. Dazu gehört auch eine Vertrauensbeziehung mit dem AWS Transfer Family Service, die in einer anderen IAM-Richtlinie definiert ist. Wenn Sie eine detaillierte Zugriffskontrolle für Ihre Benutzer benötigen, lesen Sie den Blogbeitrag [Enhance data access control with AWS Transfer Family and Amazon S3](#).

6. (Optional) Wählen Sie unter Richtlinie eine der folgenden Optionen aus:
 - Keine
 - Bestehende Richtlinie

- Wählen Sie eine Richtlinie aus IAM aus: Ermöglicht die Auswahl einer vorhandenen Sitzungsrichtlinie. Wählen Sie Ansicht, um ein JSON-Objekt mit den Details der Richtlinie anzuzeigen.
- Auto-generate Richtlinie basierend auf dem Home-Ordner: generiert eine Sitzungsrichtlinie für Sie. Wählen Sie Ansicht, um ein JSON-Objekt mit den Details der Richtlinie anzuzeigen.

 Note

Wenn Sie eine Auto-generate Richtlinie auswählen, die auf dem Basisordner basiert, wählen Sie für diesen Benutzer nicht die Option Eingeschränkt aus.

Weitere Informationen zu Sitzungsrichtlinien finden Sie unter [Erstellen Sie eine IAM-Rolle und -Richtlinie](#)[Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#), oder [Dynamische Ansätze zur Rechteverwaltung](#).

7. Wählen Sie für das Home-Verzeichnis den Amazon S3 S3-Bucket aus, in dem die zu übertragenden Daten gespeichert AWS Transfer Family werden sollen. Geben Sie den Pfad zu dem home Verzeichnis ein, in dem Ihr Benutzer landet, wenn er sich mit seinem Client anmeldet.

Wenn Sie diesen Parameter leer lassen, wird das root Verzeichnis Ihres Amazon S3 S3-Buckets verwendet. Stellen Sie in diesem Fall sicher, dass die IAM-Rolle Zugriff auf dieses root-Verzeichnis gewährt.

 Note

Wir empfehlen Ihnen, einen Verzeichnispfad zu wählen, der den Benutzernamen des Benutzers enthält, sodass Sie eine Sitzungsrichtlinie effektiv verwenden können. Die Sitzungsrichtlinie beschränkt den Benutzerzugriff im Amazon S3 S3-Bucket auf das home Verzeichnis dieses Benutzers.

8. (Optional) Aktivieren Sie für Eingeschränkt das Kontrollkästchen, sodass Ihre Benutzer auf nichts außerhalb dieses Ordners zugreifen können und den Amazon S3 S3-Bucket- oder Ordernamen nicht sehen können.

 Note

Dem Benutzer ein Home-Verzeichnis zuzuweisen und den Benutzer auf dieses Home-Verzeichnis zu beschränken, sollte ausreichen, um den Zugriff des Benutzers auf den angegebenen Ordner zu sperren. Wenn Sie weitere Kontrollen anwenden müssen, verwenden Sie eine Sitzungsrichtlinie.

Wenn Sie für diesen Benutzer die Option Eingeschränkt auswählen, können Sie keine auf dem Basisordner basierende Auto-generate Richtlinie auswählen, da der Basisordner kein definierter Wert für Benutzer mit eingeschränkten Rechten ist.

9. Geben Sie für den öffentlichen SSH-Schlüssel den öffentlichen SSH-Schlüsselteil des SSH-Schlüsselpaars key pair.

Der Schlüssel wird vom Service validiert, bevor Sie den neuen Benutzer hinzufügen können.

 Note

Anleitungen zum Generieren eines SSH-Schlüsselpaars siehe [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).

10. (Optional) Geben Sie für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie Tag hinzufügen aus.
11. Wählen Sie Add (Hinzufügen), um den neuen Benutzer dem ausgewählten Server hinzuzufügen.

Der neue Benutzer wird auf der Seite mit den Serverdetails im Bereich Benutzer angezeigt.

Nächste Schritte — Fahren Sie für den nächsten Schritt fort mit [Übertragung von Dateien über einen Serverendpunkt mit einem Client](#).

Hinzufügen von vom Service verwalteten Amazon EFS-Benutzern

Amazon EFS verwendet das POSIX-Dateiberechtigungsmodell (Portable Operating System Interface), um den Dateibesitz darzustellen.

- Weitere Informationen zum Besitz von Amazon EFS-Dateien finden Sie unter [Amazon EFS-Dateibesitz](#).

- Weitere Informationen zum Einrichten von Verzeichnissen für Ihre EFS-Benutzer finden Sie unter [Amazon EFS-Benutzer für Transfer Family einrichten](#).

So fügen Sie Ihrem Server einen vom Amazon EFS Service verwalteten Benutzer hinzu

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie dann im Navigationsbereich Server aus.
2. Wählen Sie auf der Seite Server den Amazon EFS-Server aus, zu dem Sie einen Benutzer hinzufügen möchten.
3. Wählen Sie Benutzer hinzufügen, um die Seite Benutzer hinzufügen anzuzeigen.
4. Verwenden Sie im Abschnitt Benutzerkonfiguration die folgenden Einstellungen.
 - a. Der Benutzername muss mindestens 3 und maximal 100 Zeichen lang sein. Sie können die folgenden Zeichen im Benutzernamen verwenden: a—z, 0—9 A-Z, Unterstrich '_', Bindestrich '-', Punkt '.' und beim Zeichen „@“. Der Benutzername darf nicht mit einem Bindestrich '-' oder Punkt '.' beginnen, oder beim Zeichen „@“.
 - b. Beachten Sie bei Benutzer-ID und Gruppen-ID Folgendes:
 - Für den ersten Benutzer, den Sie erstellen, empfehlen wir, den Wert sowohl **0** für die Gruppen-ID als auch für die Benutzer-ID einzugeben. Dadurch werden dem Benutzer Administratorrechte für Amazon EFS gewährt.
 - Geben Sie für weitere Benutzer die POSIX-Benutzer-ID und die Gruppen-ID des Benutzers ein. Diese IDs werden für alle vom Benutzer ausgeführten Amazon Elastic File System-Operationen verwendet.
 - Verwenden Sie für Benutzer-ID und Gruppen-ID keine führenden Nullen. Zum Beispiel **12345** ist akzeptabel, **012345** ist nicht.
 - c. (Optional) Geben Sie für sekundäre Gruppen-IDs eine oder mehrere zusätzliche POSIX-Gruppen-IDs für jeden Benutzer ein, getrennt durch Kommas.
 - d. Wählen Sie für Access die IAM-Rolle aus, die:
 - Gewährt dem Benutzer nur Zugriff auf die Amazon EFS-Ressourcen (Dateisysteme), auf die er zugreifen soll.
 - Definiert, welche Dateisystemoperationen der Benutzer ausführen kann und welche nicht.

Wir empfehlen, dass Sie die IAM-Rolle für die Auswahl des Amazon EFS-Dateisystems mit Bereitstellungszugriff und read/write -berechtigungen verwenden. Die Kombination der folgenden beiden AWS verwalteten Richtlinien ist zwar recht freizügig, gewährt Ihrem Benutzer jedoch die erforderlichen Berechtigungen:

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

Weitere Informationen finden Sie im Blogbeitrag [AWS Transfer Family Unterstützung für Amazon Elastic File System](#).

e. Gehen Sie für das Home-Verzeichnis wie folgt vor:

- Wählen Sie das Amazon EFS-Dateisystem aus, das Sie zum Speichern der zu übertragenden Daten verwenden möchten AWS Transfer Family.
- Entscheiden Sie, ob Sie das Home-Verzeichnis auf Eingeschränkt setzen möchten. Das Setzen des Home-Verzeichnisses auf Eingeschränkt hat folgende Auswirkungen:
 - Amazon EFS-Benutzer können auf keine Dateien oder Verzeichnisse außerhalb dieses Ordners zugreifen.
 - Amazon EFS-Benutzer können den Namen des Amazon EFS-Dateisystems (fs-xxxxxxx) nicht sehen.

 Note

Wenn Sie die Option Eingeschränkt auswählen, werden Symlinks für Amazon EFS-Benutzer nicht aufgelöst.

- (Optional) Geben Sie den Pfad zu dem Basisverzeichnis ein, in dem sich Benutzer befinden sollen, wenn sie sich mit ihrem Client anmelden.

Wenn Sie kein Home-Verzeichnis angeben, wird das Stammverzeichnis Ihres Amazon EFS-Dateisystems verwendet. Stellen Sie in diesem Fall sicher, dass Ihre IAM-Rolle Zugriff auf dieses Stammverzeichnis bietet.

5. Geben Sie für den öffentlichen SSH-Schlüssel den öffentlichen SSH-Schlüsselteil des SSH-Schlüsselpaars key pair.

Der Schlüssel wird vom Service validiert, bevor Sie den neuen Benutzer hinzufügen können.

 Note

Anleitungen zum Generieren eines SSH-Schlüsselpaars siehe [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).

6. (Optional) Geben Sie beliebige Tags für den Benutzer ein. Geben Sie für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein und wählen Sie Tag hinzufügen aus.
7. Wählen Sie Add (Hinzufügen), um den neuen Benutzer dem ausgewählten Server hinzuzufügen.

Der neue Benutzer wird auf der Seite mit den Serverdetails im Bereich Benutzer angezeigt.

Probleme, die beim ersten SFTP-Zugriff auf Ihren Transfer Family Family-Server auftreten können:

- Wenn Sie den `sftp` Befehl ausführen und die Eingabeaufforderung nicht angezeigt wird, wird möglicherweise die folgende Meldung angezeigt:

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

In diesem Fall müssen Sie die Richtlinienberechtigungen für die Rolle Ihres Benutzers erhöhen. Sie können eine AWS verwaltete Richtlinie hinzufügen, z. `AmazonElasticFileSystemClientFullAccess` B.

- Wenn Sie `pwd` an der `sftp` Eingabeaufforderung das Home-Verzeichnis des Benutzers aufrufen, wird möglicherweise die folgende Meldung angezeigt, in der ***USER-HOME-DIRECTORY*** es um das Home-Verzeichnis für den SFTP-Benutzer geht:

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

In diesem Fall sollten Sie in der Lage sein, zum übergeordneten Verzeichnis (`cd ..`) zu navigieren und das Home-Verzeichnis des Benutzers zu erstellen (`mkdir username`).

Nächste Schritte — Fahren Sie für den nächsten Schritt fort mit [Übertragung von Dateien über einen Serverendpunkt mit einem Client](#).

Verwaltung von Benutzern, die vom Service verwaltet werden

In diesem Abschnitt finden Sie Informationen zum Anzeigen einer Benutzerliste, zum Bearbeiten von Benutzerdetails und zum Hinzufügen eines öffentlichen SSH-Schlüssels.

- [Eine Liste von Benutzern anzeigen](#)
- [Benutzerdetails anzeigen oder bearbeiten](#)
- [Löschen eines Benutzers](#)
- [Öffentlichen SSH-Schlüssel hinzufügen](#)
- [Löschen Sie den öffentlichen SSH-Schlüssel](#)

Um eine Liste Ihrer Benutzer zu finden

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im Navigationsbereich Server aus, um die Seite Server anzuzeigen.
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Sehen Sie sich unter Benutzer eine Liste der Benutzer an.

Um Benutzerdetails anzuzeigen oder zu bearbeiten

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im Navigationsbereich Server aus, um die Seite Server anzuzeigen.
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Seite mit den Benutzerdetails aufzurufen.

Sie können die Eigenschaften des Benutzers auf dieser Seite ändern, indem Sie Bearbeiten wählen.

5. Wählen Sie auf der Seite mit den Benutzerdetails neben Benutzerkonfiguration die Option Bearbeiten aus.

Edit configuration

User configuration

Access [Info](#)
User's IAM role for Amazon S3 access

Admin ▼ ↻

Policy [Info](#)
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

View

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted [Info](#)

Cancel Save

6. Wählen Sie auf der Seite Konfiguration bearbeiten für Access die IAM-Rolle aus, die Sie zuvor erstellt haben und die Zugriff auf Ihren Amazon S3 S3-Bucket bietet.

Sie haben diese IAM-Rolle in der Prozedur [Erstellen Sie eine IAM-Rolle und -Richtlinie](#) erstellt. Diese IAM-Rolle beinhaltet eine IAM-Richtlinie, die den Zugriff auf Ihren Amazon S3 S3-Bucket ermöglicht. Dazu gehört auch eine Vertrauensbeziehung mit dem AWS Transfer Family Service, die in einer anderen IAM-Richtlinie definiert ist.

7. (Optional) Wählen Sie für Policy eine der folgenden Optionen aus:
- Keine
 - Bestehende Richtlinie
 - Wählen Sie eine Richtlinie aus IAM aus, um eine bestehende Richtlinie auszuwählen. Wählen Sie Ansicht, um ein JSON-Objekt mit den Details der Richtlinie anzuzeigen.

Weitere Informationen zu Sitzungsrichtlinien finden Sie unter [Erstellen Sie eine IAM-Rolle und -Richtlinie](#). Weitere Informationen zum Erstellen einer Sitzungsrichtlinie finden Sie unter [Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#).

8. Wählen Sie für das Home-Verzeichnis den Amazon S3 S3-Bucket aus, in dem die zu übertragenden Daten gespeichert AWS Transfer Family werden sollen. Geben Sie den Pfad zu dem home Verzeichnis ein, in dem Ihr Benutzer landet, wenn er sich mit seinem Client anmeldet.

Wenn Sie diesen Parameter leer lassen, wird das `root` Verzeichnis Ihres Amazon S3 S3-Buckets verwendet. Stellen Sie in diesem Fall sicher, dass die IAM-Rolle Zugriff auf dieses `root`-Verzeichnis gewährt.

 Note

Wir empfehlen Ihnen, einen Verzeichnispfad zu wählen, der den Benutzernamen des Benutzers enthält, sodass Sie eine Sitzungsrichtlinie effektiv verwenden können. Die Sitzungsrichtlinie beschränkt den Benutzerzugriff im Amazon S3 S3-Bucket auf das home Verzeichnis dieses Benutzers.

9. (Optional) Aktivieren Sie für Eingeschränkt das Kontrollkästchen, sodass Ihre Benutzer auf nichts außerhalb dieses Ordners zugreifen können und den Amazon S3 S3-Bucket- oder Ordernamen nicht sehen können.

 Note

Wenn Sie dem Benutzer ein Home-Verzeichnis zuweisen und den Benutzer auf dieses Home-Verzeichnis beschränken, sollte dies ausreichen, um den Zugriff des Benutzers auf den angegebenen Ordner zu sperren. Verwenden Sie eine Sitzungsrichtlinie, wenn Sie weitere Kontrollen vornehmen müssen.

10. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

So löschen Sie einen Benutzer

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im Navigationsbereich Server aus, um die Seite Server anzuzeigen.
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Seite mit den Benutzerdetails aufzurufen.

5. Wählen Sie auf der Seite mit den Benutzerdetails rechts neben dem Benutzernamen die Option Löschen aus.
6. Geben Sie im daraufhin angezeigten Bestätigungsdialogfeld das Wort ein und wählen Sie dann Löschen **delete**, um zu bestätigen, dass Sie den Benutzer löschen möchten.

Der Benutzer wird aus der Benutzerliste gelöscht.

Um einen öffentlichen SSH-Schlüssel für einen Benutzer hinzuzufügen

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Seite mit den Benutzerdetails aufzurufen.
5. Wählen Sie Add SSH public key (Öffentlichen SSH-Schlüssel hinzufügen), um einem Benutzer einen neuen öffentlichen SSH-Schlüssel hinzuzufügen.

 Note

SSH-Schlüssel werden nur von Servern verwendet, die für Secure Shell (SSH) File Transfer Protocol (SFTP) aktiviert sind. Hinweise zum Generieren eines SSH-Schlüsselpaars finden Sie unter [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).

6. Geben Sie für SSH public key (Öffentlicher SSH-Schlüssel) den öffentlichen SSH-Schlüssel des SSH-Schlüsselpaars ein.

Der Schlüssel wird vom Service validiert, bevor Sie den neuen Benutzer hinzufügen können.

Das Format des SSH-Schlüssels lautet `ssh-rsa string`. Informationen zum Generieren eines SSH-Schlüsselpaars finden Sie unter [Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer](#).

7. Wählen Sie Schlüssel hinzufügen.

So löschen Sie einen öffentlichen SSH-Schlüssel für einen Benutzer

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Seite mit den Benutzerdetails aufzurufen.
5. Um einen öffentlichen Schlüssel zu löschen, aktivieren Sie das entsprechende Kontrollkästchen für den SSH-Schlüssel und wählen Sie Löschen aus.

Mit Anbietern benutzerdefinierter Identitäten arbeiten

AWS Transfer Family bietet verschiedene Optionen für benutzerdefinierte Identitätsanbieter zur Authentifizierung und Autorisierung von Benutzern für sichere Dateiübertragungen. Hier sind die wichtigsten Ansätze:

- [Lösung für einen benutzerdefinierten Identitätsanbieter](#)— In diesem Thema wird die benutzerdefinierte Identitätsanbieter-Lösung von Transfer Family mithilfe eines Toolkits beschrieben, das unter gehostet wird. GitHub

Note

Für die meisten Anwendungsfälle ist dies die empfohlene Option. Insbesondere wenn Sie mehr als 100 Active Directory-Gruppen unterstützen müssen, bietet die benutzerdefinierte Identitätsanbieter-Lösung eine skalierbare Alternative ohne Gruppenbeschränkungen. Diese Lösung wird im Blogbeitrag [Simplify Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

- [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters](#)— In diesem Thema wird beschrieben, wie eine AWS Lambda Funktion zur Unterstützung einer Amazon API Gateway Gateway-Methode verwendet wird.

Sie können eine RESTful-Schnittstelle mit einer einzigen Amazon API Gateway Gateway-Methode bereitstellen. Transfer Family ruft diese Methode auf, um eine Verbindung zu Ihrem Identitätsanbieter herzustellen, der Ihre Benutzer authentifiziert und für den Zugriff auf Amazon S3 oder Amazon EFS autorisiert. Verwenden Sie diese Option, wenn Sie eine RESTful-API zur

Integration Ihres Identitätsanbieters benötigen oder wenn Sie dessen Funktionen für Geoblocking- oder Ratenbegrenzungsanfragen nutzen AWS WAF möchten. Details hierzu finden Sie unter [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters](#).

- [Dynamische Ansätze zur Rechteverwaltung](#)— In diesem Thema werden Ansätze für die dynamische Verwaltung von Benutzerberechtigungen mithilfe von Sitzungsrichtlinien beschrieben.

Um Ihre Benutzer zu authentifizieren, können Sie Ihren vorhandenen Identitätsanbieter mit verwenden. AWS Transfer Family Sie integrieren Ihren Identitätsanbieter mithilfe einer AWS Lambda Funktion, die Ihre Benutzer authentifiziert und für den Zugriff auf Amazon S3 oder Amazon Elastic File System (Amazon EFS) autorisiert. Details hierzu finden Sie unter [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet](#). In der AWS Transfer Family Management Console können Sie auch auf CloudWatch Diagramme für Messwerte wie die Anzahl der übertragenen Dateien und Byte zugreifen, sodass Sie Dateiübertragungen über ein zentrales Dashboard überwachen können.

- Transfer Family bietet einen Blogbeitrag und einen Workshop, die Sie durch den Aufbau einer Dateiübertragungslösung führen. Diese Lösung nutzt AWS Transfer Family für verwaltete SFTP/FTPS Endgeräte sowie Amazon Cognito und DynamoDB für die Benutzerverwaltung.

Der Blogbeitrag ist unter [Amazon Cognito als Identitätsanbieter mit AWS Transfer Family Amazon S3 verwenden](#) verfügbar. Die Details zum Workshop finden Sie [hier](#).

Note

Für benutzerdefinierte Identitätsanbieter muss der Benutzername mindestens 3 und maximal 100 Zeichen lang sein. Sie können die folgenden Zeichen im Benutzernamen verwenden: a—z, 0—9 A-Z, Unterstrich '_', Bindestrich '-', Punkt '.' und das At-Zeichen '@'. Der Benutzername darf nicht mit einem Bindestrich '-', einem Punkt '.' oder einem Zeichen '@' beginnen.

Beachten Sie bei der Implementierung eines benutzerdefinierten Identitätsanbieters die folgenden bewährten Methoden:

- Stellen Sie die Lösung in derselben AWS-Konto Region wie Ihre Transfer Family Family-Server bereit.
- Implementieren Sie bei der Konfiguration von IAM-Rollen und -Richtlinien das Prinzip der geringsten Rechte.

- Verwenden Sie Funktionen wie die IP-Zulassungsliste und die standardisierte Protokollierung für mehr Sicherheit.
- Testen Sie Ihren benutzerdefinierten Identitätsanbieter vor der Bereitstellung gründlich in einer Umgebung außerhalb der Produktionsumgebung.

Themen

- [Lösung für einen benutzerdefinierten Identitätsanbieter](#)
- [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet](#)
- [Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters](#)
- [Verwendung mehrerer Authentifizierungsmethoden](#)
- [IPv6-Unterstützung für benutzerdefinierte Identitätsanbieter](#)

Lösung für einen benutzerdefinierten Identitätsanbieter

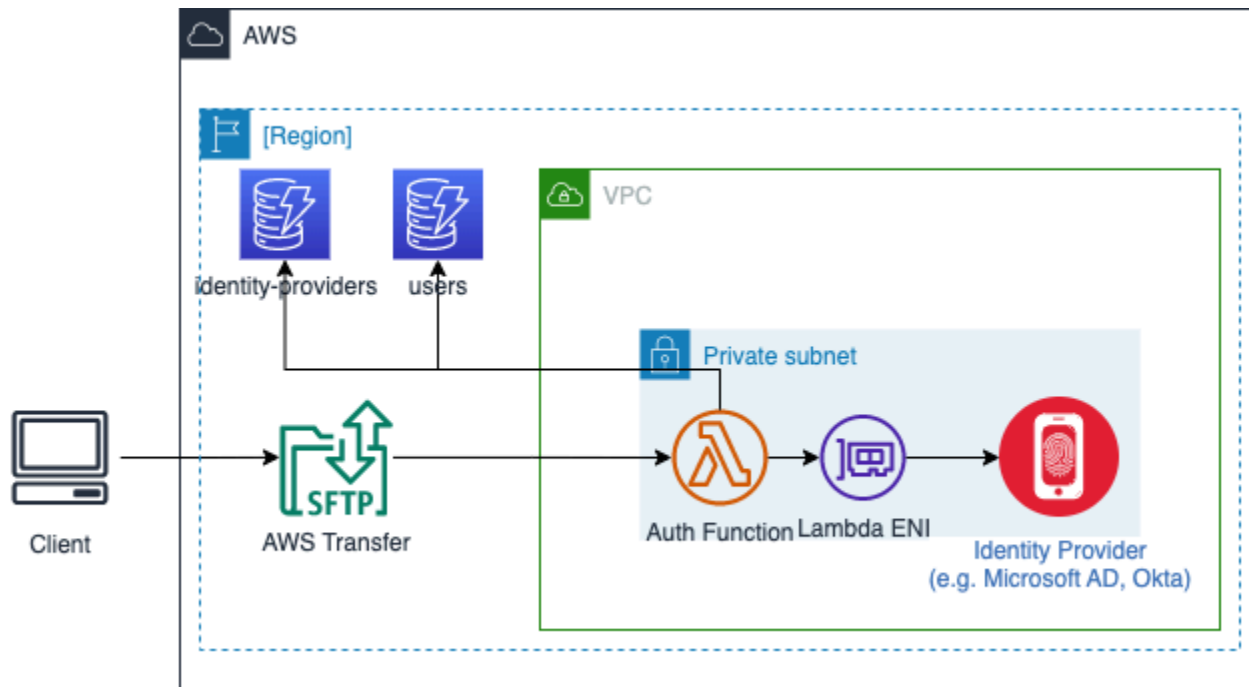
Die AWS Transfer Family benutzerdefinierte Identitätsanbieter-Lösung ist eine modulare benutzerdefinierte Identitätsanbieter-Lösung, die viele gängige Authentifizierungs- und Autorisierungsanwendungsfälle löst, mit denen Unternehmen bei der Implementierung des Dienstes konfrontiert sind. Diese Lösung bietet eine wiederverwendbare Grundlage für die Implementierung benutzerdefinierter Identitätsanbieter mit detaillierter Sitzungskonfiguration pro Benutzer. Sie trennt die Authentifizierungs- und Autorisierungslogik und bietet so eine flexible und leicht zu wartende Grundlage für verschiedene Anwendungsfälle.

Mit der AWS Transfer Family benutzerdefinierten Identitätsanbieter-Lösung können Sie gängige Anwendungsfälle für die Authentifizierung und Autorisierung in Unternehmen adressieren. Diese modulare Lösung bietet:

- Eine wiederverwendbare Grundlage für die Implementierung benutzerdefinierter Identitätsanbieter
- Granulare Sitzungskonfiguration pro Benutzer
- Separate Authentifizierungs- und Autorisierungslogik

Implementierungsdetails für das Custom Identity Toolkit

Die Lösung bietet eine flexible und wartungsfreundliche Basis für verschiedene Anwendungsfälle. Sehen Sie sich zunächst das Toolkit unter an <https://github.com/aws-samples/toolkit-for-aws-transfer-family> und folgen Sie dann den Bereitstellungsanweisungen im Abschnitt [Erste Schritte](#).



Note

Wenn Sie zuvor benutzerdefinierte Vorlagen und Beispiele für Identitätsanbieter verwendet haben, sollten Sie stattdessen diese Lösung in Betracht ziehen. In Zukunft werden anbieterspezifische Module diese Lösung standardisieren. Diese Lösung wird fortlaufend gewartet und die Funktionen erweitert.

Diese Lösung enthält Standardmuster für die Implementierung eines benutzerdefinierten Anbieters, der Details wie die Protokollierung und den Speicherort der zusätzlichen Sitzungsmetadaten AWS Transfer Family, wie z. B. der `HomeDirectoryDetails` Parameter, berücksichtigt. Diese Lösung bietet eine wiederverwendbare Grundlage für die Implementierung benutzerdefinierter Identitätsanbieter mit einer detaillierten Sitzungskonfiguration pro Benutzer und entkoppelt die Authentifizierungslogik des Identitätsanbieters von der wiederverwendbaren Logik, die eine Konfiguration erstellt, die an Transfer Family zurückgegeben wird, um die Authentifizierung abzuschließen und Einstellungen für die Sitzung festzulegen.

Den Code und die unterstützenden Ressourcen für diese Lösung finden Sie unter <https://github.com/aws-samples/toolkit-for-aws-transfer-family>

Das Toolkit enthält die folgenden Funktionen:

- Eine [AWS Serverless Application Model](#) Vorlage, die die erforderlichen Ressourcen bereitstellt. Optional können Sie Amazon API Gateway zur Integration bereitstellen und konfigurieren AWS WAF, wie im Blogbeitrag [Securing AWS Transfer Family with AWS Web Application Firewall and Amazon API Gateway](#) beschrieben.
- Ein [Amazon DynamoDB DynamoDB-Schema](#) zum Speichern von Konfigurationsmetadaten über Identitätsanbieter, einschließlich Benutzersitzungseinstellungen wie `HomeDirectoryDetailsRole`, und `Policy`
- Ein modularer Ansatz, der es Ihnen ermöglicht, der Lösung in future neue Identitätsanbieter als Module hinzuzufügen.
- Abruf von Attributen: Rufen Sie optional IAM-Rollen- und POSIX-Profilattribute (UID und GID) von unterstützten Identitätsanbietern ab, einschließlich AD, LDAP und Okta.
- Support für mehrere Identitätsanbieter, die mit einem einzigen Transfer Family Family-Server verbunden sind, und für mehrere Transfer Family Family-Server, die dieselbe Bereitstellung der Lösung verwenden.
- Built-in Überprüfung von IP-Zulassungslisten, z. B. IP-Zulassungslisten, die optional pro Benutzer oder pro Identitätsanbieter konfiguriert werden können.
- Detaillierte Protokollierung mit konfigurierbarer Protokollebene und Ablaufverfolgungsunterstützung zur Unterstützung bei der Fehlerbehebung.

Bevor Sie mit der Bereitstellung der benutzerdefinierten Identitätsanbieter-Lösung beginnen, benötigen Sie die folgenden Ressourcen. AWS

- Eine Amazon Virtual Private Cloud (VPC) mit privaten Subnetzen, mit Internetkonnektivität entweder über ein NAT-Gateway oder einen DynamoDB-Gateway-Endpunkt.
- Entsprechende IAM-Berechtigungen zur Ausführung der folgenden Aufgaben:
 - Stellen Sie die `custom-idp.yaml` CloudFormation Vorlage bereit,
 - AWS CodePipeline Projekte erstellen
 - AWS CodeBuild Projekte erstellen
 - Erstellen Sie IAM-Rollen und -Richtlinien

⚠ Important

Sie müssen die Lösung auf demselben AWS-Konto Server bereitstellen AWS-Region , der Ihre Transfer Family Family-Zielservers enthält.

Unterstützte Identitätsanbieter

Die folgende Liste enthält Informationen zu Identitätsanbietern, die für die benutzerdefinierte Identitätsanbieterlösung unterstützt werden.

Anbieter	Kennwortflüsse	Öffentliche Schlüssel fließen	Multi-factor	Abrufen von Attributen	Details
Active Directory und LDAP	Ja	Ja	Nein	Ja	Die Benutzerverifizierung kann im Rahmen der Authentifizierung mit öffentlichen Schlüsseln durchgeführt werden.
Argon2 (lokaler Hash)	Ja	Nein	Nein	Nein	Argon2-Hashes werden im Benutzersatz für Anwendungsfälle der „lokalen“ passwortbasierten Authentifizierung verwendet.

Anbieter	Kennwortflüsse	Öffentliche Schlüssel fließen	Multi-factor	Abrufen von Attributen	Details
					isierung gespeichert.
Amazon Cognito	Ja	Nein	Ja*	Nein	Time-based One-Time Nur auf Passwort (TOTP) basierende Multifactor-Authentifizierung. * SMS-based MFA wird nicht unterstützt.
Entra ID (früher Azure AD)	Ja	Nein	Nein	Nein	
Okta	Ja	Ja	Ja*	Ja	TOTP-based Nur MFA.
Öffentlicher Schlüssel	Nein	Ja	Nein	Nein	Öffentliche Schlüssel werden im Benutzerdatensatz in DynamoDB gespeichert.

Anbieter	Kennwortflüsse	Öffentliche Schlüssel fließen	Multi-factor	Abrufen von Attributen	Details
Secrets Manager	Ja	Ja	Nein	Nein	

Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet

In diesem Thema wird beschrieben, wie Sie eine AWS Lambda Funktion erstellen, die eine Verbindung zu Ihrem benutzerdefinierten Identitätsanbieter herstellt. Sie können einen beliebigen benutzerdefinierten Identitätsanbieter wie Okta, Secrets Manager oder einen benutzerdefinierten Datenspeicher verwenden OneLogin, der Autorisierungs- und Authentifizierungslogik enthält.

Für die meisten Anwendungsfälle wird empfohlen, einen benutzerdefinierten Identitätsanbieter zu konfigurieren, die [Lösung für einen benutzerdefinierten Identitätsanbieter](#) Verwendung von.

Note

Bevor Sie einen Transfer Family Family-Server erstellen, der Lambda als Identitätsanbieter verwendet, müssen Sie die Funktion erstellen. Eine Beispielfunktion für Lambda finden Sie unter [Beispiele für Lambda-Funktionen](#). Oder Sie können einen CloudFormation Stack bereitstellen, der einen der [Lambda-Funktionsvorlagen](#) folgenden verwendet. Stellen Sie außerdem sicher, dass Ihre Lambda-Funktion eine ressourcenbasierte Richtlinie verwendet, die Transfer Family vertraut. Eine Beispielrichtlinie finden Sie unter [Ressourcenbasierte Lambda-Richtlinie](#).

1. Öffnen Sie die [AWS Transfer Family -Konsole](#).
2. Wählen Sie Server erstellen, um die Seite Server erstellen zu öffnen. Wählen Sie für Wählen Sie einen Identitätsanbieter die Option Benutzerdefinierter Identitätsanbieter aus, wie im folgenden Screenshot gezeigt.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel

Previous

Next

Note

Die Wahl der Authentifizierungsmethoden ist nur verfügbar, wenn Sie SFTP als eines der Protokolle für Ihren Transfer Family Family-Server aktivieren.

3. Stellen Sie sicher, dass der Standardwert „AWS Lambda Zur Verbindung Ihres Identitätsanbieters verwenden“ ausgewählt ist.
4. Wählen Sie unter AWS Lambda Funktion den Namen Ihrer Lambda-Funktion.

5. Füllen Sie die verbleibenden Felder aus und wählen Sie dann Server erstellen aus. Einzelheiten zu den verbleibenden Schritten zum Erstellen eines Servers finden Sie unter [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#).

Ressourcenbasierte Lambda-Richtlinie

Sie benötigen eine Richtlinie, die auf den Transfer Family Family-Server und Lambda-ARNs verweist. Sie könnten beispielsweise die folgende Richtlinie mit Ihrer Lambda-Funktion verwenden, die eine Verbindung zu Ihrem Identitätsanbieter herstellt. Bei der Richtlinie wird JSON als Zeichenfolge maskiert.

```
"Policy":
"{\"Version\":\"2012-10-17\",
  \"Id\":\"default\",
  \"Statement\":[
    {\"Sid\":\"AllowTransferInvocation\",
      \"Effect\":\"Allow\",
      \"Principal\":{\"Service\":\"transfer.amazonaws.com\"},
      \"Action\":\"lambda:InvokeFunction\",
      \"Resource\":\"arn:aws:lambda:region:123456789012:function:my-lambda-auth-
function\",
      \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
        \"arn:aws:transfer:region:123456789012:server/server-id\"}}}}
  ]}"
```

Note

Ersetzen Sie in der obigen Beispielrichtlinie jede Richtlinie *user input placeholder* durch Ihre eigenen Informationen.

Struktur von Ereignismeldungen

Die Struktur der Ereignisnachrichten, die vom SFTP-Server an die Lambda-Funktion des Autorisierers für einen benutzerdefinierten IDP gesendet werden, lautet wie folgt.

```
{
  "username": "value",
```

```
"password": "value",  
"protocol": "SFTP",  
"serverId": "s-abcd123456",  
"sourceIp": "192.168.0.100"  
}
```

Wo username und password sind die Werte für die Anmeldeinformationen, die an den Server gesendet werden.

Sie geben beispielsweise den folgenden Befehl ein, um eine Verbindung herzustellen:

```
sftp bobusa@server_hostname
```

Sie werden dann aufgefordert, Ihr Passwort einzugeben:

```
Enter password:  
mysecretpassword
```

Sie können dies von Ihrer Lambda-Funktion aus überprüfen, indem Sie das übergebene Ereignis aus der Lambda-Funktion heraus drucken. Es sollte dem folgenden Textblock ähneln.

```
{  
  "username": "bobusa",  
  "password": "mysecretpassword",  
  "protocol": "SFTP",  
  "serverId": "s-abcd123456",  
  "sourceIp": "192.168.0.100"  
}
```

Die Ereignisstruktur ist für FTP und FTPS ähnlich: Der einzige Unterschied besteht darin, dass diese Werte für den protocol Parameter und nicht für SFTP verwendet werden.

Lambda-Funktionen für die Authentifizierung

Bearbeiten Sie die Lambda-Funktion, um verschiedene Authentifizierungsstrategien zu implementieren. Um die Anforderungen Ihrer Anwendung zu erfüllen, können Sie einen CloudFormation Stack bereitstellen. Weitere Informationen zu Lambda finden Sie im [AWS Lambda Developer Guide](#) oder unter [Building Lambda functions with Node.js](#).

Themen

- [Gültige Lambda-Werte](#)

- [Beispiele für Lambda-Funktionen](#)
- [Testen Sie Ihre Konfiguration](#)
- [Lambda-Funktionsvorlagen](#)

Gültige Lambda-Werte

In der folgenden Tabelle werden Details zu den Werten beschrieben, die Transfer Family für Lambda-Funktionen akzeptiert, die für benutzerdefinierte Identitätsanbieter verwendet werden.

Wert	Description	Erforderlich
Role	Gibt den Amazon-Ressourcennamen (ARN) der IAM-Rolle an, die den Zugriff Ihrer Benutzer auf Ihren Amazon S3-Bucket oder Ihr Amazon EFS-Dateisystem steuert. Die mit dieser Rolle verknüpften Richtlinien bestimmen die Zugriffsebene, die Sie Ihren Benutzern beim Übertragen von Dateien in und aus Ihrem Amazon S3- oder Amazon EFS-Dateisystem gewähren möchten. Die IAM-Rolle sollte außerdem eine Vertrauensstellung enthalten, mit der der Server Zugriff auf Ihre Ressourcen erhält, wenn er die Übertragungsanfragen Ihres Benutzers bearbeitet. Einzelheiten zum Aufbau einer Vertrauensbeziehung finden Sie unter So stellen Sie eine Vertrauensbeziehung her.	Erforderlich

Wert	Description	Erforderlich
PosixProfile	Die vollständige POSIX-Identität, einschließlich Benutzer-ID (Uid), Gruppen-ID (Gid) und aller sekundären Gruppen-IDs (Secondary Gids), die den Zugriff Ihrer Benutzer auf Ihre Amazon EFS-Dateisysteme steuert. Die POSIX-Berechtigungen, die für Dateien und Verzeichnisse in Ihrem Dateisystem festgelegt sind, bestimmen die Zugriffsebene, die Ihre Benutzer beim Übertragen von Dateien in und aus Ihren Amazon EFS-Dateisystemen erhalten.	Erforderlich für Amazon EFS-Backing-Speicher
PublicKeys	Eine Liste der Werte für öffentliche SSH-Schlüssel, die für diesen Benutzer gültig sind. Eine leere Liste bedeutet, dass dies kein gültiges Login ist. Darf bei der Passwortauthentifizierung nicht zurückgegeben werden.	Optional

Wert	Description	Erforderlich
Policy	Eine Sitzungsrichtlinie für Ihren Benutzer, sodass Sie dieselbe IAM-Rolle für mehrere Benutzer verwenden können. Diese Richtlinie grenzt den Benutzerzugriff auf Teile ihres Amazon S3-Buckets ein. Weitere Informationen zur Verwendung von Sitzungsrichtlinien mit benutzerdefinierten Identitätsanbietern finden Sie in den Beispielen für Sitzungsrichtlinien in diesem Thema.	Optional

Wert	Description	Erforderlich
HomeDirectoryType	Die Art des Zielverzeichnis (Ordnern), das das Home-Verzeichnis Ihrer Benutzer sein soll, wenn sie sich beim Server anmelden. • Wenn Sie es auf <code>einstellenPATH</code>, sieht der Benutzer die absoluten Amazon S3 S3-Bucket- oder Amazon EFS-Pfade wie in seinen File Transfer Protocol-Clients. • Wenn Sie es auf <code>einstellenLOGICAL</code>, müssen Sie im <code>HomeDirectoryDetails</code> Parameter Zuordnungen angeben, um Amazon S3- oder Amazon EFS-Pfade für Ihre Benutzer sichtbar zu machen.	Optional

Wert	Description	Erforderlich
HomeDirectoryDetails	Logische Verzeichniszuordnungen, die angeben, welche Amazon S3- oder Amazon EFS-Pfade und -Schlüssel für Ihren Benutzer sichtbar sein sollen und wie Sie sie sichtbar machen möchten. Sie müssen das Entry Target Und-Paar angeben, das Entry zeigt, wie der Pfad sichtbar gemacht Target wird und der tatsächliche Amazon S3- oder Amazon EFS-Pfad ist.	Erforderlich, wenn HomeDirectoryType es einen Wert von hat LOGICAL

Wert	Description	Erforderlich
HomeDirectory	Das Zielverzeichnis für einen Benutzer, wenn er sich über den Client am Server anmeldet. Das Format hängt von Ihrem Speicher-Backend ab: • Für Amazon S3: /bucket-name/user-home-directory Beispiel: /amzn-s3-demo-bucket/users/john • Für Amazon EFS: /fs-12345/user-home-directory Beispiel: /fs-faa1a123/users/john  Important Der Bucket-Name oder die Amazon EFS-Dateisystem-ID müssen im Pfad enthalten sein. Wenn Sie diese Informationen weglassen, treten bei Dateiübertragungen die Fehlermeldung „Datei nicht gefunden“ auf.	Optional

 Note

`HomeDirectoryDetails` ist eine Zeichenkettendarstellung einer JSON-Map. Dies steht im Gegensatz zu `PosixProfile`, was ein eigentliches JSON-Map-Objekt ist und `PublicKeys` welches ein JSON-Array von Zeichenketten ist. Die sprachspezifischen Details finden Sie in den Codebeispielen.

 HomeDirectory Anforderungen an das Format

Achten Sie bei der Verwendung des `HomeDirectory` Parameters darauf, dass Sie das vollständige Pfadformat angeben:

- Für Amazon S3 S3-Speicher: Geben Sie immer den Bucket-Namen im Format an `/bucket-name/path`
- Für Amazon EFS-Speicher: Geben Sie immer die Dateisystem-ID im Format an `/fs-12345/path`

Eine häufige Ursache für Fehler „Datei nicht gefunden“ ist das Auslassen des Bucket-Namens oder der EFS-Dateisystem-ID im `HomeDirectory` Pfad. Die Einstellung „`HomeDirectory`Nur / ohne Speicher-ID“ führt dazu, dass die Authentifizierung erfolgreich ist, Dateioperationen jedoch fehlschlagen.

Beispiele für Lambda-Funktionen

In diesem Abschnitt werden einige Lambda-Beispielfunktionen sowohl in NodeJS als auch in Python vorgestellt.

 Note

In diesen Beispielen sind der Benutzer, die Rolle, das POSIX-Profil, das Passwort und die Home-Verzeichnisdetails allesamt Beispiele und müssen durch Ihre tatsächlichen Werte ersetzt werden.

Logical home directory, NodeJS

Die folgende NodeJS-Beispielfunktion stellt die Details für einen Benutzer bereit, der über ein [logisches Home-Verzeichnis](#) verfügt.

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
      not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
  }
}
```

```

    }
    callback(null, response);
};

```

Path-based home directory, NodeJS

Die folgende NodeJS-Beispielfunktion stellt die Details für einen Benutzer bereit, der über ein pfadbasiertes Home-Verzeichnis verfügt.

```

// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
    console.log("Username:", event.username, "ServerId: ", event.serverId);

    var response;
    // Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    (e.g., "127.0.0.1") to further restrict logins.
    if (event.serverId !== "" && event.username == 'example-user') {
        response = {
            Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
            authenticated if and only if the Role field is not blank
            Policy: '', // Optional, JSON stringified blob to further restrict this user's
            permissions
            // HomeDirectory format depends on your storage backend:
            // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            users/john')
            // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
            replace with your bucket name
            // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
            for EFS
        };

        // Check if password is provided
        if (!event.password) {
            // If no password provided, return the user's SSH public key
            response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
            // Check if password is correct
        } else if (event.password !== 'Password1234') {

```

```

    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
  }
} else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
  }
  callback(null, response);
};

```

Logical home directory, Python

Die folgende Python-Beispielfunktion stellt die Details für einen Benutzer bereit, der über ein [logisches Home-Verzeichnis](#) verfügt.

```

# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
import json

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    if event['serverId'] != '' and event['username'] == 'example-user':
        homeDirectoryDetails = [
            {
                'Entry': '/',
                'Target': '/fs-faa1a123'
            }
        ]
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            be authenticated if and only if the Role field is not blank
            'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
            not needed for S3
            'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
            'HomeDirectoryType': "LOGICAL"
        }
    }

```



```

    # Check if password is provided
    if event.get('password', '') == '':
        # If no password provided, return the user's SSH public key
        response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}
    else:
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}

    return response

```

Path-based home directory, Python

Die folgende Python-Beispielfunktion stellt die Details für einen Benutzer bereit, der über ein pfadbasiertes Home-Verzeichnis verfügt.

```

# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    # (e.g., "127.0.0.1") to further restrict logins.
    if event['serverId'] != '' and event['username'] == 'example-user':
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'Policy': '', # Optional, JSON stringified blob to further restrict this
            # user's permissions
            # HomeDirectory format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            # users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')

```

```

    'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
    replace with your bucket name
    # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
    uncomment for EFS
    'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH
  }

  # Check if password is provided
  if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {}
    else:
      # Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {}

  return response

```

Testen Sie Ihre Konfiguration

Nachdem Sie Ihren benutzerdefinierten Identitätsanbieter erstellt haben, sollten Sie Ihre Konfiguration testen.

Console

Um Ihre Konfiguration mit der AWS Transfer Family Konsole zu testen

1. Öffnen Sie die [AWS Transfer Family -Konsole](#).
2. Wählen Sie auf der Seite Server Ihren neuen Server aus, klicken Sie auf Aktionen und dann auf Test.
3. Geben Sie den Text für Benutzername und Passwort ein, den Sie bei der Bereitstellung des CloudFormation Stacks festgelegt haben. Wenn Sie die Standardoptionen beibehalten haben, lautet der Benutzername myuser und das PasswortMySuperSecretPassword.


```

\"s3:GetObjectVersion\\\\\",\\\\\\\"s3:GetObjectVersion\\\\\\\"],\\\\\\\"Resource\\\\\\\":\\\\\\\"*\\\\\\\"}}\\\\\\\",
\"Role\\\\\\\":\\\\\\\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\\\\\\",\\\\\\\"HomeDirectory\\\\\\\":\\\\\\\"/
\\\\\\\"\\\\\\\"\",
  \"StatusCode\": 200,
  \"Message\": \"\"
}

```

Lambda-Funktionsvorlagen

Sie können einen CloudFormation Stack bereitstellen, der eine Lambda-Funktion zur Authentifizierung verwendet. Wir stellen mehrere Vorlagen zur Verfügung, mit denen Sie Ihre Benutzer mithilfe von Anmeldeinformationen authentifizieren und autorisieren können. Sie können diese Vorlagen oder den AWS Lambda Code ändern, um den Benutzerzugriff weiter anzupassen.

Note

Sie können einen FIPS-enabled AWS Transfer Family Server erstellen, CloudFormation indem Sie in Ihrer Vorlage eine FIPS-enabled Sicherheitsrichtlinie angeben. Die verfügbaren Sicherheitsrichtlinien werden unter beschrieben [Sicherheitsrichtlinien für Server AWS Transfer Family](#)

Um einen CloudFormation Stack für die Authentifizierung zu erstellen

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Folgen Sie den Anweisungen zum Bereitstellen eines CloudFormation Stacks anhand einer vorhandenen Vorlage im [Abschnitt Auswahl einer Stack-Vorlage](#) im AWS CloudFormation Benutzerhandbuch.
3. Verwenden Sie eine der folgenden Vorlagen, um eine Lambda-Funktion für die Authentifizierung in Transfer Family zu erstellen.

- [Klassische \(Amazon Cognito\) Stack-Vorlage](#)

Eine grundlegende Vorlage zum Erstellen einer Vorlage AWS Lambda zur Verwendung als benutzerdefinierter Identitätsanbieter in AWS Transfer Family. Es authentifiziert sich bei Amazon Cognito für die kennwortbasierte Authentifizierung und öffentliche Schlüssel werden aus einem Amazon S3 S3-Bucket zurückgegeben, wenn eine Authentifizierung auf Basis eines öffentlichen Schlüssels verwendet wird. Nach der Bereitstellung können Sie den Lambda-Funktionscode ändern, um etwas anderes zu tun.

- [AWS Secrets Manager Vorlage stapeln](#)

Eine grundlegende Vorlage, die AWS Lambda zusammen mit einem AWS Transfer Family Server verwendet wird, um Secrets Manager als Identitätsanbieter zu integrieren. Sie authentifiziert sich anhand eines Eintrags in AWS Secrets Manager diesem Formataws/`transfer/`*server-id/username*. Darüber hinaus muss das Geheimnis die Schlüssel-Wert-Paare für alle an Transfer Family zurückgegebenen Benutzereigenschaften enthalten. Nach der Bereitstellung können Sie den Lambda-Funktionscode ändern, um etwas anderes zu tun.

- [Okta-Stack-Vorlage](#): Eine Basisvorlage, die AWS Lambda zusammen mit einem AWS Transfer Family Server verwendet wird, um Okta als benutzerdefinierten Identitätsanbieter zu integrieren.
- [Okta-mfa Stack-Vorlage](#): Eine Basisvorlage, die AWS Lambda zusammen mit einem AWS Transfer Family Server zur Integration von Okta mit Multi-Faktor-Authentifizierung als benutzerdefiniertem Identitätsanbieter verwendet wird.
- [Azure Active Directory-Vorlage](#): Einzelheiten zu diesem Stack werden im Blogbeitrag [Authentifizierung AWS Transfer Family mit Azure Active Directory](#) und beschrieben. AWS Lambda

Nachdem der Stack bereitgestellt wurde, können Sie Details dazu auf der Registerkarte Aufgaben in der CloudFormation Konsole einsehen.

Die Bereitstellung eines dieser Stacks ist der einfachste Weg, einen benutzerdefinierten Identitätsanbieter in den Transfer Family Family-Workflow zu integrieren.

Verwenden Sie Amazon API Gateway zur Integration Ihres Identitätsanbieters

In diesem Thema wird beschrieben, wie Sie eine AWS Lambda Funktion verwenden, um eine API-Gateway-Methode zu unterstützen. Verwenden Sie diese Option, wenn Sie eine RESTful-API zur Integration Ihres Identitätsanbieters benötigen oder wenn Sie deren Funktionen für Geoblocking- oder Ratenbegrenzungsanfragen nutzen möchten. AWS WAF

In den meisten Anwendungsfällen wird empfohlen, einen benutzerdefinierten Identitätsanbieter zu konfigurieren, die Verwendung von. [Lösung für einen benutzerdefinierten Identitätsanbieter](#)

Einschränkungen bei der Verwendung eines API Gateway zur Integration Ihres Identitätsanbieters

- Diese Konfiguration unterstützt keine benutzerdefinierten Domänen.
- Diese Konfiguration unterstützt keine private API-Gateway-URL.

Wenn Sie eines davon benötigen, können Sie Lambda als Identitätsanbieter ohne API Gateway verwenden. Details hierzu finden Sie unter [Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet.](#)

Authentifizierung mit einer API-Gateway-Methode

Sie können eine API-Gateway-Methode zur Verwendung als Identitätsanbieter für Transfer Family erstellen. Dieser Ansatz bietet Ihnen eine äußerst sichere Möglichkeit, APIs zu erstellen und bereitzustellen. Mit API Gateway können Sie einen HTTPS-Endpunkt erstellen, sodass alle eingehenden API-Operationen mit größerer Sicherheit übertragen werden. Weitere Informationen zum API Gateway-Dienst finden Sie im [API Gateway Developer Guide](#).

API Gateway bietet eine Autorisierungsmethode mit dem Namen `AWS_IAM`, die Ihnen dieselbe Authentifizierung auf Basis von AWS Identity and Access Management (IAM) bietet, die auch intern AWS verwendet wird. Wenn Sie die Authentifizierung mit `aktivierenAWS_IAM` aktivieren, können nur Aufrufer mit ausdrücklichen Berechtigungen zum Aufrufen einer API die API-Gateway-Methode dieser API erreichen.

Um Ihre API Gateway Gateway-Methode als benutzerdefinierten Identitätsanbieter für Transfer Family zu verwenden, aktivieren Sie IAM für Ihre API Gateway Gateway-Methode. Im Rahmen dieses Prozesses stellen Sie eine IAM-Rolle mit Berechtigungen für Transfer Family bereit, Ihr Gateway zu verwenden.

Note

Um die Sicherheit zu verbessern, können Sie eine Firewall für Webanwendungen konfigurieren. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie die HTTP- und HTTPS-Anfragen überwachen können, die an ein Amazon API Gateway weitergeleitet werden. Details hierzu finden Sie unter [Fügen Sie eine Firewall für Webanwendungen hinzu.](#)

API-Gateway-Caching nicht aktivieren

Aktivieren Sie das Caching nicht für Ihre API-Gateway-Methode, wenn Sie sie als benutzerdefinierten Identitätsanbieter für Transfer Family verwenden. Caching ist aus folgenden Gründen unangemessen und für Authentifizierungsanfragen ungültig:

- Jede Authentifizierungsanfrage ist einzigartig und erfordert eine Live-Antwort, keine zwischengespeicherte Antwort
- Caching bietet keine Vorteile, da Transfer Family niemals doppelte oder wiederholte Anfragen an das API Gateway sendet.
- Wenn Sie das Caching aktivieren, antwortet das API Gateway mit nicht übereinstimmenden Daten, was zu ungültigen Antworten auf Authentifizierungsanfragen führt

So verwenden Sie Ihre API Gateway Gateway-Methode für die benutzerdefinierte Authentifizierung mit Transfer Family

1. Erstellen Sie einen CloudFormation Stapel. So gehen Sie vor:

Note

Die Stack-Vorlagen wurden aktualisiert und verwenden nun BASE64-encoded Passwörter: Einzelheiten finden Sie unter [Verbesserungen der Vorlagen CloudFormation](#).

- a. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
- b. Folgen Sie den Anweisungen zum Bereitstellen eines CloudFormation Stacks anhand einer vorhandenen Vorlage im [Abschnitt Auswahl einer Stack-Vorlage](#) im AWS CloudFormation Benutzerhandbuch.
- c. Verwenden Sie eine der folgenden Basisvorlagen, um eine AWS Lambda-gestützte API-Gateway-Methode zur Verwendung als benutzerdefinierter Identitätsanbieter in Transfer Family zu erstellen.
 - [Einfache Stack-Vorlage](#)

Standardmäßig wird Ihre API Gateway Gateway-Methode als benutzerdefinierter Identitätsanbieter verwendet, um einen einzelnen Benutzer auf einem einzelnen Server mithilfe eines hartcodierten SSH-Schlüssels (Secure Shell) oder eines Passworts zu authentifizieren. Nach der Bereitstellung können Sie den Lambda-Funktionscode ändern, um etwas anderes zu tun.

- [AWS Secrets Manager Vorlage stapeln](#)

Standardmäßig authentifiziert sich Ihre API Gateway Gateway-Methode anhand eines Eintrags im Secrets Manager des Formats `saws/transfer/`*server-id/username*. Darüber hinaus muss das Geheimnis die Schlüssel-Wert-Paare für alle an Transfer Family zurückgegebenen Benutzereigenschaften enthalten. Nach der Bereitstellung können Sie den Lambda-Funktionscode ändern, um etwas anderes zu tun. Weitere Informationen finden Sie im Blogbeitrag [Aktivieren der Kennwortauthentifizierung für die AWS Transfer Family Verwendung AWS Secrets Manager](#).

- [Okta-Stack-Vorlage](#)

Ihre API-Gateway-Methode lässt sich in Okta als benutzerdefinierter Identitätsanbieter in Transfer Family integrieren. Weitere Informationen finden Sie im Blogbeitrag [Okta als Identitätsanbieter verwenden mit](#). AWS Transfer Family

Die Bereitstellung eines dieser Stacks ist der einfachste Weg, einen benutzerdefinierten Identitätsanbieter in den Transfer Family Family-Workflow zu integrieren. Jeder Stack verwendet die Lambda-Funktion, um Ihre API-Methode auf Basis von API Gateway zu unterstützen. Anschließend können Sie Ihre API-Methode als benutzerdefinierten Identitätsanbieter in Transfer Family verwenden. Standardmäßig authentifiziert die Lambda-Funktion einen einzelnen Benutzer, der `myuser` mit dem Passwort aufgerufen wird. `MySuperSecretPassword` Nach der Bereitstellung können Sie diese Anmeldeinformationen bearbeiten oder den Lambda-Funktionscode aktualisieren, um etwas anderes zu tun.

 Important

Wir empfehlen, dass Sie die standardmäßigen Benutzer- und Kennwortanmeldedaten bearbeiten.

Nachdem der Stack bereitgestellt wurde, können Sie Details dazu auf der Registerkarte Ausgaben in der CloudFormation Konsole einsehen. Zu diesen Details gehören der Amazon-Ressourcenname (ARN) des Stacks, der ARN der IAM-Rolle, die der Stack erstellt hat, und die URL für Ihr neues Gateway.

 Note

Wenn Sie die Option des benutzerdefinierten Identitätsanbieters verwenden, um die passwortbasierte Authentifizierung für Ihre Benutzer zu aktivieren, und Sie die von API Gateway bereitgestellte Anfrage- und Antwortprotokollierung aktivieren, protokolliert API Gateway die Passwörter Ihrer Benutzer in Ihren Amazon Logs. CloudWatch Wir empfehlen nicht, dieses Protokoll in Ihrer Produktionsumgebung zu verwenden. Weitere Informationen finden Sie unter [CloudWatch API-Protokollierung in API Gateway einrichten](#) im API Gateway Developer Guide.

2. Überprüfen Sie die Konfiguration der API Gateway Gateway-Methode für Ihren Server. So gehen Sie vor:
 - a. Öffnen Sie die API Gateway Gateway-Konsole unter <https://console.aws.amazon.com/apigateway/>.
 - b. Wählen Sie die Basisvorlagen-API für Transfer Custom Identity Provider aus, die von der CloudFormation Vorlage generiert wurde. Möglicherweise müssen Sie Ihre Region auswählen, um Ihre Gateways zu sehen.
 - c. Wählen Sie im Bereich Ressourcen die Option GET aus. Der folgende Screenshot zeigt die korrekte Methodenkonfiguration.

The screenshot displays the AWS API Gateway console interface for configuring a new method. On the left, a sidebar shows a resource tree with paths: `/`, `/servers`, `/serverId`, `/users`, `/username`, and `/config`. The `GET` method is selected for the `/config` resource. The main panel shows the 'Method request settings' for the `GET` method. The settings include:

- Authorization:** AWS_IAM
- API key required:** False
- Request validator:** None
- SDK operation name:** Generated based on method and path
- Request paths (0):** No request paths defined.
- URL query string parameters (2):**

Name	Required	Caching
protocol	False	Inactive
sourceIp	False	Inactive
- HTTP request headers (1):**

Name	Required	Caching
PasswordBase64	False	Inactive
- Request body (0):** No request body defined.

Zu diesem Zeitpunkt ist Ihr API-Gateway bereit für die Bereitstellung.

- Wählen Sie für Aktionen die Option Deploy API aus. Wählen Sie für die Bereitstellungsphase die Option prod und dann Deploy aus.

Nachdem die API Gateway Gateway-Methode erfolgreich bereitgestellt wurde, können Sie sich ihre Leistung unter Stufen > Phasendetails ansehen, wie im folgenden Screenshot gezeigt.

Note

Kopieren Sie die Aufruf-URL-Adresse, die oben auf dem Bildschirm angezeigt wird. Möglicherweise benötigen Sie sie für den nächsten Schritt.

API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages

Stages

Stage actions ▼ Create stage

prod

Stage details info

Stage name: prod

API cache: ☐ Inactive

Rate: 10000

Burst: 5000

Web ACL: -

Client certificate: -

Invoke URL: <https://execute-api.us-east-1.amazonaws.com/prod>

Active deployment: t8aqrn on December 12, 2023, 10:49 (UTC-05:00)

Logs and tracing info

CloudWatch logs: Error and info logs

Detailed metrics: ☐ Inactive

X-Ray tracing: ☐ Inactive

Custom access logging: ☐ Inactive

Stage variables (0/0)

Find resources

No variables

No variables associated with the stage.

Manage variables

4. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
5. Eine Transfer Family sollte für Sie erstellt worden sein, als Sie den Stack erstellt haben. Wenn nicht, konfigurieren Sie Ihren Server mithilfe dieser Schritte.
 - a. Wählen Sie Server erstellen, um die Seite Server erstellen zu öffnen. Wählen Sie für Wählen Sie einen Identitätsanbieter die Option Benutzerdefiniert und dann Amazon API Gateway verwenden, um eine Verbindung zu Ihrem Identitätsanbieter herzustellen, wie im folgenden Screenshot gezeigt.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory**
Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Role
IAM role for the service to invoke your Amazon API Gateway URL

- b. Fügen Sie in das Textfeld Geben Sie eine Amazon API Gateway Gateway-URL ein die Aufruf-URL-Adresse des API Gateway-Endpunkts ein, den Sie in Schritt 3 dieses Verfahrens erstellt haben.
- c. Wählen Sie unter Rolle die IAM-Rolle aus, die mit der CloudFormation Vorlage erstellt wurde. Diese Rolle ermöglicht es Transfer Family, Ihre API-Gateway-Methode aufzurufen.

Die Aufrufrolle enthält den CloudFormation Stack-Namen, den Sie für den Stack ausgewählt haben, den Sie in Schritt 1 erstellt haben. Es hat das folgende Format: *CloudFormation-stack-name*-TransferIdentityProviderRole-*ABC123DEF456GHI*.

- d. Füllen Sie die verbleibenden Felder aus und wählen Sie dann Server erstellen. Einzelheiten zu den verbleibenden Schritten zum Erstellen eines Servers finden Sie unter [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#).

Implementierung Ihrer API-Gateway-Methode

Um einen benutzerdefinierten Identitätsanbieter für Transfer Family zu erstellen, muss Ihre API-Gateway-Methode eine einzelne Methode implementieren, die einen Ressourcenpfad von `/servers/{serverId}/users/{username}/config`. Die `username` Werte `serverId` und `username` stammen aus dem RESTful-Ressourcenpfad. Fügen Sie außerdem `sourceIp` und `protocol` als URL-Abfragezeichenfolgenparameter zur Methodenanforderung hinzu, wie in der folgenden Abbildung gezeigt.

The screenshot shows the AWS API Gateway console interface for configuring a GET method. The left sidebar shows the resource hierarchy: `/` > `/servers` > `/servers/{serverId}` > `/users` > `/users/{username}` > `/config` (selected). The main panel shows the method configuration for `/servers/{serverId}/users/{username}/config - GET - Method execution`.

Method execution flow: Client → Method request → Integration request → Lambda integration → Integration response → Method response → Client.

Method request settings:

- Authorization: `AWS_IAM`
- Request validator: `None`
- API key required: `False`
- SDK operation name: `Generated based on method and path`

Request paths (0): No request paths defined.

URL query string parameters (2):

Name	Required	Caching
<code>protocol</code>	<code>False</code>	Inactive
<code>sourceIp</code>	<code>False</code>	Inactive

Note

Der Benutzername muss mindestens 3 und maximal 100 Zeichen lang sein. Sie können die folgenden Zeichen im Benutzernamen verwenden: `a—z`, `0—9`, `A—Z`, Unterstrich `'_'`, Bindestrich `'-'`, Punkt `'.'` und das Zeichen `'@'`. Der Benutzername darf nicht mit einem Bindestrich `'-'`, einem Punkt `'.'` oder einem Zeichen `'@'` beginnen.

Wenn Transfer Family versucht, Ihren Benutzer mit einem Passwort zu authentifizieren, stellt der Dienst ein `Password: Header-Feld` bereit. In Ermangelung eines `Password: Headers` versucht Transfer Family, Ihren Benutzer mit einer Authentifizierung mit öffentlichem Schlüssel zu authentifizieren.

Wenn Sie einen Identitätsanbieter zur Authentifizierung und Autorisierung von Endbenutzern verwenden, können Sie neben der Überprüfung ihrer Anmeldeinformationen auch Zugriffsanfragen auf der Grundlage der IP-Adressen der von Ihren Endbenutzern verwendeten Clients zulassen oder ablehnen. Mit dieser Funktion können Sie sicherstellen, dass auf Daten, die in Ihren S3-Buckets oder Ihrem Amazon EFS-Dateisystem gespeichert sind, über die unterstützten Protokolle nur von IP-Adressen aus zugegriffen werden kann, die Sie als vertrauenswürdig angegeben haben. Um diese Funktion zu aktivieren, müssen Sie die `sourceIp` in der Abfragezeichenfolge angeben.

Wenn Sie mehrere Protokolle für Ihren Server aktiviert haben und den Zugriff mit demselben Benutzernamen über mehrere Protokolle ermöglichen möchten, können Sie dies tun, sofern die für jedes Protokoll spezifischen Anmeldeinformationen in Ihrem Identitätsanbieter eingerichtet wurden. Um diese Funktion zu aktivieren, müssen Sie den *protocol* Wert in den RESTful-Ressourcenpfad aufnehmen.

Ihre API Gateway Gateway-Methode sollte immer den HTTP-Statuscode zurückgeben `200`. Jeder andere HTTP-Statuscode bedeutet, dass beim Zugriff auf die API ein Fehler aufgetreten ist.

Amazon S3 S3-Beispielantwort

Der Beispiellantworttext ist ein JSON-Dokument der folgenden Form für Amazon S3.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

Der Richtlinie wird JSON als Zeichenfolge maskiert. Beispiel:

```

"Policy":
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
  [
    {\"Condition\":
      {\"StringLike\":
        {\"s3:prefix\":
          [\"user/*\", \"user/\"]}},
      \"Resource\": \"arn:aws:s3:::amzn-s3-demo-bucket\",
      \"Action\": \"s3:ListBucket\",
      \"Effect\": \"Allow\",
      \"Sid\": \"ListHomeDir\"},
    {\"Resource\": \"arn:aws:s3:::*\",
      \"Action\": [\"s3:PutObject\",
        \"s3:GetObject\",
        \"s3:DeleteObjectVersion\",
        \"s3:DeleteObject\",
        \"s3:GetObjectVersion\",
        \"s3:GetObjectACL\",
        \"s3:PutObjectACL\"],
      \"Effect\": \"Allow\",
      \"Sid\": \"HomeDirObjectAccess\"}]
}"

```

Die folgende Beispielantwort zeigt, dass ein Benutzer einen logischen Home-Verzeichnistyp hat.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\", \"Target\": \"/amzn-s3-demo-bucket1\"}]",
  "PublicKeys": ["" ]
}

```

Amazon EFS-Beispielantwort

Der Beispielantworttext ist ein JSON-Dokument der folgenden Form für Amazon EFS.

```

{

```

```

"Role": "IAM role with configured EFS permissions",
"PublicKeys": [
  "ssh-rsa public-key1",
  "ssh-rsa public-key2"
],
"PosixProfile": {
  "Uid": "POSIX user ID",
  "Gid": "POSIX group ID",
  "SecondaryGids": [Optional list of secondary Group IDs],
},
"HomeDirectory": "/fs-id/path/to/home/directory"
}

```

Das `Role` Feld zeigt, dass eine erfolgreiche Authentifizierung stattgefunden hat. Bei der Passwortauthentifizierung (wenn Sie einen `Password: Header` angeben), müssen Sie keine öffentlichen SSH-Schlüssel angeben. Wenn ein Benutzer nicht authentifiziert werden kann, z. B. wenn das Passwort falsch ist, sollte Ihre Methode eine Antwort zurückgeben, die nicht gesetzt ist. `Role` Ein Beispiel für eine solche Antwort ist ein leeres JSON-Objekt.

Die folgende Beispielantwort zeigt einen Benutzer mit einem logischen Home-Verzeichnistyp.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\"/\\\"\", \"Target\": \"\\\"/faa1a123\\\"\"}]",
  "PublicKeys": [""],
  "PosixProfile": {"Uid": 65534, "Gid": 65534}
}

```

Sie können Benutzerrichtlinien in die Lambda-Funktion im JSON-Format aufnehmen. Weitere Informationen zur Konfiguration von Benutzerrichtlinien in Transfer Family finden Sie unter [Verwaltung von Zugriffssteuerungen](#).

Standard-Lambda-Funktion

Um verschiedene Authentifizierungsstrategien zu implementieren, bearbeiten Sie die Lambda-Funktion, die Ihr Gateway verwendet. Um Ihnen zu helfen, die Anforderungen Ihrer Anwendung zu erfüllen, können Sie die folgenden Lambda-Beispielfunktionen in Node.js verwenden. Weitere Informationen zu Lambda finden Sie im [AWS Lambda Developer Guide](#) oder unter [Building Lambda functions with](#). Node.js

Die folgende Lambda-Beispielfunktion verwendet Ihren Benutzernamen, Ihr Passwort (wenn Sie eine Passwortauthentifizierung durchführen), Ihre Server-ID, Ihr Protokoll und Ihre Client-IP-Adresse. Sie können eine Kombination dieser Eingaben verwenden, um nach Ihrem Identitätsanbieter zu suchen und festzustellen, ob die Anmeldung akzeptiert werden soll.

 Note

Wenn Sie mehrere Protokolle für Ihren Server aktiviert haben und den Zugriff mit demselben Benutzernamen über mehrere Protokolle ermöglichen möchten, können Sie dies tun, sofern die für das Protokoll spezifischen Anmeldeinformationen in Ihrem Identitätsanbieter eingerichtet wurden.

Für das File Transfer Protocol (FTP) empfehlen wir, separate Anmeldeinformationen für Secure Shell (SSH) File Transfer Protocol (SFTP) und File Transfer Protocol over SSL (FTPS) zu verwenden. Wir empfehlen, separate Anmeldeinformationen für FTP zu verwenden, da FTP im Gegensatz zu SFTP und FTPS Anmeldeinformationen im Klartext überträgt. Wenn FTP-Anmeldeinformationen von SFTP oder FTPS isoliert werden, bleiben Ihre Workloads, die SFTP oder FTPS verwenden, sicher, wenn FTP-Anmeldeinformationen geteilt oder offengelegt werden.

Diese Beispielfunktion gibt die Rollen- und logischen Basisverzeichnisdetails zusammen mit den öffentlichen Schlüsseln zurück (sofern sie die Authentifizierung mit öffentlichen Schlüsseln durchführt).

Wenn Sie vom Service verwaltete Benutzer erstellen, legen Sie deren Basisverzeichnis fest, entweder logisch oder physisch. In ähnlicher Weise benötigen wir die Ergebnisse der Lambda-Funktion, um die gewünschte physische oder logische Verzeichnisstruktur des Benutzers zu vermitteln. Die von Ihnen festgelegten Parameter hängen vom Wert für das [HomeDirectoryType](#)-Feld ab.

- `HomeDirectoryType` gesetzt auf `PATH` — das `HomeDirectory`-Feld muss dann ein absolutes Amazon S3 S3-Bucket-Präfix oder ein absoluter Amazon EFS-Pfad sein, der für Ihre Benutzer sichtbar ist.
- `HomeDirectoryType` gesetzt auf `LOGICAL` — Legen Sie kein `HomeDirectory`-Feld fest. Stattdessen legen wir ein `HomeDirectoryDetails`-Feld fest, das die gewünschten Entry/Target Zuordnungen bereitstellt, ähnlich den im [HomeDirectoryDetails](#)-Parameter beschriebenen Werten für vom Service verwaltete Benutzer.

Die Beispielfunktionen sind unter aufgeführt. [Beispiele für Lambda-Funktionen](#)

Lambda-Funktion zur Verwendung mit AWS Secrets Manager

Um die AWS Secrets Manager als Identitätsanbieter zu verwenden, können Sie mit der Lambda-Funktion in der CloudFormation Beispielvorlage arbeiten. Die Lambda-Funktion fragt den Secrets Manager Manager-Dienst mit Ihren Anmeldeinformationen ab und gibt bei Erfolg ein bestimmtes Geheimnis zurück. Weitere Informationen zu Secrets Manager finden Sie im [Benutzerhandbuch für AWS Secrets Manager](#).

Um eine CloudFormation Beispielvorlage herunterzuladen, die diese Lambda-Funktion verwendet, rufen Sie den [Amazon S3 S3-Bucket auf, der von bereitgestellt wird AWS Transfer Family](#).

Verbesserungen der Vorlagen CloudFormation

An den veröffentlichten CloudFormation Vorlagen wurden Verbesserungen an der API Gateway Gateway-Schnittstelle vorgenommen. Die Vorlagen verwenden jetzt BASE64-encoded Passwörter mit dem API Gateway. Ihre bestehenden Bereitstellungen funktionieren auch ohne diese Erweiterung, lassen jedoch keine Passwörter mit Zeichen außerhalb des US-ASCII Basiszeichensatzes zu.

Die Änderungen in der Vorlage, die diese Funktion ermöglichen, lauten wie folgt:

- Die `GetUserConfigRequest` `AWS::ApiGateway::Method` Ressource muss diesen `RequestTemplates` Code haben (die kursiv gedruckte Zeile ist die aktualisierte Zeile)

```
RequestTemplates:
  application/json: |
    {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
        "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll("\
        \", \"'\")",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')",
    }
```

- Der Wert `RequestParameters` für die `GetUserConfig` Ressource muss geändert werden, damit der `PasswordBase64` Header verwendet werden kann (die kursiv gedruckte Zeile ist die aktualisierte Zeile):

```
RequestParameters:
```

```
method.request.header.PasswordBase64: false
method.request.querystring.protocol: false
method.request.querystring.sourceIp: false
```

Um zu überprüfen, ob die Vorlage für Ihren Stack die neueste ist

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Wählen Sie aus der Liste der Stacks Ihren Stack aus.
3. Wählen Sie im Detailbereich die Registerkarte Vorlage aus.
4. Achten Sie auf Folgendes:

- Suchen Sie nach dieser Zeile und stellen Sie sicherRequestTemplates, dass Sie sie haben:

```
"password":
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
    \',\'',\'"\')",
```

- Suchen Sie nach dieser Zeile und stellen Sie sicherRequestParameters, dass Sie sie haben:

```
method.request.header.PasswordBase64: false
```

Wenn Sie die aktualisierten Zeilen nicht sehen, bearbeiten Sie Ihren Stapel. Einzelheiten zum Aktualisieren Ihres CloudFormation Stacks finden Sie unter [Ändern einer Stack-Vorlage](#) im AWS CloudFormation; Benutzerhandbuch.

Verwendung mehrerer Authentifizierungsmethoden

Der Transfer Family Family-Server steuert die AND-Logik, wenn Sie mehrere Authentifizierungsmethoden verwenden. Transfer Family behandelt dies als zwei separate Anfragen an Ihren benutzerdefinierten Identitätsanbieter: Ihre Wirkung ist jedoch kombiniert.

Beide Anfragen müssen erfolgreich mit der richtigen Antwort zurückgegeben werden, damit die Authentifizierung abgeschlossen werden kann. Transfer Family setzt voraus, dass die beiden Antworten vollständig sind, d. h. sie enthalten alle erforderlichen Elemente (Rolle, Home-Verzeichnis, Richtlinie und das POSIX-Profil, wenn Sie Amazon EFS als Speicher verwenden). Transfer Family verlangt außerdem, dass die Passwortantwort keine öffentlichen Schlüssel enthalten darf.

Die Anfrage nach einem öffentlichen Schlüssel muss vom Identitätsanbieter separat beantwortet werden. Dieses Verhalten bleibt unverändert, wenn Password OR Key oder Password AND Key verwendet wird.

Das SSH/SFTP Protokoll fordert den Software-Client zunächst mit einer Authentifizierung mit einem öffentlichen Schlüssel auf und fordert dann eine Kennwortauthentifizierung an. Dieser Vorgang setzt voraus, dass beide erfolgreich sind, bevor der Benutzer die Authentifizierung abschließen kann.

Für benutzerdefinierte Identitätsanbieter-Optionen können Sie eine der folgenden Optionen für die Authentifizierung angeben.

- **Password ODER Schlüssel** — Benutzer können sich entweder mit ihrem Passwort oder ihrem Schlüssel authentifizieren. Dies ist der Standardwert.
- **NUR Passwort** — Benutzer müssen ihr Passwort angeben, um eine Verbindung herzustellen.
- **NUR Schlüssel** — Benutzer müssen ihren privaten Schlüssel angeben, um eine Verbindung herzustellen.
- **Password UND Schlüssel** — Benutzer müssen sowohl ihren privaten Schlüssel als auch ihr Passwort angeben, um eine Verbindung herzustellen. Der Server überprüft zuerst den Schlüssel. Wenn der Schlüssel gültig ist, fordert das System dann zur Eingabe eines Kennworts auf. Wenn der angegebene private Schlüssel nicht mit dem gespeicherten öffentlichen Schlüssel übereinstimmt, schlägt die Authentifizierung fehl.

IPv6-Unterstützung für benutzerdefinierte Identitätsanbieter

AWS Transfer Family benutzerdefinierte Identitätsanbieter unterstützen IPv6-Verbindungen vollständig. Bei der Implementierung eines benutzerdefinierten Identitätsanbieters kann Ihre Lambda-Funktion Authentifizierungsanfragen von IPv4- und IPv6-Clients ohne zusätzliche Konfiguration empfangen und verarbeiten. Die Lambda-Funktion empfängt die IP-Adresse des Clients im `sourceIp` Feld der Anfrage. Dabei kann es sich entweder um eine IPv4-Adresse (zum Beispiel `203.0.113.42`) oder eine IPv6-Adresse (zum Beispiel `2001:db8:85a3:8d3:1319:8a2e:370:7348`) handeln. Ihre benutzerdefinierte Identitätsanbieter-Implementierung sollte beide Adressformate angemessen handhaben.

Important

Wenn Ihr benutzerdefinierter Identitätsanbieter eine IP-based Validierung oder Protokollierung durchführt, stellen Sie sicher, dass Ihre Implementierung die IPv6-

Adressformate ordnungsgemäß verarbeitet. IPv6-Adressen sind länger als IPv4-Adressen und verwenden ein anderes Notationsformat.

 Note

Achten Sie bei der Verarbeitung von IPv6-Adressen in Ihrem benutzerdefinierten Identitätsanbieter darauf, dass Sie die richtigen Funktionen zur IPv6-Adressanalyse verwenden und nicht einfache Zeichenkettenvergleiche. IPv6-Adressen können in verschiedenen kanonischen Formaten dargestellt werden (z. B. oder). `fd00:b600::ec2` `fd00:b600:0:0:0:0:ec2` Verwenden Sie geeignete IPv6-Adressbibliotheken oder Funktionen in Ihrer Implementierungssprache, um IPv6-Adressen korrekt zu validieren und zu vergleichen.

Example Behandlung von IPv4- und IPv6-Adressen in einem benutzerdefinierten Identitätsanbieter

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

Weitere Informationen zur Implementierung benutzerdefinierter Identitätsanbieter finden Sie unter.

[Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet](#)

Verwenden des AWS Directory Service für Microsoft Active Directory

Sie können Endbenutzer verwenden AWS Transfer Family , um Ihre Dateiübertragung mithilfe AWS Directory Service for Microsoft Active Directory von zu authentifizieren. Es ermöglicht eine nahtlose Migration von Dateiübertragungsworkflows, die auf der Active Directory-Authentifizierung basieren, ohne die Anmeldeinformationen der Endbenutzer zu ändern oder einen benutzerdefinierten Autorisierer zu benötigen.

Mit AWS Managed Microsoft AD können Sie Directory Service Benutzern und Gruppen sicheren Zugriff über SFTP, FTPS und FTP auf Daten gewähren, die in Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) gespeichert sind. Wenn Sie Active Directory zum Speichern der Anmeldeinformationen Ihrer Benutzer verwenden, haben Sie jetzt eine einfachere Möglichkeit, Dateiübertragungen für diese Benutzer zu aktivieren.

Sie können den Zugriff auf Active Directory-Gruppen AWS Managed Microsoft AD in Ihrer lokalen Umgebung oder in der AWS Cloud mithilfe von Active Directory-Connectors bereitstellen. Sie können Benutzern, die bereits in Ihrer Microsoft Windows-Umgebung konfiguriert sind, entweder in der AWS Cloud oder in ihrem lokalen Netzwerk, Zugriff auf einen AWS Transfer Family Server gewähren, der AWS Managed Microsoft AD für die Identität verwendet wird. Der AWS Speicher-Blog enthält einen Beitrag, in dem eine Lösung für die Verwendung von Active Directory mit Transfer Family beschrieben wird: [Vereinfachen Sie die Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für AWS Transfer Family](#).

Note

- AWS Transfer Family unterstützt Simple AD nicht.
- Transfer Family unterstützt keine regionsübergreifenden Active Directory-Konfigurationen: Wir unterstützen nur Active Directory-Integrationen, die sich in derselben Region wie die des Transfer Family Family-Servers befinden.
- Transfer Family unterstützt AWS Managed Microsoft AD weder die Verwendung von AD Connector noch die Verwendung von AD Connector zur Aktivierung der Multi-Faktor-Authentifizierung (MFA) für Ihre bestehende RADIUS-based MFA-Infrastruktur.
- AWS Transfer Family unterstützt keine replizierten Regionen von Managed Active Directory.

Zur Verwendung AWS Managed Microsoft AD müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie mit der Directory Service Konsole ein oder mehrere AWS Managed Microsoft AD Verzeichnisse.
2. Verwenden Sie die Transfer Family Family-Konsole, um einen Server zu erstellen, der ihn AWS Managed Microsoft AD als Identitätsanbieter verwendet.
3. Richten Sie AWS Directory mit einem Active Directory Connector ein.
4. Fügen Sie Zugriff von einer oder mehreren Ihrer Directory Service Gruppen aus hinzu.
5. Obwohl dies nicht erforderlich ist, empfehlen wir Ihnen, den Benutzerzugriff zu testen und zu überprüfen.

Themen

- [Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory](#)
- [Arbeiten mit Active Directory-Bereichen](#)
- [Wählen Sie AWS Managed Microsoft AD als Ihren Identitätsanbieter](#)
- [Verbindung mit lokalem Microsoft Active Directory herstellen](#)
- [Zugriff auf Gruppen gewähren](#)
- [Benutzer werden getestet](#)
- [Serverzugriff für eine Gruppe wird gelöscht](#)
- [Mit SSH \(Secure Shell\) eine Verbindung zum Server herstellen](#)
- [Mithilfe von Gesamtstrukturen und Vertrauensstellungen eine Verbindung AWS Transfer Family zu einem selbstverwalteten Active Directory herstellen](#)

Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory

Note

AWS Transfer Family hat ein Standardlimit von 100 Active Directory-Gruppen pro Server. Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Geben Sie eine eindeutige Kennung für Ihre AD-Gruppen ein

Bevor Sie es verwenden können AWS Managed Microsoft AD, müssen Sie für jede Gruppe in Ihrem Microsoft AD-Verzeichnis eine eindeutige Kennung angeben. Sie können dazu die Sicherheits-ID (SID) für jede Gruppe verwenden. Die Benutzer der Gruppe, die Sie zuordnen, haben über die aktivierten Protokolle mithilfe von AWS Transfer Family Zugriff auf Ihre Amazon S3- oder Amazon EFS-Ressourcen.

Verwenden Sie den folgenden PowerShell Windows-Befehl, um die SID für eine Gruppe abzurufen, und *YourGroupName* ersetzen Sie sie durch den Namen der Gruppe.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName, ObjectSid
```

 Note

Wenn Sie AWS Directory Service als Identitätsanbieter verwenden und wenn `userPrincipalName` und unterschiedliche Werte `SamAccountName` haben, AWS Transfer Family akzeptiert der Wert in `SamAccountName`. Transfer Family akzeptiert den in angegebenen Wert nicht `userPrincipalName`.

Fügen Sie Ihrer Rolle Directory Service Berechtigungen hinzu

Sie benötigen außerdem Directory Service API-Berechtigungen, um sie AWS Directory Service als Ihren Identitätsanbieter verwenden zu können. Die folgenden Berechtigungen sind erforderlich oder werden empfohlen:

- `ds:DescribeDirectories` ist erforderlich, damit Transfer Family das Verzeichnis nachschlagen kann
- `ds:AuthorizeApplication` ist erforderlich, um die Autorisierung für Transfer Family hinzuzufügen
- `ds:UnauthorizeApplication` wird empfohlen, alle provisorisch erstellten Ressourcen zu entfernen, falls bei der Servererstellung etwas schief geht

Fügen Sie diese Berechtigungen der Rolle hinzu, die Sie für die Erstellung Ihrer Transfer Family Family-Server verwenden. Weitere Informationen zu diesen Berechtigungen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

Arbeiten mit Active Directory-Bereichen

Wenn Sie überlegen, wie Ihre Active Directory-Benutzer auf AWS Transfer Family Server zugreifen können, sollten Sie den Bereich des Benutzers und den Bereich seiner Gruppe berücksichtigen. Idealerweise sollten die Realm des Benutzers und der Realm seiner Gruppe übereinstimmen. Das heißt, sowohl der Benutzer als auch die Gruppe befinden sich im Standardbereich oder beide befinden sich im vertrauenswürdigen Bereich. Ist dies nicht der Fall, kann der Benutzer nicht von Transfer Family authentifiziert werden.

Sie können den Benutzer testen, um sicherzustellen, dass die Konfiguration korrekt ist. Details hierzu finden Sie unter [Benutzer werden getestet](#). Wenn es ein Problem mit dem user/group Bereich gibt, erhalten Sie die Fehlermeldung Kein zugeordneter Zugriff für Benutzergruppen gefunden.

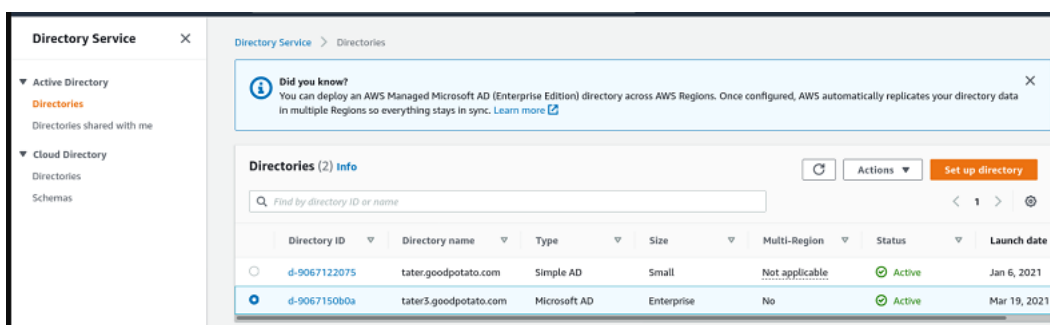
Wählen Sie AWS Managed Microsoft AD als Ihren Identitätsanbieter

In diesem Abschnitt wird die Verwendung AWS Directory Service for Microsoft Active Directory mit einem Server beschrieben.

Zur Verwendung AWS Managed Microsoft AD mit Transfer Family

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.

Verwenden Sie die Directory Service Konsole, um ein oder mehrere verwaltete Verzeichnisse zu konfigurieren. Weitere Informationen finden Sie unter [AWS Managed Microsoft AD](#) im Administratorhandbuch für Directory Service .



2. Öffnen Sie die AWS Transfer Family Konsole <https://console.aws.amazon.com/transfer/> unter und wählen Sie Server erstellen.
3. Wählen Sie auf der Seite „Protokolle auswählen“ ein oder mehrere Protokolle aus der Liste aus.

Note

Wenn Sie FTPS auswählen, müssen Sie das AWS Certificate Manager Zertifikat bereitstellen.

- Wählen Sie für Wählen Sie einen Identitätsanbieter die Option AWS Directory Service aus.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☒ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

Directory

TATER3 ▼ 

[Cancel](#)
[Previous](#)
[Next](#)

- Die Verzeichnisliste enthält alle verwalteten Verzeichnisse, die Sie konfiguriert haben. Wählen Sie ein Verzeichnis aus der Liste und klicken Sie auf Weiter.

Note

- Cross-Account und Gemeinsam genutzte Verzeichnisse werden für nicht unterstützt AWS Managed Microsoft AD.
- Um einen Server mit Directory Service als Identitätsanbieter einzurichten, müssen Sie einige Directory Service Berechtigungen hinzufügen. Details hierzu finden Sie unter [Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory](#).

- Verwenden Sie eines der folgenden Verfahren, um die Erstellung des Servers abzuschließen:

- [Erstellen Sie einen SFTP-enabled Server](#)
- [Einen FTPS-enabled Server erstellen](#)
- [Erstellen Sie einen FTP-enabled Server](#)

Fahren Sie in diesen Verfahren mit dem folgenden Schritt fort: Wählen Sie einen Identitätsanbieter.

 Important

Sie können ein Microsoft AD-Verzeichnis nicht löschen, Directory Service wenn Sie es auf einem Transfer Family Family-Server verwendet haben. Sie müssen zuerst den Server löschen, und dann können Sie das Verzeichnis löschen.

Verbindung mit lokalem Microsoft Active Directory herstellen

In diesem Abschnitt wird beschrieben, wie Sie ein AWS Verzeichnis mithilfe eines AD Connector einrichten.

So richten Sie Ihr AWS Verzeichnis mit AD Connector ein

1. Öffnen Sie die [Directory Service Service-Konsole](#) und wählen Sie Verzeichnisse aus.
2. Wählen Sie Verzeichnis einrichten aus.
3. Wählen Sie als Verzeichnistyp AD Connector aus.
4. Wählen Sie eine Verzeichnisgröße aus, klicken Sie auf Weiter und wählen Sie dann Ihre VPC und Subnetze aus.
5. Wählen Sie Weiter aus und füllen Sie dann die Felder wie folgt aus:
 - Verzeichnis-DNS-Name: Geben Sie den Domainnamen ein, den Sie für Ihr Microsoft Active Directory verwenden.
 - DNS-IP-Adressen: Geben Sie Ihre Microsoft Active Directory-IP-Adressen ein.
 - Benutzername und Passwort des Serverkontos: Geben Sie die Details für das zu verwendende Dienstkonto ein.
6. Füllen Sie die Bildschirme aus, um den Verzeichnisdienst zu erstellen.

Der nächste Schritt besteht darin, einen Transfer Family Family-Server mit dem SFTP-Protokoll und dem Identitätsanbieter AWS Directory Service zu erstellen. Wählen Sie in der Dropdownliste Verzeichnis das Verzeichnis aus, das Sie im vorherigen Verfahren hinzugefügt haben.

Zugriff auf Gruppen gewähren

Nachdem Sie den Server erstellt haben, müssen Sie auswählen, welche Gruppen im Verzeichnis Zugriff auf das Hoch- und Herunterladen von Dateien über die aktivierten Protokolle haben sollen AWS Transfer Family. Dazu erstellen Sie einen Zugriff.

Note

AWS Transfer Family hat ein Standardlimit von 100 Active Directory-Gruppen pro Server. Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Note

Benutzer müssen direkt zu der Gruppe gehören, der Sie Zugriff gewähren. Nehmen wir beispielsweise an, dass Bob ein Benutzer ist und zu Gruppe A gehört und dass Gruppe A selbst in Gruppe B enthalten ist.

- Wenn Sie Zugriff auf Gruppe A gewähren, wird Bob Zugriff gewährt.
- Wenn Sie Zugriff auf Gruppe B (und nicht auf Gruppe A) gewähren, hat Bob keinen Zugriff.

Um einer Gruppe Zugriff zu gewähren

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Navigieren Sie zu Ihrer Serverdetailseite.
3. Wählen Sie im Abschnitt Zugriffe die Option Zugriff hinzufügen aus.
4. Geben Sie die SID für das AWS Managed Microsoft AD Verzeichnis ein, auf das Sie Zugriff auf diesen Server haben möchten.

 Note

Informationen darüber, wie Sie die SID für Ihre Gruppe finden, finden Sie unter [the section called “Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory”](#).

5. Wählen Sie für Access eine AWS Identity and Access Management (IAM-) Rolle für die Gruppe aus.
6. Wählen Sie im Abschnitt Richtlinie eine Richtlinie aus. Die Standardeinstellung ist Keine.
7. Wählen Sie für Home-Verzeichnis einen Amazon S3 S3-Bucket aus, der dem Home-Verzeichnis der Gruppe entspricht.

 Note

Sie können die Teile des Buckets einschränken, die Benutzer sehen, indem Sie eine Sitzungsrichtlinie erstellen. Um beispielsweise Benutzer auf ihren eigenen Ordner im / filetest Verzeichnis zu beschränken, geben Sie den folgenden Text in das Feld ein.

```
/filetest/${transfer:UserName}
```

Weitere Informationen zum Erstellen einer Sitzungsrichtlinie finden Sie unter [Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#).

8. Wählen Sie Hinzufügen, um die Zuordnung zu erstellen.
9. Wählen Sie Ihren Server aus.
10. Wählen Sie Zugriff hinzufügen.
 - Geben Sie die SID für die Gruppe ein.

 Note

Informationen darüber, wie Sie die SID finden, finden Sie unter [the section called “Bevor Sie mit der Verwendung beginnen AWS Directory Service for Microsoft Active Directory”](#).

11. Wählen Sie Zugriff hinzufügen aus.

Im Bereich Zugriffe werden die Zugriffe für den Server aufgelistet.

The screenshot displays the AWS Transfer Family console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', the 'Subnet ID' as 'subnet-...', and the 'Private IPv4 Address' as '172.31.80.36'. Below this, the 'Accesses (1)' section features a search bar, an 'Actions' dropdown menu, and an 'Associate access' button. A table lists the access details with columns for 'External Id', 'Home directory', and 'Role'. The table contains one entry: 'S...' for 'External Id', '/padbucket3' for 'Home directory', and 'ADGuy_S3_And_EFS' for 'Role'. The 'Additional details' section at the bottom includes 'Logging role' (Server activity not logged to Amazon CloudWatch), 'Server host key', 'Security Policy' (TransferSecurityPolicy-2018-11), and 'Domain' (Amazon S3). An 'Edit' button is located in the top right of the 'Additional details' section.

Benutzer werden getestet

Sie können testen, ob ein Benutzer Zugriff auf das AWS Managed Microsoft AD Verzeichnis für Ihren Server hat.

Note

Ein Benutzer muss zu genau einer Gruppe gehören (eine externe ID), die im Abschnitt Zugriff auf der Endpunktkonfigurationsseite aufgeführt ist. Wenn der Benutzer keiner oder mehreren Gruppen angehört, wird diesem Benutzer kein Zugriff gewährt.

Um zu testen, ob ein bestimmter Benutzer Zugriff hat

1. Wählen Sie auf der Seite mit den Serverdetails Aktionen und dann Test aus.
2. Geben Sie zum Testen des Identitätsanbieters die Anmeldeinformationen für einen Benutzer ein, der zu einer der Gruppen gehört, die Zugriff haben.
3. Wählen Sie Test aus.

Sie sehen einen erfolgreichen Identitätsanbieter-Test, der zeigt, dass dem ausgewählten Benutzer Zugriff auf den Server gewährt wurde.

Identity provider testing

User configuration [Info](#)

Username

Password

Response

```
{
  "Response": "
  {\"homeDirectory\":\"/padbucket3\", \"homeDirectoryDetails\":null, \"homeDirectoryType\":\"PATH\", \"posixProfile\":
  null, \"publicKeys\":null, \"role\":\"arn:aws:iam::195886157073:role/ADGuy_53_Aud_EFS\", \"policy\":\"mail\", \"userNa
  me\":\"transferuser1\", \"identityProviderType\":null, \"userConfigMessage\":null}",
  "StatusCode": 200,
  "Message": ""
}
```

Cancel

Test

Wenn der Benutzer zu mehr als einer Gruppe gehört, die Zugriff hat, erhalten Sie die folgende Antwort.

```
"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."
```

Serverzugriff für eine Gruppe wird gelöscht

Um den Serverzugriff für eine Gruppe zu löschen

1. Wählen Sie auf der Seite mit den Serverdetails Aktionen und anschließend Zugriff löschen aus.
2. Bestätigen Sie im Dialogfeld, dass Sie den Zugriff für diese Gruppe entfernen möchten.

Wenn Sie zur Seite mit den Serverdetails zurückkehren, sehen Sie, dass der Zugriff für diese Gruppe nicht mehr aufgeführt ist.

Mit SSH (Secure Shell) eine Verbindung zum Server herstellen

Nachdem Sie Ihren Server und Ihre Benutzer konfiguriert haben, können Sie über SSH eine Verbindung zum Server herstellen und den vollqualifizierten Benutzernamen für einen Benutzer verwenden, der Zugriff hat.

```
sftp user@active-directory-domain@vpc-endpoint
```

Beispiel: `transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`.

Dieses Format zielt auf die Suche im Verbund ab und schränkt die Suche in einem potenziell großen Active Directory ein.

Note

Sie können den einfachen Benutzernamen angeben. In diesem Fall muss der Active Directory-Code jedoch alle Verzeichnisse im Verbund durchsuchen. Dadurch kann die Suche eingeschränkt werden, und die Authentifizierung schlägt möglicherweise fehl, selbst wenn der Benutzer Zugriff haben sollte.

Nach der Authentifizierung befindet sich der Benutzer in dem Basisverzeichnis, das Sie bei der Konfiguration des Benutzers angegeben haben.

Mithilfe von Gesamtstrukturen und Vertrauensstellungen eine Verbindung AWS Transfer Family zu einem selbstverwalteten Active Directory herstellen

Directory Service bietet die folgenden Optionen, um eine Verbindung zu einem selbstverwalteten Active Directory herzustellen:

- One-way Forest Trust (ausgehend von AWS Managed Microsoft AD und eingehend für lokales Active Directory) funktioniert nur für die Stammdomäne.
- Für untergeordnete Domänen können Sie eine der folgenden Optionen verwenden:
 - Verwenden Sie bidirektionale Vertrauensstellung zwischen AWS Managed Microsoft AD und lokalem Active Directory

- Verwenden Sie für jede untergeordnete Domäne eine unidirektionale externe Vertrauensstellung.

Wenn der Benutzer über eine vertrauenswürdige Domäne eine Verbindung zum Server herstellt, muss er beispielsweise `transferuserexample@mycompany.com` die vertrauenswürdige Domäne angeben.

Verwenden des AWS Directory Service für Entra ID Domain Services

Für Kunden, die nur SFTP-Transfer benötigen und keine Domain verwalten möchten, gibt es Simple Active Directory. Alternativ können Kunden, die die Vorteile von Active Directory und hoher Verfügbarkeit in einem vollständig verwalteten Dienst nutzen möchten, AWS Managed Microsoft AD verwenden. Und für Kunden, die ihre bestehende Active Directory-Gesamtstruktur für ihre SFTP-Übertragung nutzen möchten, gibt es den Active Directory Connector.

Beachten Sie Folgendes:

- Um Ihre bestehende Active Directory-Gesamtstruktur für Ihre SFTP-Übertragungsanforderungen zu nutzen, können Sie [Active Directory Connector](#) verwenden.
- Wenn Sie die Vorteile von Active Directory und hoher Verfügbarkeit in einem vollständig verwalteten Dienst nutzen möchten, können Sie Folgendes verwenden AWS Directory Service for Microsoft Active Directory. Details hierzu finden Sie unter [Verwenden des AWS Directory Service für Microsoft Active Directory](#).

In diesem Thema wird beschrieben, wie Sie einen Active Directory-Connector und [Entra ID-Domänendienste \(früher Azure AD\)](#) verwenden, um SFTP-Übertragungsbenutzer mit Entra ID zu authentifizieren.

Themen

- [Bevor Sie beginnen, AWS Directory Service für Entra ID Domain Services zu verwenden](#)
- [Schritt 1: Hinzufügen von Entra ID Domain Services](#)
- [Schritt 2: Ein Dienstkonto erstellen](#)
- [Schritt 3: AWS Verzeichnis mit AD Connector einrichten](#)
- [Schritt 4: AWS Transfer Family Server einrichten](#)
- [Schritt 5: Zugriff auf Gruppen gewähren](#)
- [Schritt 6: Benutzer testen](#)

Bevor Sie beginnen, AWS Directory Service für Entra ID Domain Services zu verwenden

 Note

AWS Transfer Family hat ein Standardlimit von 100 Active Directory-Gruppen pro Server. Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Für AWS benötigen Sie Folgendes:

- Eine virtuelle private Cloud (VPC) in einer AWS Region, in der Sie Ihre Transfer Family Family-Server verwenden
- Mindestens zwei private Subnetze in Ihrer VPC
- Die VPC muss über eine Internetverbindung verfügen
- Ein Kunden-Gateway und ein virtuelles privates Gateway für eine Site-to-Site-VPN-Verbindung mit Microsoft Entra

Für Microsoft Entra benötigen Sie Folgendes:

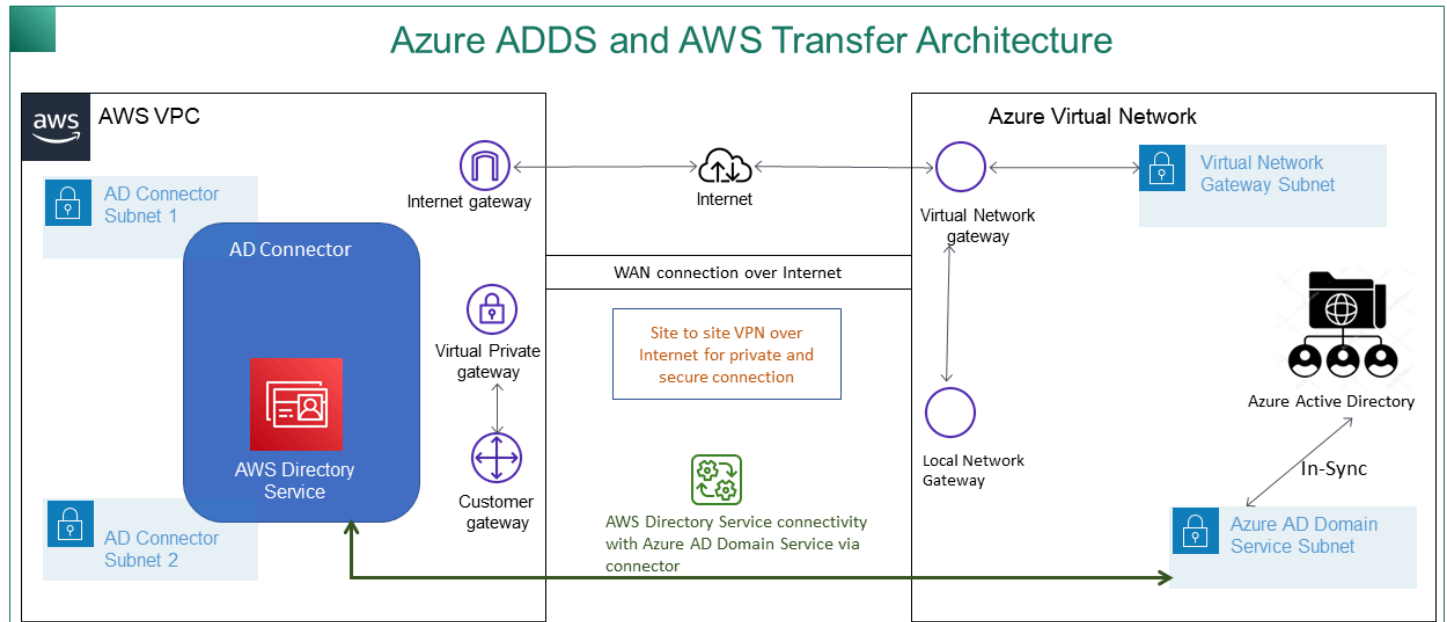
- Eine Entra-ID und ein Active Directory-Domänendienst
- Eine Entra-Ressourcengruppe
- Ein virtuelles Entra-Netzwerk
- VPN-Konnektivität zwischen Ihrer Amazon VPC und Ihrer Entra-Ressourcengruppe

 Note

Dies kann über native IPSEC-Tunnel oder mithilfe von VPN-Appliances erfolgen. In diesem Thema verwenden wir IPSEC-Tunnel zwischen einem virtuellen Entra-Netzwerk-Gateway und einem lokalen Netzwerk-Gateway. Die Tunnel müssen so konfiguriert sein, dass sie den Verkehr zwischen Ihren Entra Domain Service-Endpunkten und den Subnetzen, in denen sich Ihre VPC befindet, zulassen. AWS

- Ein Kunden-Gateway und ein virtuelles privates Gateway für eine Site-to-Site-VPN-Verbindung mit Microsoft Entra

Das folgende Diagramm zeigt die Konfiguration, die erforderlich ist, bevor Sie beginnen.



Schritt 1: Hinzufügen von Entra ID Domain Services

Entra ID unterstützt standardmäßig keine Domänenbeitritte. Um Aktionen wie den Domänenbeitritt durchzuführen und Tools wie Gruppenrichtlinien zu verwenden, müssen Administratoren die Entra ID Domain Services aktivieren. Wenn Sie Entra DS noch nicht hinzugefügt haben oder Ihre bestehende Implementierung nicht mit der Domain verknüpft ist, die Ihr SFTP-Übertragungsserver verwenden soll, müssen Sie eine neue Instanz hinzufügen.

Informationen zur Aktivierung der Entra ID Domain Services finden Sie unter [Tutorial: Erstellen und Konfigurieren einer von Microsoft Entra Domain Services verwalteten Domain Services](#).

Note

Wenn Sie Entra DS aktivieren, stellen Sie sicher, dass es für die Ressourcengruppe und die Entra-Domäne konfiguriert ist, mit der Sie Ihren SFTP-Übertragungsserver verbinden.

The screenshot shows the Azure AD Domain Services interface for the **bob.us** domain. On the left, there is a navigation pane with options: Overview (selected), Activity log, Access control (IAM), Tags, Settings, and Properties. The main area displays a warning message: "Configuration issues for your managed domain were detected. Run configuration diagnostics". Below this, the domain **bob.us** is shown with a status of "Running" (indicated by a green checkmark) and a "View health" button.

Schritt 2: Ein Dienstkonto erstellen

Entra muss über ein Dienstkonto verfügen, das Teil einer Admin-Gruppe in Entra DS ist. Dieses Konto wird mit dem AWS Active Directory-Connector verwendet. Stellen Sie sicher, dass dieses Konto mit Entra DS synchronisiert ist.

[Home](#) > [Default Directory](#) > [Users](#) > [bobatusa](#)

The screenshot shows the Microsoft Entra ID user profile page for the user **bobatusa**. The page includes a navigation pane on the left with options: Profile (selected), Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods. The main area displays the user's profile information, including the email address **bobsmith@xyz.com** and a pink circular profile picture with the initials "SU". Below the profile picture, the creation time is listed as "10/6/2021, 1:32:27 AM". To the right, there is a "User Sign-ins" chart showing a single sign-in event on October 31. Below the chart, the "Group memberships" section shows that the user is a member of 2 groups. At the bottom, the "Identity" section provides details about the user's name, principal name, and user type.

Property	Value
Name	bobatusa
User Principal Name	bobsmith@xyz.com
First name	Bob
Last name	Smith
User type	Member

Tip

Multi-factor Die Authentifizierung für Entra ID wird für Transfer Family Family-Server, die das SFTP-Protokoll verwenden, nicht unterstützt. Der Transfer Family Family-Server kann das MFA-Token nicht bereitstellen, nachdem sich ein Benutzer bei SFTP authentifiziert hat. Stellen Sie sicher, dass MFA deaktiviert ist, bevor Sie versuchen, eine Verbindung herzustellen.

multi-factor authentication
users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

☐ DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
☐ Christopher	admin@christopher[REDACTED].com	Disabled
☐ Robert	test@christopher[REDACTED].com	Disabled

Select a user

Schritt 3: AWS Verzeichnis mit AD Connector einrichten

Nachdem Sie Entra DS konfiguriert und ein Dienstkonto mit IPSEC-VPN-Tunneln zwischen Ihrer AWS VPC und dem Entra Virtual Network erstellt haben, können Sie die Konnektivität testen, indem Sie die Entra DS-DNS-IP-Adresse von einer beliebigen EC2-Instance aus pingen. AWS

Nachdem Sie sich vergewissert haben, dass die Verbindung aktiv ist, können Sie weiter unten fortfahren.

So richten Sie Ihr AWS Verzeichnis mit AD Connector ein

1. Öffnen Sie die [Directory Service Service-Konsole](#) und wählen Sie Verzeichnisse aus.
2. Wählen Sie Verzeichnis einrichten aus.
3. Wählen Sie als Verzeichnistyp AD Connector aus.
4. Wählen Sie eine Verzeichnisgröße aus, wählen Sie Weiter und dann Ihre VPC und Subnetze aus.
5. Wählen Sie Weiter aus und füllen Sie dann die Felder wie folgt aus:

- DNS-Name des Verzeichnisses: Geben Sie den Domainnamen ein, den Sie für Ihren Entra DS verwenden.
- DNS-IP-Adressen: Geben Sie Ihre Entra DS-IP-Adressen ein.
- Benutzername und Passwort für das Serverkonto: Geben Sie die Details für das Dienstkonto ein, das Sie in Schritt 2: Dienstkonto erstellen erstellt haben.

6. Füllen Sie die Bildschirme aus, um den Verzeichnisdienst zu erstellen.

Jetzt sollte der Verzeichnisstatus Aktiv lauten und es kann mit einem SFTP-Übertragungsserver verwendet werden.

Directory Service > Directories

 **Did you know?**
 You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)

Find by directory ID or name






 1
 


Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
 d-906752c0d7	 	AD Connector	Small	Not applicable	 Active	Nov 3, 2021

Schritt 4: AWS Transfer Family Server einrichten

Erstellen Sie einen Transfer Family Family-Server mit dem SFTP-Protokoll und dem Identitätsanbieter AWS Directory Service. Wählen Sie aus der Dropdownliste Verzeichnis das Verzeichnis aus, das Sie in Schritt 3: AWS Verzeichnis mit AD Connector einrichten hinzugefügt haben.

Note

Sie können ein Microsoft AD-Verzeichnis nicht im AWS Directory Service löschen, wenn Sie es auf einem Transfer Family Family-Server verwendet haben. Sie müssen zuerst den Server löschen, und dann können Sie das Verzeichnis löschen.

Schritt 5: Zugriff auf Gruppen gewähren

Nachdem Sie den Server erstellt haben, müssen Sie auswählen, welche Gruppen im Verzeichnis Zugriff auf das Hoch- und Herunterladen von Dateien über die aktivierten Protokolle haben sollen AWS Transfer Family. Sie tun dies, indem Sie einen Zugriff erstellen.

Note

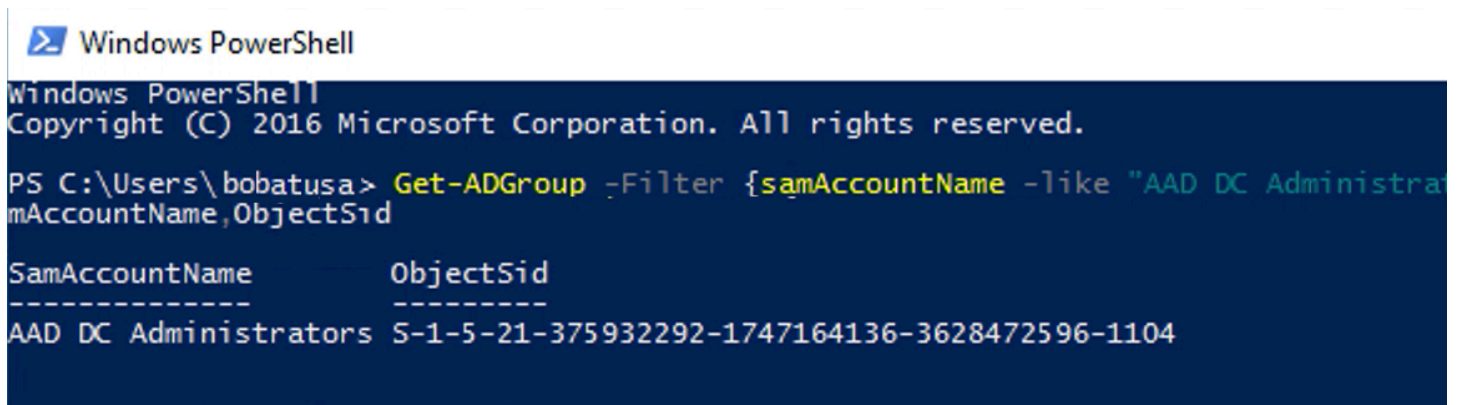
Benutzer müssen direkt zu der Gruppe gehören, der Sie Zugriff gewähren. Nehmen wir beispielsweise an, dass Bob ein Benutzer ist und zu Gruppe A gehört und dass Gruppe A selbst in Gruppe B enthalten ist.

- Wenn Sie Zugriff auf Gruppe A gewähren, wird Bob Zugriff gewährt.
- Wenn Sie Zugriff auf Gruppe B (und nicht auf Gruppe A) gewähren, hat Bob keinen Zugriff.

Um Zugriff zu gewähren, müssen Sie die SID für die Gruppe abrufen.

Verwenden Sie den folgenden PowerShell Windows-Befehl, um die SID für eine Gruppe abzurufen, und *YourGroupName* ersetzen Sie sie durch den Namen der Gruppe.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName, ObjectSid
```



```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrators*"} -Properties * | Select SamAccountName, ObjectSid  
  
SamAccountName      ObjectSid  
-----  
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

Gewähren Sie Gruppen Zugriff

1. Öffnen Sie <https://console.aws.amazon.com/transfer/>.
2. Navigieren Sie zu Ihrer Serverdetailseite und wählen Sie im Bereich Zugriffe die Option Zugriff hinzufügen aus.

3. Geben Sie die SID ein, die Sie aus der Ausgabe des vorherigen Verfahrens erhalten haben.
4. Wählen Sie für Access eine AWS Identity and Access Management Rolle für die Gruppe aus.
5. Wählen Sie im Abschnitt Richtlinie eine Richtlinie aus. Der Standardwert ist None (Kein).
6. Wählen Sie für Home-Verzeichnis einen Amazon S3 S3-Bucket aus, der dem Home-Verzeichnis der Gruppe entspricht.
7. Wählen Sie Hinzufügen, um die Zuordnung zu erstellen.

Die Details von Ihrem Transferserver sollten etwa wie folgt aussehen:

The screenshot displays the AWS Transfer Family console interface. It is divided into two main sections: 'Protocols' and 'Identity provider'. Below these is a table titled 'Accesses (1)'.

Protocols: A section with an 'Edit' button. It contains the text 'Protocols over which clients can connect to your server's endpoint' and a list with one item: 'SFTP'.

Identity provider: A section with an 'Edit' button. It contains the text 'Identity provider type' with the value 'AWS Directory Service'. Below this is 'Directory ID' with the value 'd-123456789a'.

Accesses (1): A table with columns: 'External Id', 'Home directory', and 'Role'. There is a search bar and 'Actions' and 'Add access' buttons at the top right of the table.

	External Id	Home directory	Role
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/s3/transfer-fs	sftp-user-role ↗

Schritt 6: Benutzer testen

Sie können testen ([Benutzer werden getestet](#)), ob ein Benutzer Zugriff auf das AWS Managed Microsoft AD Verzeichnis für Ihren Server hat. Ein Benutzer muss zu genau einer Gruppe gehören (eine externe ID), die im Abschnitt Zugriff auf der Endpunktkonfigurationsseite aufgeführt ist. Wenn der Benutzer keiner Gruppe angehört oder zu mehr als einer einzigen Gruppe gehört, wird diesem Benutzer kein Zugriff gewährt.

Verwendung logischer Verzeichnisse zur Vereinfachung Ihrer Transfer Family Family-Verzeichnisstrukturen

Logische Verzeichnisse vereinfachen die Verzeichnisstruktur Ihres AWS Transfer Family Servers. Mit logischen Verzeichnissen können Sie eine virtuelle Verzeichnisstruktur mit benutzerfreundlichen Namen erstellen, anhand derer Benutzer navigieren, wenn sie eine Verbindung zu Ihrem Amazon S3

S3-Bucket oder Amazon EFS-Dateisystem herstellen. Dadurch wird verhindert, dass Benutzer die tatsächlichen Verzeichnispfade, Bucket-Namen und Dateisystemnamen sehen.

Note

Sie sollten Sitzungsrichtlinien verwenden, damit Ihre Endbenutzer nur Vorgänge ausführen können, deren Ausführung Sie ihnen gestatten.

Sie sollten logische Verzeichnisse verwenden, um ein benutzerfreundliches, virtuelles Verzeichnis für Ihre Endbenutzer zu erstellen und Bucket-Namen zu abstrahieren. Logische Verzeichniszuordnungen ermöglichen Benutzern nur den Zugriff auf die ihnen zugewiesenen logischen Pfade und Unterverzeichnisse und verbieten relative Pfade, die die logischen Wurzeln durchqueren.

Transfer Family überprüft jeden Pfad, der relative Elemente enthalten könnte, und blockiert aktiv die Auflösung dieser Pfade, bevor wir diese Pfade an Amazon S3 übergeben. Dadurch wird verhindert, dass Ihre Benutzer ihre logischen Zuordnungen verlassen.

Transfer Family verhindert zwar, dass Ihre Endbenutzer auf Verzeichnisse außerhalb ihres logischen Verzeichnisses zugreifen, wir empfehlen Ihnen jedoch, auch eindeutige Rollen oder Sitzungsrichtlinien zu verwenden, um die geringsten Rechte auf Speicherebene durchzusetzen.

Grundlegendes zur Chroot- und Verzeichnisstruktur

Mit einer Chroot-Operation können Sie das Stammverzeichnis eines Benutzers auf eine beliebige Stelle in Ihrer Speicherhierarchie setzen. Dadurch werden Benutzer auf ihr konfiguriertes Home- oder Stammverzeichnis beschränkt, wodurch der Zugriff auf Verzeichnisse auf höherer Ebene verhindert wird.

Stellen Sie sich einen Fall vor, in dem ein Amazon S3 S3-Benutzer auf Folgendes beschränkt ist `amzn-s3-demo-bucket/home/${transfer:UserName}`. Ohne Chroot könnten einige Clients Benutzern erlauben, zu `/amzn-s3-demo-` zu wechseln, sodass sie sich abmelden und anmelden müssen `bucket/home`, um zum richtigen Verzeichnis zurückzukehren. Das Ausführen eines Chroot-Vorgangs verhindert dieses Problem.

Sie können benutzerdefinierte Verzeichnisstrukturen für mehrere Buckets und Präfixe erstellen. Dies ist nützlich, wenn Ihr Workflow ein bestimmtes Verzeichnislayout erfordert, das Bucket-Präfixe allein nicht bereitstellen können. Sie können auch Links zu mehreren nicht zusammenhängenden Speicherorten innerhalb von Amazon S3 erstellen, ähnlich wie beim Erstellen eines symbolischen

Links in einem Linux-Dateisystem, in dem Ihr Verzeichnispfad auf einen anderen Speicherort im Dateisystem verweist.

Regeln für die Verwendung logischer Verzeichnisse

In diesem Abschnitt werden einige Regeln und andere Überlegungen zur Verwendung logischer Verzeichnisse beschrieben.

Grenzwerte zuordnen

- Wenn ja, ist nur eine Zuordnung zulässig "/" (Entries sind keine überlappenden Pfade zulässig).
- Logische Verzeichnisse unterstützen Zuordnungen von bis zu 2,1 MB für benutzerdefinierte IDP- und AD-Benutzer und 2.000 Einträge für vom Service verwaltete Benutzer. Sie können die Größe Ihrer Zuordnungen wie folgt berechnen:
 1. Schreiben Sie ein typisches Mapping in dem Format aus{"Entry": "/"*entry-path*", "Target": "/"*target-path*"}, wo *entry-path* und wo die tatsächlichen Werte *target-path* sind, die Sie verwenden werden.
 2. Zählen Sie die Zeichen in dieser Zeichenfolge und fügen Sie dann eins hinzu (1).
 3. Multiplizieren Sie diese Zahl mit der ungefähren Anzahl von Zuordnungen, die Sie für Ihren Server haben.

Wenn die Zahl, die Sie in Schritt 3 geschätzt haben, weniger als 2,1 MB beträgt, liegen Ihre Zuordnungen innerhalb des akzeptablen Grenzwerts.

Anforderungen an den Zielpfad

- Verwenden Sie `${transfer:UserName}` eine Variable, wenn der Bucket- oder Dateisystempfad auf der Grundlage des Benutzernamens parametrisiert wurde.
- Ziele können so konfiguriert werden, dass sie auf verschiedene Amazon S3 S3-Buckets oder Dateisysteme verweisen, sofern die zugehörige IAM-Rolle über die erforderlichen Berechtigungen für den Zugriff auf diese Speicherorte verfügt.
- Alle Ziele müssen mit einem Schrägstrich (/) beginnen, dürfen aber nicht mit einem enden. Zum Beispiel `/amzn-s3-demo-bucket/images` ist richtig, während `amzn-s3-demo-bucket/images` und `/amzn-s3-demo-bucket/images/` nicht.

Überlegungen zur Speicherung

- Amazon S3 ist ein Objektspeicher, in dem Ordner nur als virtuelles Konzept existieren. Bei Verwendung von Amazon S3 S3-Speicher meldet Transfer Family Präfixe als Verzeichnisse in STAT-Vorgängen, auch wenn kein Null-Byte-Objekt mit einem abschließenden Schrägstrich vorhanden ist. Ein richtiges Null-Byte-Objekt mit einem abschließenden Schrägstrich wird bei STAT-Vorgängen auch als Verzeichnis gemeldet. Dieses Verhalten wird unter [Organisieren von Objekten in der Amazon S3 S3-Konsole mithilfe von Ordnern](#) im Amazon Simple Storage Service-Benutzerhandbuch beschrieben.
- Für Anwendungen, die zwischen Dateien und Ordnern unterscheiden müssen, verwenden Sie Amazon Elastic File System (Amazon EFS) als Ihre Transfer Family Family-Speicheroption.
- Wenn Sie logische Verzeichniswerte für Ihren Benutzer angeben, hängt der verwendete Parameter vom Benutzertyp ab:
 - Geben Sie für vom Dienst verwaltete Benutzer logische Verzeichniswerte in `HomeDirectoryMappings` ein.
 - Geben Sie für Benutzer eines benutzerdefinierten Identitätsanbieters logische Verzeichniswerte in `anHomeDirectoryDetails`.

Werte für Benutzerverzeichnisse

- Der Parameter für die Angabe logischer Verzeichniswerte hängt von Ihrem Benutzertyp ab:
 - Geben Sie für Benutzer, die vom Dienst verwaltet werden, logische Verzeichniswerte in `anHomeDirectoryMappings`.
 - Geben Sie für Benutzer eines benutzerdefinierten Identitätsanbieters logische Verzeichniswerte in `anHomeDirectoryDetails`.
- Wenn Sie LOGICAL verwenden `HomeDirectoryType`, können Sie einen `HomeDirectory` Wert für vom Service verwaltete Benutzer, Active Directory-Zugriff und benutzerdefinierte Identitätsanbieter angeben, sofern diese in der Antwort angegeben `HomeDirectoryDetails` werden. Wenn nicht angegeben, ist der `HomeDirectory` Standardwert. /

Einzelheiten zur Implementierung logischer Verzeichnisse finden Sie unter [Implementierung logischer Verzeichnisse](#).

Implementierung logischer Verzeichnisse

Important

Anforderungen an das Stammverzeichnis

- Wenn Sie die Amazon S3 S3-Einstellungen zur Leistungsoptimierung nicht verwenden, muss Ihr Stammverzeichnis beim Start vorhanden sein.
- Für Amazon S3 bedeutet dies, ein Null-Byte-Objekt zu erstellen, das mit einem Schrägstrich (/) endet. /
- Um diese Anforderung zu umgehen, sollten Sie erwägen, die Amazon S3 S3-Leistungsoptimierung zu aktivieren, wenn Sie Ihren Server erstellen oder aktualisieren.
- Wenn Sie a HomeDirectory mit LOGICAL angeben HomeDirectoryType, muss der Wert einer Ihrer logischen Verzeichniszuordnungen zugeordnet werden. Der Dienst überprüft dies sowohl bei der Benutzererstellung als auch bei Aktualisierungen, um Konfigurationen zu verhindern, die nicht funktionieren würden.

Konfiguration des logischen Home-Verzeichnisses

Wenn Sie LOGICAL als Ihr System verwenden HomeDirectoryType, beachten Sie Folgendes:

- Der HomeDirectory Wert muss einer Ihrer vorhandenen logischen Verzeichniszuordnungen entsprechen.
- Das System überprüft dies automatisch bei der Benutzererstellung und bei Aktualisierungen.
- Diese Überprüfung verhindert Konfigurationen, die zu Zugriffsproblemen führen würden.

Aktivieren Sie logische Verzeichnisse

Um logische Verzeichnisse für einen Benutzer zu verwenden, setzen Sie den HomeDirectoryType Parameter auf LOGICAL. Tun Sie dies, wenn Sie einen neuen Benutzer erstellen oder einen vorhandenen Benutzer aktualisieren.

```
"HomeDirectoryType": "LOGICAL"
```

chrootFür Benutzer aktivieren

Erstellen Sie für eine Verzeichnisstruktur `chroot`, die aus einer einzelnen Verzeichnisstruktur `Entry` und einer `Target` Paarung für jeden Benutzer besteht. Der Eintrag/steht für den Stammordner, während `Target` den tatsächlichen Speicherort in Ihrem Bucket oder Dateisystem angibt.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

Sie können einen absoluten Pfad wie im vorherigen Beispiel verwenden, oder Sie können eine dynamische Ersetzung für den Benutzernamen durch verwenden `${transfer:UserName}`, wie im folgenden Beispiel.

```
[{"Entry": "/", "Target":  
"/amzn-s3-demo-bucket${transfer:UserName}"]}]
```

Im vorherigen Beispiel ist der Benutzer an sein Stammverzeichnis gebunden und kann sich in der Hierarchie nicht weiter oben bewegen.

Struktur des virtuellen Verzeichnisses

Für eine virtuelle Verzeichnisstruktur können Sie mehrere `Entry Target` Paarungen mit Zielen an einer beliebigen Stelle in Ihren S3-Buckets oder EFS-Dateisystemen erstellen, auch über mehrere Buckets oder Dateisysteme hinweg, sofern die IAM-Rollenzuordnung des Benutzers über Zugriffsberechtigungen verfügt.

Im folgenden Beispiel für eine virtuelle Struktur befindet sich der Benutzer, wenn er sich bei AWS SFTP anmeldet, im Stammverzeichnis mit den Unterverzeichnissen, und. `/pics /doc /reporting /anotherpath/subpath/financials`

Note

Sofern Sie sich nicht dafür entscheiden, die Leistung Ihrer Amazon S3 S3-Verzeichnisse zu optimieren (wenn Sie einen Server erstellen oder aktualisieren), muss entweder der Benutzer

oder ein Administrator die Verzeichnisse erstellen, sofern sie noch nicht existieren. Die Vermeidung dieses Problems ist ein Grund, eine Optimierung der Amazon S3 S3-Leistung in Betracht zu ziehen.

Für Amazon EFS benötigen Sie weiterhin den Administrator, um die logischen Zuordnungen oder das / Verzeichnis zu erstellen.

```
[
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/financials"}]
```

Note

Sie können Dateien nur in die spezifischen Ordner hochladen, die Sie zuordnen. Das bedeutet, dass Sie im vorherigen Beispiel nicht in /anotherpath oder anotherpath/subpath Verzeichnisse hochladen können, sondern nur anotherpath/subpath/financials. Sie können diesen Pfaden auch nicht direkt zuordnen, da überlappende Pfade nicht zulässig sind.

Gehen Sie beispielsweise davon aus, dass Sie die folgenden Zuordnungen erstellen:

```
{
  "Entry": "/pics",
  "Target": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

Sie können nur Dateien in diese Buckets hochladen. Wenn Sie zum ersten Mal eine Verbindung herstellensftp, werden Sie im Stammverzeichnis abgelegt. / Wenn Sie

versuchen, eine Datei in dieses Verzeichnis hochzuladen, schlägt der Upload fehl. Die folgenden Befehle zeigen eine Beispielsequenz:

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

Um in eine beliebige Datei hochzuladen `directory/sub-directory`, müssen Sie den Pfad explizit dem zuordnen `sub-directory`.

Weitere Informationen zur Konfiguration logischer Verzeichnisse und `chroot` für Ihre Benutzer, einschließlich einer AWS CloudFormation Vorlage, die Sie herunterladen und verwenden können, finden Sie unter [Vereinfachen Sie Ihre AWS SFTP-Struktur mit Chroot und logischen Verzeichnissen](#) im AWS Storage-Blog.

Beispiele für die Konfiguration logischer Verzeichnisse

In diesem Beispiel erstellen wir einen Benutzer und weisen ihm zwei logische Verzeichnisse zu. Der folgende Befehl erstellt einen neuen Benutzer (für einen vorhandenen Transfer Family Family-Server) mit logischen Verzeichnissen `pics` und `doc`.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{"Entry\":"\"/pics\"", "\"Target\":"\"/amzn-s3-demo-bucket1/pics\""}, {"Entry\":"\"/doc\"", "\"Target\":"\"/amzn-s3-demo-bucket2/test/mydocs\""}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Wenn **marymajor** es sich um einen bestehenden Benutzer handelt und sein Home-Verzeichnistyp `PATH`, können Sie ihn `LOGICAL` mit einem ähnlichen Befehl wie dem vorherigen ändern.

```
aws transfer update-user \
  --user-name marymajor \
```

```
--server-id s-11112222333344445 \
--role arn:aws:iam::1234abcd5678:role/marymajor-role \
--home-directory-type LOGICAL \
--home-directory-mappings "[{"Entry":"/pics", "Target":"/amzn-s3-demo-
bucket1/pics"}, {"Entry":"/doc", "Target":"/amzn-s3-demo-bucket2/test/mydocs
"}]"
```

Beachten Sie Folgendes:

- Wenn die Verzeichnisse `/amzn-s3-demo-bucket1/pics` und noch `/amzn-s3-demo-bucket2/test/mydocs` nicht existieren, muss der Benutzer (oder ein Administrator) sie erstellen.

Note

Diese Verzeichnisse werden automatisch vom Transfer Family Family-Server erstellt, wenn Sie optimierte Verzeichnisse konfiguriert haben.

- Wenn Mary **marymajor** eine Verbindung zum Server herstellt und den `ls -l` Befehl ausführt, sieht Mary Folgendes:

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor** kann auf dieser Ebene keine Dateien oder Verzeichnisse erstellen. Innerhalb von `pics` und kann sie `doc` jedoch Unterverzeichnisse hinzufügen.
- Dateien, die Mary zu `pics` Amazon S3 S3-Pfaden hinzufügt `/amzn-s3-demo-bucket1/pics /amzn-s3-demo-bucket2/test/mydocs` bzw. zu diesen hinzugefügt `doc` werden.
- In diesem Beispiel geben wir zwei verschiedene Buckets an, um diese Möglichkeit zu veranschaulichen. Sie können jedoch denselben Bucket für mehrere oder alle logischen Verzeichnisse verwenden, die Sie für den Benutzer angeben.

Dieses Beispiel bietet eine alternative Konfiguration für einen logischen Home-Pfad.

```
aws transfer create-user \
--user-name marymajor \
--server-id s-11112222333344445 \
--role arn:aws:iam::1234abcd5678:role/marymajor-role \
--home-directory-type LOGICAL \
--home-directory /home/marymajor \
```



```
--home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
--ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Beachten Sie Folgendes:

- Die Zuordnungen sehen einen gemeinsamen Pfad vor/home/marymajor, der der erste Teil der beiden logischen Pfade ist. Dateien können dann zu den Ordnern pics und doc hinzugefügt werden.
- Wie im vorherigen Beispiel ist das Home-Verzeichnis,/home/marymajor, schreibgeschützt.

Logische Verzeichnisse für Amazon EFS konfigurieren

Wenn Ihr Transfer Family Family-Server Amazon EFS verwendet, muss das Home-Verzeichnis für den Benutzer mit Lese- und Schreibzugriff erstellt werden, bevor der Benutzer in seinem logischen Home-Verzeichnis arbeiten kann. Der Benutzer kann dieses Verzeichnis nicht selbst erstellen, da ihm die entsprechenden Berechtigungen für `mkdir` sein logisches Home-Verzeichnis fehlen würden.

Wenn das Basisverzeichnis des Benutzers nicht existiert und er einen `ls` Befehl ausführt, reagiert das System wie folgt:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Ein Benutzer mit Administratorzugriff auf das übergeordnete Verzeichnis muss das logische Home-Verzeichnis des Benutzers erstellen.

Benutzerdefinierte AWS Lambda Antwort

Sie können logische Verzeichnisse mit einer Lambda-Funktion verwenden, die eine Verbindung zu Ihrem benutzerdefinierten Identitätsanbieter herstellt. Dazu geben Sie in Ihrer Lambda-Funktion die Target Werte `HomeDirectoryType` als **LOGICAL** und `add Entry` und für den `HomeDirectoryDetails` Parameter an. Beispiel:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/amzn-s3-demo-bucket/theRealFolder\"}]"
```

Der folgende Code ist ein Beispiel für eine erfolgreiche Antwort auf einen benutzerdefinierten Lambda-Authentifizierungsaufwurf.

```
aws transfer test-identity-provider \  
  --server-id s-1234567890abcdef0 \  
  --user-name myuser  
{  
  "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/  
s-1234567890abcdef0/users/myuser/config",  
  "Message": "",  
  "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",  
    \"HomeDirectoryType\": \"LOGICAL\",  
    \"HomeDirectoryDetails\": \"[{\\\"Entry\\\": \\\"/myhome\\\", \\\"  
\\\"Target\\\": \\\"/amzn-s3-demo-bucket/theRealFolder\\\"]}\"",  
    \"PublicKeys\": \"[ssh-rsa myrsapubkey]\"}",  
  "StatusCode": 200  
}
```

Note

Die "Url"-Zeile wird nur zurückgegeben, wenn Sie eine API Gateway Gateway-Methode als Ihren benutzerdefinierten Identitätsanbieter verwenden.

Greifen Sie mit Transfer Family auf Ihre FSx for NetApp ONTAP-Dateisysteme zu

Inhalt

- [-Übersicht](#)
- [Voraussetzungen](#)
 - [FSx für NetApp ONTAP — Anforderungen](#)
 - [Erforderliche IAM-Berechtigungen](#)
- [So funktioniert FSx-Speicher mit Transfer Family](#)
 - [Benutzeridentität im Dateisystem](#)
- [Einen S3-Zugangspunkt für FSx erstellen](#)
 - [Benennung von Zugriffspunkten](#)

- [Einen Access Point für FSx for NetApp ONTAP erstellen](#)
- [Konfiguration von Dateisystemberechtigungen](#)
- [Verwendung von S3-Zugangspunkt-Aliassen mit FSx](#)
 - [Über Aliase für Access Points](#)
 - [Finden Sie den Alias Ihres Access Points](#)
- [Konfiguration der Transfer Family für FSx-Speicher](#)
 - [Erstellen einer IAM-Rolle](#)
- [Benutzer für FSx-Speicher verwalten](#)
 - [Erstellen eines Benutzers](#)
 - [Konfiguration mehrerer Verzeichniszuordnungen](#)
- [Konfiguration von Dateiübertragungsclients](#)
 - [WinSCP-Konfiguration](#)
 - [Andere SFTP-Clients](#)
- [Problembehandlung bei FSx-Speicher](#)
 - [Probleme beim Betrieb von Dateien](#)

-Übersicht

Transfer Family unterstützt Amazon FSx for NetApp ONTAP über S3-Zugriffspunkte. Amazon FSx for NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässige, skalierbare, leistungsstarke und funktionsreiche Dateispeicherung bietet, die auf dem beliebten ONTAP-Dateisystem NetApp basiert. Wenn Sie Transfer Family mit einem FSx-Dateisystem konfigurieren, stellen Ihre Benutzer mithilfe von Standard-Dateiübertragungsclients eine Verbindung zu Transfer Family-Endpunkten her. Transfer Family leitet Dateioperationen über einen S3-Zugriffspunkt weiter, der an Ihr FSx-Volume angeschlossen ist, während Ihre Daten im FSx-Dateisystem verbleiben. Weitere Informationen zu FSx for NetApp ONTAP finden Sie unter [Was ist Amazon FSx](#) for ONTAP? NetApp

Diese Integration ermöglicht Ihnen:

- Dateien mithilfe der Protokolle SFTP, FTPS oder FTP in einen Dateispeicher der Enterprise-Klasse übertragen
- Greifen Sie über mehrere Protokolle (SFTP, NFS, SMB) auf dieselben Daten zu
- Verwenden Sie FSx-Funktionen wie Snapshots, Backups und Data Tiering

Important

Einige Dateioperationen werden nicht unterstützt, wenn FSx-Dateisysteme mit Transfer Family verwendet werden, einschließlich Umbenennungs- und Anfügeoperationen. Bei Upload-Vorgängen sind die Dateigrößen auf 5 GB begrenzt. Eine vollständige Liste der Einschränkungen finden Sie unter [Access Point-Kompatibilität](#).

Voraussetzungen

Bevor Sie Transfer Family mit Amazon FSx konfigurieren, müssen Sie die folgenden Anforderungen erfüllen.

FSx für NetApp ONTAP — Anforderungen

Um FSx for NetApp ONTAP mit Transfer Family zu verwenden, benötigen Sie:

- Ein FSx for NetApp ONTAP-Dateisystem, auf dem ONTAP Version 9.17.1 oder höher ausgeführt wird
- Das Dateisystem und der S3-Zugangspunkt befinden sich in derselben Region AWS
- Dasselbe AWS Konto, dem sowohl das Dateisystem als auch der Access Point gehören

Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx for NetApp ONTAP](#).

Erforderliche IAM-Berechtigungen

Sie können jeden S3-Zugriffspunkt mit unterschiedlichen Berechtigungen und Netzwerkkontrollen konfigurieren, die S3 für jede Anfrage anwendet, die über diesen Access Point gestellt wird. S3-Zugriffspunkte unterstützen IAM-Ressourcenrichtlinien, mit denen Sie die Nutzung des Access Points nach Ressourcen, Benutzern oder anderen Bedingungen steuern können. Damit eine Anwendung oder ein Benutzer über einen Access Point auf Dateien zugreifen kann, müssen sowohl der Access Point als auch das zugrunde liegende Volume die Anfrage zulassen. Weitere Informationen finden Sie unter [Richtlinien für IAM-Zugriffspunkte](#).

Amazon S3 Access Points für FSx verwenden ein duales Autorisierungsmodell, das IAM-Berechtigungen mit Berechtigungen auf Dateisystemebene kombiniert. Dieser Ansatz stellt sicher, dass Datenzugriffsanfragen sowohl auf der AWS Service-Ebene als auch auf der Ebene des zugrunde liegenden Dateisystems ordnungsgemäß autorisiert werden.

Damit eine Anwendung oder ein Benutzer erfolgreich über einen Access Point auf Daten zugreifen kann, müssen sowohl die S3-Zugriffspunktrichtlinie als auch das zugrunde liegende FSx-Volume die Anfrage zulassen.

Um diese Integration zu erstellen und zu konfigurieren, benötigen Sie die folgenden Berechtigungen:

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(wenn Sie eine optionale Zugriffspunktrichtlinie erstellen)

So funktioniert FSx-Speicher mit Transfer Family

Wenn Sie Transfer Family mit einem FSx-Dateisystem konfigurieren, arbeiten die folgenden Komponenten zusammen, um Dateiübertragungen zu ermöglichen:

1. Ein Benutzer stellt über einen SFTP-, FTPS- oder FTP-Client eine Verbindung zum Transfer Family Family-Server her.
2. Transfer Family authentifiziert den Benutzer mithilfe von vom Dienst verwalteten Identitäten, einem benutzerdefinierten Identitätsanbieter oder AWS Directory Service for Microsoft Active Directory. Nach der Authentifizierung übernimmt Transfer Family die dem Benutzer zugeordnete IAM-Rolle.
3. Bei jedem Dateivorgang fungiert Transfer Family als standardmäßiger S3-API-Client, der Anfragen an den S3 Access Point unter Verwendung der angenommenen IAM-Rolle des Benutzers sendet und die Berechtigungen anhand der S3-Zugriffspunktrichtlinie überprüft.
4. Das FSx-Dateisystem überprüft, ob der mit dem Access Point verknüpfte Dateisystembenutzer berechtigt ist, den angeforderten Vorgang auszuführen. Die Dateioperation wird dann auf dem FSx-Volume ausgeführt.

Damit ein Dateivorgang erfolgreich ist, müssen beide Autorisierungsebenen die Anfrage zulassen.

Note

Das Anhängen eines S3-Zugriffspunkts an ein FSx-Volume ändert nichts daran, wie sich das Volume verhält, wenn direkt über NFS oder SMB darauf zugegriffen wird. Der bestehende Dateiprotokollzugriff funktioniert unverändert weiter.

Benutzeridentität im Dateisystem

Jeder Access Point verwendet eine Dateisystem-Benutzeridentität, die Sie bei der Erstellung des Access Points angeben. Diese Identität autorisiert alle Dateizugriffsanforderungen, die über diesen Access Point gestellt werden. Der Dateisystembenutzer ist ein Benutzerkonto auf dem zugrunde liegenden Amazon FSx-Dateisystem. Wenn der Dateisystembenutzer nur Lesezugriff hat, sind nur Leseanfragen autorisiert, die über den Access Point gestellt werden, und Schreibsanforderungen werden blockiert. Wenn der Dateisystembenutzer über Lese- und Schreibzugriff verfügt, sind sowohl Lese- als auch Schreibsanforderungen an das angehängte Volume autorisiert, die über den Zugriffspunkt gestellt werden.

Einen S3-Zugangspunkt für FSx erstellen

Bevor Sie Transfer Family konfigurieren, müssen Sie einen S3-Zugriffspunkt erstellen, der an Ihr FSx-Volume angeschlossen ist. S3-Zugriffspunkte sind so genannte Netzwerkendpunkte, die mit einer Datenquelle wie einem Bucket oder einem Amazon FSx for ONTAP-Volume verbunden sind. Sie können mithilfe der Amazon FSx-Konsole, AWS CLI oder API einen Access Point für NetApp ONTAP erstellen und an einen FSx anhängen. Nach dem Anhängen können Sie die S3-Objekt-APIs verwenden, um auf Ihre Dateidaten zuzugreifen. Ihre Daten befinden sich weiterhin im Amazon FSx-Dateisystem und sind weiterhin für Ihre vorhandenen Workloads direkt zugänglich. Sie verwalten Ihren Speicher weiterhin mit allen Speicherverwaltungsfunktionen von FSx for NetApp ONTAP, einschließlich Backups, Snapshots, Benutzer- und Gruppenkontingenten sowie Komprimierung.

Weitere Informationen finden Sie unter [Erstellen von Zugriffspunkten](#).

Benennung von Zugriffspunkten

Beachten Sie bei der Benennung Ihres Access Points die folgenden Richtlinien:

- Die Namen der Access Points müssen innerhalb Ihres AWS Kontos und Ihrer Region eindeutig sein.
- Namen dürfen nicht mit `-ext-s3alias` (reserviert für Aliase) enden.
- Vermeiden Sie es, vertrauliche Informationen in Namen aufzunehmen, da diese im DNS veröffentlicht werden.

Eine vollständige Liste der Benennungsregeln finden Sie unter [Benennungsregeln, Einschränkungen und Einschränkungen für Access Points](#).

Einen Access Point für FSx for NetApp ONTAP erstellen

Gehen Sie wie folgt vor, um einen S3-Zugriffspunkt für ein FSx for NetApp ONTAP-Volume zu erstellen.

Um einen Access Point (Konsole) zu erstellen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie Ihr FSx for NetApp ONTAP-Dateisystem.
4. Wählen Sie die Registerkarte Volumes.
5. Wählen Sie das Volume aus, das Sie anhängen möchten.
6. Wählen Sie unter Aktionen die Option S3-Zugangspunkt erstellen aus.
7. Geben Sie unter Name des Zugriffspunkts einen aussagekräftigen Namen ein (z. B. `transfer-family-ap`).
8. Wählen Sie für den Identitätstyp des Dateisystembenutzers eine der folgenden Optionen aus:
 - UNIX-Identität — Für Volumes mit UNIX-Sicherheitsstil
 - Windows-Identität — Für Volumes mit NTFS-Sicherheitsstil
9. (Optional) Geben Sie für die Zugriffspunktrichtlinie eine IAM-Richtlinie ein, die definiert, welche IAM-Prinzipale welche Operationen an Objekten ausführen können, auf die über diesen Access Point zugegriffen wird. Weitere Informationen finden Sie unter [Zugriffspunktzugriff verwalten](#).
10. Wählen Sie Erstellen aus.
11. Notieren Sie sich nach der Erstellung den Access Point-Alias für die Verwendung in der Transfer Family Family-Konfiguration.

Note

Wenn im Namen Ihrer verbundenen SFTP/FTPS Benutzer auf S3-Ressourcen AWS Transfer Family zugegriffen wird, stammen Anfragen von der AWS Transfer Family Infrastruktur, nicht von Ihrer VPC. Aus diesem Grund lehnen S3 Access Points, die mit einem VPC-Netzwerkursprung konfiguriert sind, diese Anfragen ab. Selbst wenn Sie einen Access Point verwenden, der mit einem Internet-Netzwerkursprung konfiguriert ist, bleibt der gesamte Datenverkehr zwischen Transfer Family und dem Access Point privat und wird über das AWS Backbone-Netzwerk übertragen — er durchquert nicht das öffentliche Internet.

Konfiguration von Dateisystemberechtigungen

Der von Ihnen angegebene Dateisystembenutzer bestimmt, welche Operationen Transfer Family Family-Benutzer ausführen können. Sie müssen die entsprechenden Berechtigungen für Ihr FSx-Volume konfigurieren.

UNIX-Beispiel:

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users

# Set permissions
chmod 755 /vol1/transfer-users
```

Windows-Beispiel:

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Verwendung von S3-Zugangspunkt-Aliasen mit FSx

Wenn Sie FSx-Dateisysteme mit Transfer Family verwenden, müssen Sie S3-Zugriffspunkt-Aliase verwenden. Transfer Family unterstützt nicht die Verwendung von Access Point-ARNs oder anderen Referenzmethoden für FSx-Speicher.

Important

AWS Transfer Family unterstützt nur S3-Zugriffspunkt-Aliase, wenn FSx-Dateisysteme verwendet werden. Sie können keine Access Point-ARNs oder URIs im virtuellen Hosted-Stil verwenden.

 Important

Der Access Point muss sich in derselben Region wie das Volume befinden.

Über Aliase für Access Points

Wenn Sie einen S3-Zugriffspunkt erstellen, der an ein FSx-Volume angehängt ist, generiert Amazon S3 automatisch einen Access Point-Alias. Dieser Alias ist eine eindeutige Kennung, die Sie überall verwenden können, wo Sie einen S3-Bucket-Namen verwenden.

Für Access Points, die an FSx-Volumes angeschlossen sind, verwendet der Alias das folgende Format:

```
access-point-name-metadata-ext-s3alias
```

Beispiel für einen Alias:

```
my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias
```

 Note

Das `-ext-s3alias` Suffix ist für FSx Access Point-Aliase reserviert. Sie können dieses Suffix nicht in Zugriffspunktnamen verwenden.

Finden Sie den Alias Ihres Access Points

Sie können den Alias des Access Points finden, nachdem Sie den Access Point erstellt haben.

Um den Alias des Access Points zu finden (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie Ihr Dateisystem aus.
4. Wählen Sie die Registerkarte Volumes und wählen Sie das Volume aus, für das Sie den Access Point erstellt haben.

5. Gehen Sie zur Spalte mit den S3-Zugangspunkt-Details.
6. Der Alias wird in der Alias-Spalte angezeigt.

So finden Sie den Access Point-Alias (CLI)

Verwenden Sie den Befehl `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Die Antwort enthält den Alias:

```
{
  "S3AccessPointAttachments": [
    {
      "S3AccessPoint": {
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-
ap",
        "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias"
      }
    }
  ]
}
```

Wenn Sie Transfer Family Family-Benutzer konfigurieren, verwenden Sie den Access Point-Alias in Basisverzeichniszuordnungen.

Format des Home-Verzeichnisses:

```
/access-point-alias/path/to/directory
```

Beispiel:

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith
```

Konfiguration der Transfer Family für FSx-Speicher

Nachdem Sie den S3-Zugriffspunkt erstellt haben, konfigurieren Sie einen Transfer Family Family-Server für die Verwendung.

Erstellen einer IAM-Rolle

Sie müssen eine IAM-Rolle erstellen, die Transfer Family Zugriff auf den S3-Zugriffspunkt gewährt.

Important

IAM-Richtlinien erfordern das Access Point-ARN-Format, nicht den Alias. Verwenden Sie das Format `arn:aws:s3:region:account-id:accesspoint/access-point-name` in den Ressourcenanweisungen Ihrer IAM-Richtlinie. Der Access Point-Alias (endet auf `-ext-s3alias`) wird nur für Zuordnungen von Home-Verzeichnissen verwendet.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
4. Wählen Sie als Anwendungsfall die Option Transfer aus.
5. Wählen Sie Weiter aus.
6. Wählen Sie Richtlinie erstellen und geben Sie Ihre Richtlinie ein (siehe Beispielrichtlinie unten).
7. Hängen Sie die Richtlinie an die Rolle an und wählen Sie Rolle erstellen aus.

Beispiel für eine IAM-Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/object/*"
    }
  ]
}
```

```
    },  
    {  
      "Sid": "AllowDirectoryOperations",  
      "Effect": "Allow",  
      "Action": [  
        "s3:ListBucket",  
        "s3:GetBucketLocation"  
      ],  
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"  
    }  
  ]  
}
```

Benutzer für FSx-Speicher verwalten

Erstellen Sie Transfer Family Family-Benutzer mit Stammverzeichniszuordnungen, die den S3-Zugriffspunkt-Alias verwenden.

Erstellen eines Benutzers

Wenn Sie einen Benutzer für FSx-Speicher erstellen, verwenden Sie den Access Point-Alias in Home-Verzeichniszuordnungen.

So erstellen Sie einen Service Managed-Benutzer (Konsole)

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Wählen Sie Ihren Server aus.
4. Wählen Sie im Bereich Benutzer die Option Benutzer hinzufügen aus.
5. Geben Sie unter Benutzername einen Benutzernamen ein.
6. Wählen Sie unter Rolle die IAM-Rolle aus, die Sie erstellt haben.
7. Wählen Sie für Home-Verzeichnis die Option Eingeschränkt aus.
8. Fügen Sie für Zuordnungen von Home-Verzeichnissen eine Zuordnung mit dem Access Point-Alias hinzu:

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprinstn7aefdfbarligizwgfyfouse1a-ext-s3alias/users/jsmith"}]
```

Um einen Benutzer zu erstellen (CLI)

Verwenden Sie den Befehl `create-user`. Ersetzen Sie den Access Point-Alias durch Ihren Alias.

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/  
jsmith"  
    }  
  ]'
```

Konfiguration mehrerer Verzeichniszuordnungen

Sie können mehrere virtuelle Verzeichnisse verschiedenen Pfaden auf dem FSx-Volume zuordnen.

Beispiel: Separate Upload- und Download-Verzeichnisse

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/inbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/  
jsmith/inbox"  
    },  
    {  
      "Entry": "/outbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/  
jsmith/outbox"  
    }  
  ]'
```

Konfiguration von Dateiübertragungsclients

Wenn Sie FSx-Dateisysteme mit Transfer Family verwenden, müssen Sie Ihre Dateiübertragungsclients so konfigurieren, dass Funktionen deaktiviert werden, die nicht unterstützt werden.

WinSCP-Konfiguration

WinSCP verwendet standardmäßig eine temporäre Umbenennungsfunktion, die von S3-Zugriffspunkten für FSx nicht unterstützt wird.

Warning

Wenn Sie die Funktion zum temporären Umbenennen in WinSCP nicht deaktivieren, schlagen Dateiuploads fehl.

Um die temporäre Umbenennung in WinSCP zu deaktivieren

1. Öffnen Sie WinSCP.
2. Wählen Sie im Anmeldedialogfeld Bearbeiten, um Ihre Sitzungseinstellungen zu ändern.
3. Wählen Sie Erweitert aus.
4. Wählen Sie in der linken Navigationsleiste unter Transfer die Option Endurance aus.
5. Wählen Sie für „Übertragung resume/transfer auf temporären Dateinamen aktivieren“ die Option „Deaktivieren“.
6. Wählen Sie OK, um die Einstellungen zu speichern.

Alternativ können Sie diese Einstellung für eine bestehende Sitzung deaktivieren:

1. Connect zu Ihrem Transfer Family Family-Server her.
2. Wählen Sie Optionen und dann Einstellungen.
3. Wähle Transfer und dann Endurance.
4. Wählen Sie für „Übertragung resume/transfer auf temporären Dateinamen aktivieren“ die Option „Deaktivieren“.
5. Wählen Sie OK aus.

Andere SFTP-Clients

Deaktivieren Sie für andere SFTP-Clients die folgenden Funktionen, sofern verfügbar:

- Temporäre Datei-Uploads (in eine temporäre Datei hochladen und dann umbenennen)
- Übertragungen mithilfe temporärer Dateien fortsetzen
- Atomare Uploads mithilfe von Umbenennungsoperationen
- Anfügen-Modus für Uploads

Spezifische Konfigurationsschritte finden Sie in Ihrer Client-Dokumentation.

Problembehandlung bei FSx-Speicher

In diesem Abschnitt wird beschrieben, wie Sie häufig auftretende Probleme bei der Verwendung von Transfer Family mit FSx-Dateisystemen identifizieren und lösen können.

Probleme beim Betrieb von Dateien

Genehmigung verweigert

Wenn Sie die Fehlermeldung „Zugriff verweigert“ erhalten:

1. Stellen Sie sicher, dass die IAM-Rolle über die richtigen Berechtigungen für den Access Point-Alias verfügt. Sie können dies tun, indem Sie direkt mit S3-APIs testen.
2. Vergewissern Sie sich, dass die Zugriffspunktrichtlinie die IAM-Rolle zulässt.
3. Stellen Sie sicher, dass der Dateisystembenutzer über Berechtigungen für den Zielpfad verfügt.
4. Vergewissern Sie sich, dass bei der Zuordnung des Home-Verzeichnisses der richtige Access Point-Alias verwendet wird.

Upload schlägt mit WinSCP fehl

Wenn Datei-Uploads mit WinSCP fehlschlagen, deaktivieren Sie das temporäre Umbenennen:

1. Wählen Sie in WinSCP Optionen und dann Einstellungen.
2. Wählen Sie Transfer und dann Endurance.
3. Wählen Sie für „Übertragung resume/transfer auf temporären Dateinamen aktivieren“ die Option „Deaktivieren“.

Weitere Informationen finden Sie unter [the section called “Konfiguration von Dateiübertragungsclients”](#).

Das Hochladen der Datei schlägt fehl

Wenn Datei-Uploads fehlschlagen:

1. Stellen Sie sicher, dass die Dateigröße unter 5 GB liegt.
2. Stellen Sie sicher, dass auf dem FSx-Volume ausreichend Speicherplatz verfügbar ist.
3. Überwachen Sie die CloudWatch Metriken auf Drosselung.

Familien-Web-Apps übertragen

Sie können Web-Apps erstellen, um eine einfache Schnittstelle für die Übertragung von Daten zu und von Amazon Simple Storage Service (S3) über einen Webbrowser zu ermöglichen. Dazu müssen Sie keine AWS Transfer Family Server erstellen oder bereitstellen.

Vor der Einführung der Transfer Family Family-Web-Apps mussten Endbenutzer eine Kundenlösung, eine maßgeschneiderte Lösung oder eine Drittanbieterlösung verwenden, um auf ihre Daten in Amazon S3 zuzugreifen. Dies lag an den strengen Sicherheitsanforderungen für Kunden und Partner und daran, dass die Bedienung von Kunden-Apps für technisch nicht versierte Benutzer eine Herausforderung darstellt.

Mit der Einführung von Web-Apps können Sie jetzt ein markenspezifisches, sicheres und hochverfügbares Portal erweitern, über das Ihre Endbenutzer Daten in Amazon S3 durchsuchen, hochladen und herunterladen können. Web-Apps sind nativ in Amazon S3 Access Grants integriert. AWS IAM Identity Center Das bedeutet, dass nur Ihre authentifizierten Benutzer die Daten einsehen können, auf die sie zugreifen dürfen. Web-Apps werden mit dem [Storage Browser für Amazon S3](#) erstellt und bieten dieselben Endbenutzerfunktionen in einem vollständig verwalteten Angebot, ohne dass Sie Code schreiben oder Ihre eigene Anwendung hosten müssen.

Weitere Informationen zu den anderen AWS-Services , die Sie mit Transfer Family Family-Web-Apps verwenden, finden Sie in der folgenden Dokumentation:

- [Verwaltung des Zugriffs mit S3 Access Grants im Amazon Simple Storage Service-Benutzerhandbuch](#)
- [AWS IAM Identity Center Benutzerhandbuch](#)
- [Workshop „Amazon S3 Access Grants“](#)
- [Ankündigung von AWS Transfer Family Web-Apps für vollständig verwaltete Amazon S3 S3-Dateiübertragungen](#)

Die folgenden Ressourcen helfen Ihnen bei den ersten Schritten mit den Transfer Family Family-Web-Apps.

- Das Benutzerhandbuch bietet hier eine detaillierte, schrittweise Anleitung zur Einrichtung einer Transfer Family Family-Web-App: [Tutorial: Eine einfache Transfer Family Family-Web-App einrichten](#).

- Das AWS Getting Started Resource Center bietet hier ein Tutorial: [Erste Schritte mit der AWS Transfer Family Web-App](#).
- Sehen Sie [sich Erste Schritte mit der AWS Transfer Family Web-App](#) an.

AWS-Regionen für Transfer Family Family-Web-Apps

AWS Transfer Family Web-Apps sind in allen von Transfer Family unterstützten Regionen verfügbar, wie in der [AWS Regionentabelle](#) aufgeführt, mit Ausnahme von Asien-Pazifik (Neuseeland) und AWS European Sovereign Cloud.

VPC-Endpunkte für Web-Apps werden überall unterstützt, AWS-Regionen wo Web-Apps verfügbar sind.

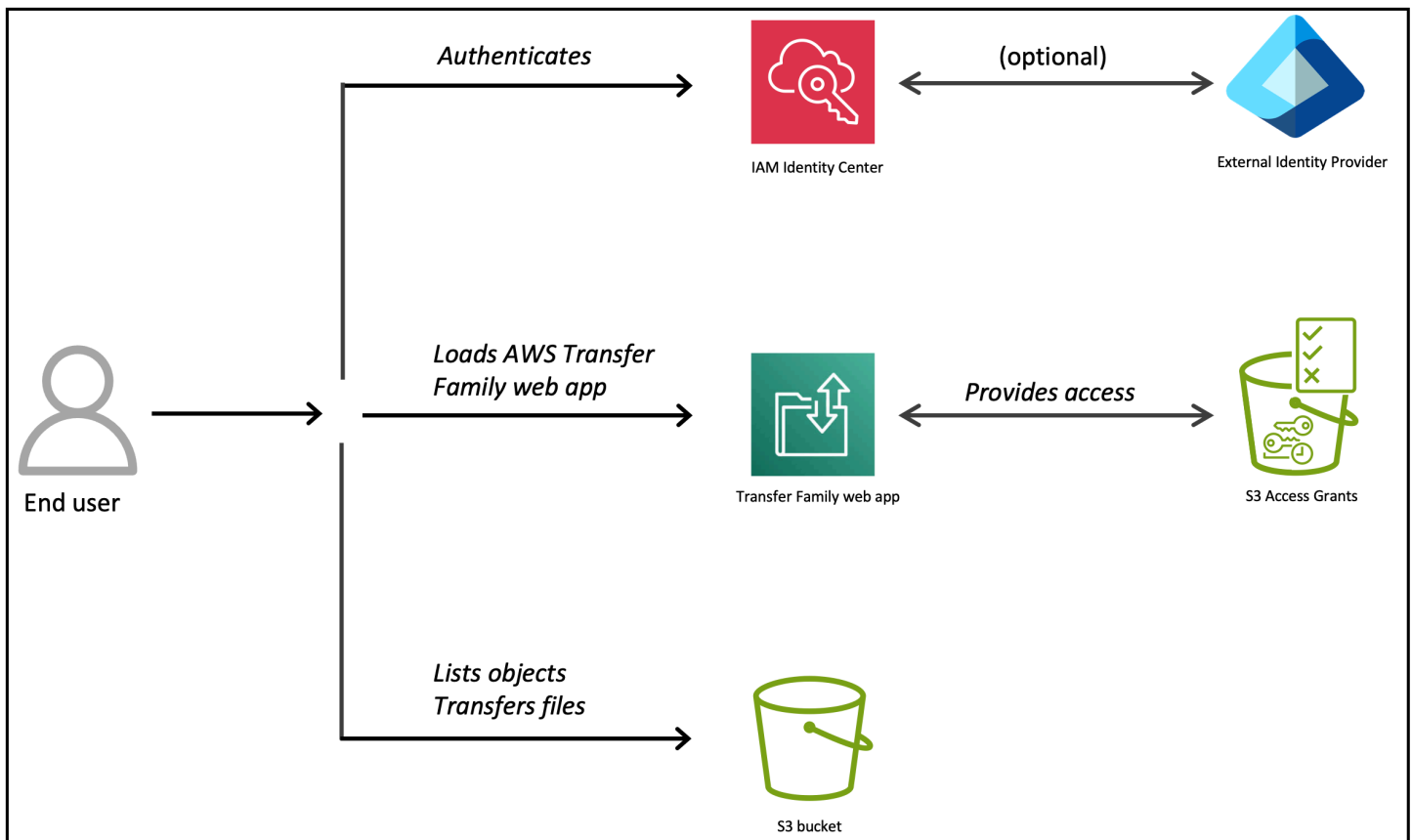
Browserkompatibilität für AWS Transfer Family Web-Apps

Transfer Family Family-Web-Apps unterstützen die folgenden Browser.

Browser	Version	Kompatibilität
Microsoft Edge	Die 3 neuesten Versionen	Kompatibel
Mozilla Firefox	Die 3 neuesten Versionen	Kompatibel
Google Chrome	Die 3 neuesten Versionen	Kompatibel
Apple Safari	Die 3 neuesten Versionen	Kompatibel

So erstellen Sie eine Transfer Family Family-Web-App

Das folgende Diagramm veranschaulicht die Architektur der Transfer Family Family-Web-App.



Anhand des Diagramms können Sie sehen, dass die Transfer Family Family-Web-Apps mit folgenden Funktionen interagieren AWS-Services:

- Amazon S3 für Speicher und Amazon S3 Access Grants zum Abrufen von Sitzungsanmeldedaten.
- AWS IAM Identity Center als verbundener Identitätsanbieter.
- Amazon CloudFront , wenn Sie eine benutzerdefinierte URL für Ihre Web-App konfigurieren.

Beachten Sie die folgenden Einschränkungen bei der Verwendung von Web-Apps.

- Maximale Anzahl von Suchergebnissen pro Abfrage: 10.000
- Die Amazon S3 S3-Buckets, die von der Transfer Family Family-Web-App verwendet werden, müssen sich auf demselben Konto wie die Web-App selbst befinden. Cross-account Buckets werden derzeit nicht unterstützt.
- Maximale Suchbreite pro Abfrage: 10.000 durchsuchte Dateien
- Maximale Upload-Größe pro Datei: 160 GB (149 GiB)
- Maximale Größe der Datei zum Kopieren: 5,36 GB (5 GiB)

- Ordernamen, die mit Punkten (.) beginnen oder enden, werden nicht unterstützt

Voraussetzungen

Konfigurieren AWS Identity and Access Management Sie unter die erforderlichen Rollen. Fügen Sie die Codeblöcke ein, die wir in der Anleitung bereitstellen. Informationen zur Konfiguration der erforderlichen Rollen finden Sie unter [Konfiguration von IAM-Rollen für Transfer Family Family-Web-Apps](#).

- Erstellen Sie eine Rolle als Identitätsträger.
- Erstellen Sie eine IAM-Rolle, die von S3 Access Grants verwendet werden soll. S3 Access Grants übernimmt diese IAM-Rolle, um temporäre Anmeldeinformationen für den registrierten Amazon S3 S3-Standort an den Empfänger zu verkaufen.

Prozess zum Erstellen einer Transfer Family Family-Web-App

Um Ihre Web-App zu erstellen und Ihre Endbenutzer zum Laufen zu bringen, führen Sie die folgenden Aufgaben aus:

1. Konfigurieren Sie IAM Identity Center so, dass es als Ihr föderierter Identitätsanbieter fungiert. Führen Sie die folgenden Aufgaben in IAM Identity Center aus. Weitere Informationen zur Konfiguration von IAM Identity Center finden Sie unter [Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps](#)
 - a. Erstellen Sie eine IAM Identity Center-Instanz, falls Sie noch keine haben.
 - b. Ermitteln Sie Ihre Identitätsquelle. Dabei kann es sich um das standardmäßige IAM Identity Center-Verzeichnis oder um einen Drittanbieter (z. B. Okta) handeln.
 - c. Erstellen oder identifizieren Sie die Benutzer oder Gruppen, die Ihre Web-App verwenden werden.
 - d. Wenn Sie das IAM Identity Center-Verzeichnis für Ihre Identitätsquelle verwenden, notieren Sie sich die Benutzer- oder Gruppen-IDs, die Sie erstellen. Sie benötigen sie später, wenn Sie mithilfe von S3 Access Grants eine Zugriffsberechtigung erstellen.
2. Konfigurieren Sie in Amazon S3 Amazon S3 Access Grants. Weitere Informationen zu S3 Access Grants finden Sie unter [Amazon S3 S3-Zugriffsberechtigungen für Transfer Family Family-Web-Apps konfigurieren](#).
 - Erstellen Sie eine S3 Access Grants-Instance, falls Sie noch keine darin haben AWS-Region.

- Registrieren Sie Ihren Standort mithilfe der IAM-Rolle.
 - Erstellen Sie die Zugriffsgewährung.
3. Führen Sie in Transfer Family die folgenden Aufgaben aus.
- a. Erstellen Sie die Transfer Family Family-Web-App. Weitere Informationen zum Erstellen der Transfer Family Family-Web-App finden Sie unter [Eine Transfer Family Family-Web-App konfigurieren](#).
-  **Important**

Richten Sie Cross-origin Resource Sharing (CORS) für alle Amazon S3 S3-Buckets ein, die von Ihrer Web-App verwendet werden. Informationen zur Einrichtung von CORS finden Sie unter [Richten Sie Cross-origin Resource Sharing \(CORS\) für Ihren Bucket ein](#)
- b. Weisen Sie der Web-App Benutzer oder Gruppen zu. Weitere Informationen zum Zuweisen von Benutzern und Gruppen finden Sie unter [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#).
 - c. (Optional) Aktualisieren Sie den Zugriffsendpunkt für Ihre Web-App mit einer benutzerdefinierten URL. Informationen zum Erstellen einer benutzerdefinierten URL finden Sie unter [Aktualisieren Sie Ihren Zugriffsendpunkt mit einer benutzerdefinierten URL](#).
 - d. Stellen Sie Ihren Endbenutzern die URL des Zugriffsendpunkts zur Verfügung, damit sie sich anmelden und mit Ihrer Web-App interagieren können.

Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps

Im folgenden Abschnitt wird beschrieben, wie Sie Ihren Identitätsanbieter konfigurieren.

Zu Beginn benötigen Sie eine Identitätsquelle. Sie können ein IAM Identity Center-Verzeichnis oder einen externen Identitätsanbieter verwenden. AWS Directory Service for Microsoft Active Directory Transfer Family verwendet IAM Identity Center als föderierten Identitätsanbieter. Dabei handelt es sich um ein System, das Benutzeranmeldeinformationen speichert und Benutzer in mehreren Organisationen authentifiziert.

Wenn Sie kein IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, lesen Sie die folgenden Themen:

- [Einen externen Identitätsanbieter verwalten](#)
- [Stellen Sie eine Connect zu einem Microsoft AD-Verzeichnis her](#)
- [Organisations- und Kontoinstanzen von IAM Identity Center](#)
- [Tutorials zur Identitätsquelle im IAM Identity Center](#)

 Note

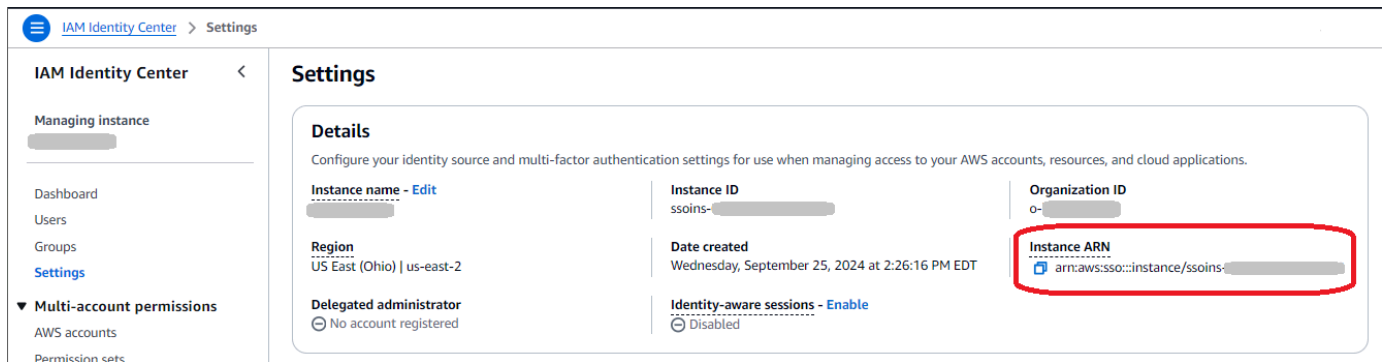
Sie können in IAM Identity Center nur eine Identitätsquelle haben, pro Instanz, pro AWS-Region Einzelheiten finden Sie unter [Voraussetzungen und Überlegungen zu IAM Identity Center](#).

Wenn Sie beabsichtigen, das IAM Identity Center-Verzeichnis als Identitätsquelle zu verwenden und eine schnelle Einrichtung wünschen, können Sie dieses Thema überspringen und mit dem Assistenten [Eine Transfer Family Family-Web-App erstellen](#) zum Erstellen einer IAM Identity Center-Instanz fortfahren.

Zur Konfiguration AWS IAM Identity Center für die Verwendung mit Transfer Family Family-Web-Apps

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Sie können entweder eine Kontoinstanz oder eine Organisationsinstanz von erstellen und verwenden AWS IAM Identity Center.
 - Einzelheiten zu Kontoinstanzen finden Sie unter [Erstellen einer Kontoinstanz von AWS IAM Identity Center](#). Mit einer Kontoinstanz von IAM Identity Center können Sie unterstützte AWS verwaltete Anwendungen und OpenID Connect (OIDC) -basierte, vom Kunden verwaltete Anwendungen bereitstellen. Kontoinstanzen unterstützen isolierte Bereitstellungen von Anwendungen in einer einzigen AWS-Konto Lösung und nutzen dabei die Funktionen des IAM Identity Center für Personalidentität und Zugriff auf das IAM Identity Center.
 - Einzelheiten zu Organisationsinstanzen finden Sie unter [Organisationsinstanzen von IAM Identity Center](#). Sie können den Zugriff von Benutzern und Gruppen mit einer einzigen Organisationsinstanz zentral verwalten.

- Notieren Sie sich auf der Seite mit den IAM Identity Center-Einstellungen Ihren Instanz-ARN. Sie benötigen diesen Wert, wenn Sie eine Amazon S3 Access Grant-Instance erstellen.



- Erstellen Sie einen oder mehrere Benutzer und optional Gruppen zur Verwendung mit Ihrer Transfer Family Family-Web-App. Wenn Sie ein IAM Identity Center-Verzeichnis als Identitätsanbieter verwenden, können Sie Benutzer auch direkt über die Web-App selbst hinzufügen. Weitere Informationen finden Sie unter [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#).

Konfiguration von IAM-Rollen für Transfer Family Family-Web-Apps

Sie benötigen zwei Rollen: eine für die Verwendung als Identitätsträgerrolle für Ihre Web-App und eine zweite für die Konfiguration einer Zugriffsgewährung. Eine Identitätsträgerrolle ist eine Rolle, die die Identität eines authentifizierten Benutzers in seine Sitzungen einbezieht. Sie wird verwendet, um Anträge auf Datenzugriff im Namen des Benutzers an S3 Access Grants zu stellen.

Note

Sie können das Verfahren zum Erstellen einer Identitätsträgerrolle überspringen. Informationen dazu, wie der Transfer Family Family-Dienst die Identitätsträgerrolle erstellt, finden Sie unter [Eine Transfer Family Family-Web-App erstellen](#). Sie können das Verfahren zum Erstellen einer Rolle mit Zugriffsberechtigungen überspringen. Wählen Sie im Verfahren zum Erstellen einer Zugriffsberechtigung in dem Schritt, in dem Sie einen S3-Standort registrieren, die Option Neue Rolle erstellen aus.

Erstellen Sie eine Rolle als Identitätsträger

- Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>

2. Wählen Sie Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie und fügen Sie dann den folgenden Code ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

4. Wählen Sie Weiter und überspringen Sie dann „Berechtigungen hinzufügen“ und wählen Sie erneut Weiter aus.
5. Geben Sie beispielsweise einen Namen einweb-app-identity-bearer.
6. Wählen Sie Rolle erstellen, um die Rolle des Identitätsträgers zu erstellen.
7. Wählen Sie die Rolle, die Sie gerade erstellt haben, aus der Liste aus und wählen Sie dann im Bereich „Berechtigungsrichtlinien“ die Option „Berechtigungen hinzufügen“ > „Inline-Richtlinie erstellen“.
8. Wählen Sie im Richtlinien-Editor JSON aus und fügen Sie dann den folgenden Codeblock ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}
```



```
]
}
```

9. Geben Sie AllowS3AccessGrants den Richtlinienamen ein und wählen Sie dann Richtlinie erstellen aus.

Als Nächstes erstellen Sie die Rolle, die S3 Access Grants übernimmt, um temporäre Anmeldeinformationen an den Empfänger zu verkaufen.

 Note

Wenn Sie dem Dienst erlauben, die Rolle des Identitätsträgers für Sie zu erstellen, sorgt diese Rolle für den Schutz eines verwirrten Stellvertreters. Daher unterscheidet sich der Code von dem, der hier angezeigt wird.

Erstellen Sie eine Rolle mit Zugriffsberechtigungen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Wählen Sie Rollen und anschließend Rolle erstellen aus. Diese Rolle sollte über die Berechtigung verfügen, auf Ihre S3-Daten in der zuzugreifen AWS-Region.
3. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie und fügen Sie dann den folgenden Code ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

4. Wählen Sie Weiter und fügen Sie eine Mindestrichtlinie hinzu, wie unter [Standort registrieren](#) beschrieben. Obwohl dies nicht empfohlen wird, können Sie die AmazonS3FullAccessverwaltete Richtlinie hinzufügen, da dies für Ihre Bedürfnisse möglicherweise zu freizügig ist.
5. Wählen Sie Weiter und geben Sie einen Namen ein (z. B. access-grants-location).
6. Wählen Sie Rolle erstellen, um die Rolle zu erstellen.

 Note

Wenn Sie dem Dienst gestatten, die Rolle „Zugriffsberechtigungen“ für Sie zu erstellen, sorgt diese Rolle für den Schutz eines verwirrten Stellvertreters. Daher unterscheidet sich der Code von dem, der hier angezeigt wird.

Eine Transfer Family Family-Web-App konfigurieren

In diesem Abschnitt werden die Verfahren zum Erstellen einer Transfer Family Family-Web-App beschrieben. Informationen zum Zuweisen von Benutzern und Gruppen, die sie verwenden können, finden Sie unter [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#).

 Note

Wiederholen Sie diese Verfahren, um weitere Web-Apps hinzuzufügen. Sie können die zuvor erstellten IAM-Rollen wiederverwenden. Stellen Sie sicher, dass Sie die Zugriffsendpunkte für die neuen Web-Apps zur Cross-origin Ressourcenfreigabe (CORS) der einzelnen Buckets hinzufügen.

Eine Transfer Family Family-Web-App erstellen

 Note

Wenn Sie das IAM Identity Center-Verzeichnis nicht für Ihren Identitätsanbieter verwenden, versuchen Sie erst, eine Web-App zu erstellen, wenn Sie IAM Identity Center eingerichtet und einen externen Identitätsanbieter konfiguriert haben, wie unter beschrieben. [Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps](#)

Gehen Sie wie folgt vor, um eine Transfer Family Family-Web-App zu erstellen.

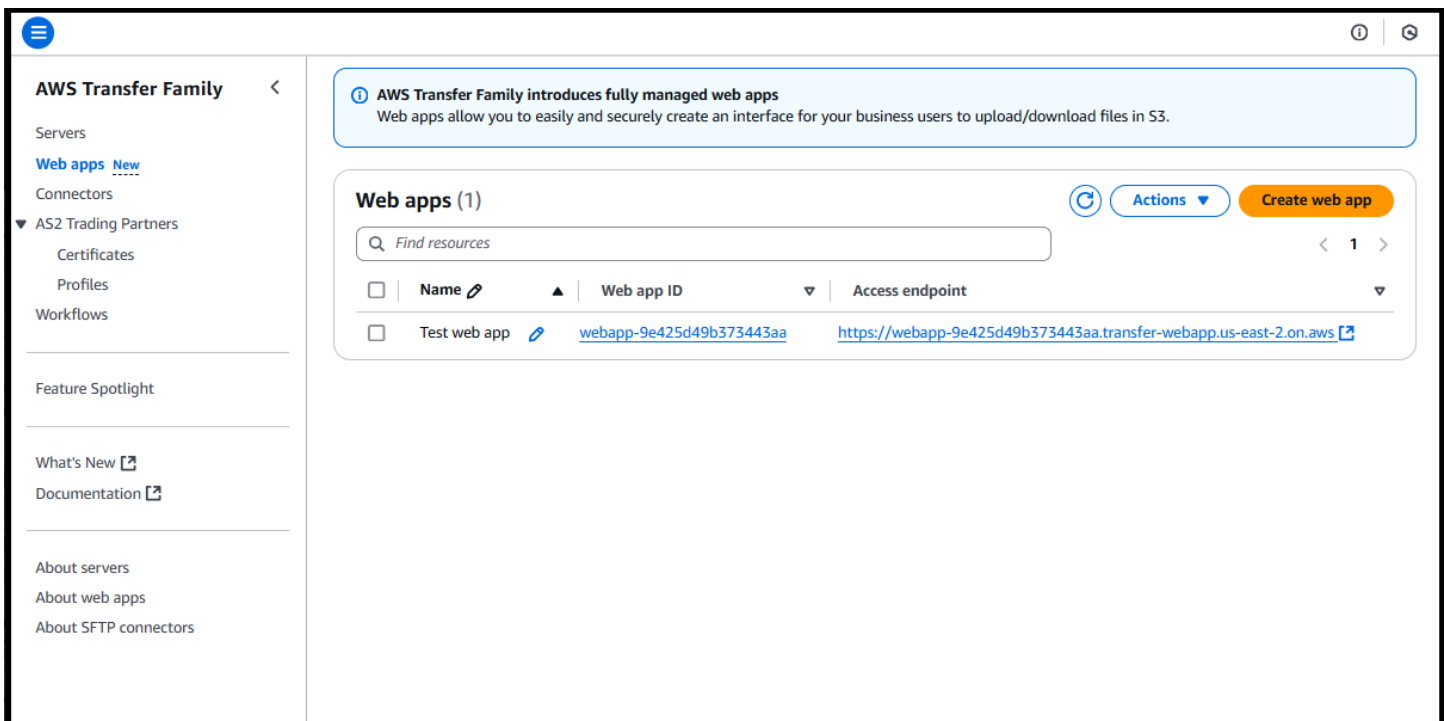
So erstellen Sie eine Transfer Family Family-Web-App

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Web-Apps aus.
3. Wählen Sie Web-App erstellen aus.

Für den Authentifizierungszugriff ist der Bereich wie folgt gefüllt.

- Wenn Sie bereits eine Organisations- oder Kontoinstanz in erstellt haben AWS IAM Identity Center, wird folgende Meldung angezeigt: Ihre AWS Transfer Family Anwendung ist mit einer Kontoinstanz von IAM Identity Center verbunden.
 - Wenn Sie bereits über eine Kontoinstanz verfügen und Mitglied einer Organisationsinstanz sind, können Sie auswählen, mit welcher Instanz Sie eine Verbindung herstellen möchten.
 - Wenn Sie noch keine Kontoinstanz haben oder Mitglied einer Organisationsinstanz sind, werden Ihnen die Optionen zum Erstellen einer Kontoinstanz angezeigt.
4. Wählen Sie als Endpunktyp den Endpunktyp Öffentlich zugänglich aus. Informationen zu einem VPC-gehosteten Endpunkt finden Sie unter [Eine Transfer Family Family-Web-App in einer VPC erstellen](#).
 5. Im Bereich Berechtigungstyp können Sie eine zuvor erstellte Rolle verwenden oder den Dienst eine für Sie erstellen lassen.
 - Wenn Sie bereits eine Rolle als Identitätsträger erstellt haben, wählen Sie Bestehende Rolle verwenden und wählen Sie Ihre Rolle aus dem Menü Vorhandene Rolle auswählen aus.
 - Damit der Dienst eine Rolle für Sie erstellt, wählen Sie Neue Servicerolle erstellen und verwenden aus.
 6. Wählen Sie im Bereich Web-App-Einheiten einen Wert aus. Eine Web-App-Einheit ermöglicht Web-App-Aktivitäten aus bis zu 250 einzelnen Sitzungen. Wenn Sie eine Web-App erstellen, geben Sie an, wie viele Einheiten Sie benötigen, und zwar auf der Grundlage der zu erwartenden Arbeitsauslastungsspitzen. Die Änderung Ihrer Web-App-Einheiten hat Auswirkungen auf Ihre Abrechnung. Informationen zu den Preisen erhalten Sie unter [AWS Transfer Family Preise](#).
 7. Wenn Sie Transfer Family in einem verwenden AWS GovCloud (US) Region, können Sie das Kontrollkästchen FIPS-aktivierter Endpunkt im Bereich FIPS aktiviert aktivieren aktivieren. Für alle anderen AWS-Regionen ist diese Option nicht verfügbar.

8. (Optional) Fügen Sie ein Tag hinzu, um Ihre Web-Apps zu organisieren. Wir empfehlen, dass Sie ein Tag mit Name als Schlüssel und einem beschreibenden Namen als Wert hinzufügen.
9. Wählen Sie Weiter aus. Auf diesem Bildschirm können Sie optional einen Titel für Ihre Web-App angeben. Wenn Sie keinen Titel angeben, wird der Standardtitel Transfer Web App angegeben. Sie können auch Bilddateien für Ihr Logo und Favicon hochladen.
10. Wähle „Weiter“ und dann „Web-App erstellen“.



Note

Stellen Sie sicher, dass Sie eine CORS-Richtlinie (Cross-origin Resource Sharing) für alle Buckets einrichten, auf die vom Web-App-Endpunkt aus zugegriffen wird.

IP-Adressierung

Die Web-Apps der Transfer Family verwenden Dual-Stack-Endpunkte, die sowohl IPv4- als auch IPv6-Konnektivität unterstützen. Für die Authentifizierung verwenden Web-Apps, die auch IPv6 über AWS IAM Identity Center Dual-Stack-Endpunkte unterstützen.

Wenn Ihr Konto Web-Apps in einer Region hatte, als die Unterstützung für Dual-Stack-IAM Identity Center-Endgeräte eingeführt wurde, verwenden alle Web-Apps in diesem Konto und dieser Region aus Gründen der Abwärtskompatibilität weiterhin den IPv4-only IAM Identity Center-Endpunkt. Dies gilt sowohl für bestehende als auch für neu erstellte Web-Apps. Konten, die zum Zeitpunkt des Starts noch nicht über Web-Apps verfügten, verwenden den Dual-Stack-Endpunkt von IAM Identity Center. Wenn Sie ändern müssen, welchen IAM Identity Center-Endpunkt Ihre Web-App verwendet, wenden Sie sich an den AWS Support.

Note

Um festzustellen, welchen Endpunkt Ihre Web-App verwendet, überprüfen Sie die URL, wenn Sie zur IAM Identity Center-Anmeldeseite weitergeleitet werden:

- IPv4-only: `[Region].signin.aws.amazon.com`
- Dual-stack: `[Region].sso.signin.aws`

Wenn Ihr Unternehmen Firewalls oder Netzwerk-Gateways verwendet, sollten Sie sowohl die vorhandenen IPv4- als auch die neuen Dual-Stack-IAM Identity Center-Endpunkte auf eine Zulassungsliste setzen, um einen unterbrechungsfreien Zugriff zu gewährleisten, unabhängig davon, welchen Endpunkt Ihre Web-Apps verwenden. Die vollständige Liste der Domänen und URL-Endpunkte, die zugelassen werden sollen, finden Sie im IAM Identity Center-Benutzerhandbuch unter [Aktualisieren von Firewalls und Gateways, um den Zugriff auf das Zugriffsportal zu ermöglichen](#).

AWS

Eine Transfer Family Family-Web-App in einer VPC erstellen

In diesem Abschnitt werden die Verfahren zum Erstellen einer Transfer Family Family-Web-App in einer VPC beschrieben. Sie können den Endpunkt Ihrer Web-App in einer Virtual Private Cloud (VPC) hosten, um Daten zu und von einem Amazon S3 S3-Bucket zu übertragen, ohne das öffentliche Internet nutzen zu müssen. Informationen zum Zuweisen von Benutzern und Gruppen, die Ihre Web-App verwenden können, finden Sie unter [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#).

Note

Um einen privaten Ende-zu-Ende-Datenfluss bei der Verwendung eines VPC-Endpunkts für die Transfer Family Family-Web-App sicherzustellen, müssen Sie drei zusätzliche

Komponenten implementieren. Richten Sie zunächst einen PrivateLink Endpunkt für Amazon S3 Control API-Operationen ein, der für API-Aufrufe von Amazon S3 Access Grants erforderlich ist. Zweitens konfigurieren Sie einen Endpunkt für den Amazon S3-Datenzugriff, indem Sie entweder einen PrivateLink Amazon S3 Gateway-Endpunkt (für Datenverkehr aus Ihrer VPC) oder einen Amazon S3 S3-Interface-Endpunkt (für Datenverkehr aus lokalen Netzwerken über VPN oder Direct Connect) verwenden. Drittens sperren Sie Ihren Amazon S3 S3-Bucket-Zugriff, indem Sie die Bucket-Richtlinien so aktualisieren, dass nur Verkehr von diesen VPC-Endpunkten zugelassen wird. Diese Kombination stellt sicher, dass alle Datenübertragungen innerhalb Ihrer privaten Netzwerkinfrastruktur bleiben und niemals das öffentliche Internet durchqueren.

Eine Transfer Family Family-Web-App erstellen

Voraussetzungen

- AWS IAM Identity Center mit dem konfigurierten Identitätsanbieter einrichten. Siehe [Konfigurieren Sie Ihren Identitätsanbieter für Transfer Family Family-Web-Apps](#).
- Einrichtung von VPC- und Netzwerkkomponenten. Siehe [Eine VPC erstellen](#).
- API-Endpunkt, der für Amazon S3 Control-Operationen eingerichtet wurde. Weitere Informationen finden Sie unter [Zugreifen auf Endpunkte der Amazon S3 S3-Schnittstelle](#).
- VPC-Endpunkte für Amazon S3 (Gateway oder Interface) eingerichtet. Siehe [Typen von VPC-Endpunkten für Amazon S3](#). Wenn Sie einen Schnittstellenendpunkt verwenden, müssen Sie privates DNS aktivieren. Ein Beispiel finden Sie unter [Einführung der privaten DNS-Unterstützung für Amazon S3 mit AWS PrivateLink](#).

Note

AWS IAM Identity Center unterstützt keine VPC-Endpunkte; alle Authentifizierungsanfragen werden über das öffentliche Internet übertragen. Darüber hinaus benötigen Webanwendungen der Transfer Family Internetzugang, um statische Inhalte (wie CSS JavaScript - und HTML-Dateien) zu laden. Die Anforderungen für den öffentlichen Internetzugang sind vom Datenzugriff getrennt. Ihr VPC-Endpunkt stellt sicher, dass Verbindungen durch Ihre VPC-Infrastruktur geleitet werden.

So erstellen Sie eine Transfer Family Family-Web-App

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Web-Apps aus.
3. Wählen Sie Web-App erstellen aus. Für den Authentifizierungszugriff ist der Bereich wie folgt gefüllt.
 - Wenn Sie bereits eine Organisations- oder Kontoinstanz in erstellt haben AWS IAM Identity Center, wird folgende Meldung angezeigt: Ihre AWS Transfer Family Anwendung ist mit einer Kontoinstanz von IAM Identity Center verbunden.
 - Wenn Sie bereits über eine Kontoinstanz verfügen und Mitglied einer Organisationsinstanz sind, können Sie auswählen, mit welcher Instanz Sie eine Verbindung herstellen möchten.
 - Wenn Sie noch keine Kontoinstanz haben oder Mitglied einer Organisationsinstanz sind, werden Ihnen die Optionen zum Erstellen einer Kontoinstanz angezeigt.
4. Wählen Sie im Abschnitt Endpunktkonfiguration aus, wie Ihre Benutzer auf Ihre Web-App zugreifen sollen:
 - Öffentlich zugänglich: Ihr Web-App-Endpunkt ist öffentlich über HTTPS zugänglich. Für diese Option ist keine VPC-Konfiguration erforderlich, sodass sie einfach einzurichten ist und sich für Anwendungen eignet, die für eine breite öffentliche Nutzung vorgesehen sind.
 - VPC-gehostet: Ihr Web-App-Endpunkt wird in Ihrer Virtual Private Cloud (VPC) gehostet und bietet privaten Netzwerkzugriff über Ihr VPC-Netzwerk oder AWS Direct Connect VPN-Verbindungen. Diese Option bietet verbesserte Sicherheit durch Netzwerkisolierung und wird für interne Anwendungen empfohlen.

Bei der Konfiguration eines VPC-gehosteten Endpunkts müssen Sie Folgendes angeben:

- VPC: Wählen Sie eine bestehende VPC aus oder erstellen Sie eine neue. Die Schaltfläche „VPC erstellen“ ist verfügbar.
- Verfügbarkeitszonen: Wählen Sie die Verfügbarkeitszonen aus, in denen Ihr Endpunkt bereitgestellt werden soll.
- Subnetze: Wählen Sie Subnetze innerhalb jeder ausgewählten Verfügbarkeitszone aus.
- Sicherheitsgruppen: Wählen oder erstellen Sie Sicherheitsgruppen, um den Zugriff auf der Grundlage von Quell-IP-Adressen zu steuern. Wenn nicht angegeben, wird die Standardsicherheitsgruppe der VPC verwendet. Verwalten Sie Sicherheitsgruppen über die VPC-Konsole. Konfigurieren Sie Ihre VPC-Sicherheitsgruppen so, dass eingehender

Datenverkehr von Ihrem Netzwerk über HTTPS auf TCP-Port 443 zugelassen wird. Dies ist für die IAM Identity Center-Authentifizierung und das Laden statischer Inhalte von Web-Apps erforderlich.

 Note

Der Zugriffsendpunkt kann nicht für VPC-Endpunkte angepasst werden. Verwenden Sie den öffentlichen Endpunkt, um eine benutzerdefinierte URL hinzuzufügen.

Post-creation Schritte

- Stellen Sie sicher, dass Sie eine Richtlinie zur gemeinsamen Nutzung von Cross-origin Ressourcen (CORS) für alle Buckets einrichten, auf die vom Web-App-Endpunkt aus zugegriffen wird. Siehe [Cross-origin Richtlinie zur gemeinsamen Nutzung von Ressourcen \(CORS\)](#).
- Aktualisieren Sie Ihre Bucket-Richtlinie, sodass nur Traffic, der von Ihrer VPC stammt, über Ihren VPC-Endpunkt zugelassen wird. Siehe [Beschränken des Zugriffs auf einen bestimmten VPC-Endpunkt](#).
- Weisen Sie der Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu. Siehe [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#).

Cross-origin Richtlinie zur gemeinsamen Nutzung von Ressourcen (CORS)

Sie müssen Cross-Origin Resource Sharing (CORS) für alle Buckets einrichten, die von Ihrer Web-App verwendet werden. Weitere Informationen über CORS finden Sie unter [Richten Sie Cross-origin Resource Sharing \(CORS\) für Ihren Bucket ein](#).

 Important

Bevor Sie die folgende Beispielrichtlinie verwenden, ersetzen Sie Allowed Origin durch Ihren Zugriffsendpunkt. Andernfalls erhalten Ihre Endbenutzer eine Fehlermeldung, wenn sie versuchen, auf einen Standort in Ihrer Web-App zuzugreifen.

Beispiel für eine Richtlinie:


```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

Beschränken des Zugriffs auf einen bestimmten VPC-Endpunkt

Nachfolgend finden Sie ein Beispiel für eine Amazon-S3-Bucket-Richtlinie, die den Zugriff auf einen bestimmten Bucket einschränkt, `amzn-s3-demo-bucket`, nur vom VPC-Endpunkt mit der ID `vpce-1a2b3c4d`. Wenn der angegebene Endpunkt nicht verwendet wird, verweigert die Richtlinie jeglichen Zugriff auf den Bucket. Die `aws:SourceVpce`-Bedingung gibt den Endpunkt an. Die `aws:SourceVpce`-Bedingung benötigt keine ARN für die VPC-Endpunkt-Ressource, sondern nur die VPC-Endpunkt-ID. Weitere Informationen zur Aktualisierung Ihrer Bucket-Richtlinie, sodass nur Traffic zugelassen wird, der von Ihrer VPC stammt, finden Sie unter [Steuern des Zugriffs von](#)

[VPC-Endpunkten mit](#) Bucket-Richtlinien. Weitere Informationen zur Verwendung von Bedingungen in einer Richtlinie finden Sie unter [Beispiele für Bucket-Richtlinien mit](#) Bedingungsschlüsseln. Als Voraussetzung für die Anwendung dieser Richtlinie sollten Sie einen [Amazon S3 S3-VPC-Endpunkt](#) erstellen.

⚠ Important

Bevor Sie die folgende Beispielrichtlinie verwenden, ersetzen Sie die VPC-Endpunkt-ID durch einen geeigneten Wert für Ihren Anwendungsfall. Andernfalls können Sie nicht auf Ihren Bucket zugreifen.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",
                  "arn:aws:s3:::amzn-s3-demo-bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu

Nachdem Sie eine Transfer Family Family-Web-App erstellt haben, können Sie Benutzern und Gruppen zuweisen, die dann auf die Web-App zugreifen können. Sie können entweder Benutzer abrufen, die bereits im IAM Identity Center erstellt und gespeichert wurden, oder Sie können [neue Benutzer direkt hinzufügen](#) (wenn Sie ein IAM Identity Center-Verzeichnis als Identitätsanbieter

verwenden). Wenn Sie neue Benutzer hinzufügen, werden diese auch zu Ihrer IAM Identity Center-Instanz hinzugefügt.

Beachten Sie Folgendes:

- Sie können nur neue Benutzer hinzufügen, wenn Sie das IAM Identity Center-Verzeichnis als Identitätsquelle verwenden und über die entsprechenden Berechtigungen verfügen. Wenn Sie Mitglied einer Organisationsinstanz sind, verfügen Sie möglicherweise nicht über die erforderlichen Berechtigungen, um Benutzer hinzuzufügen.

 Note

Wenn Sie Ihrer Anwendung keine Benutzer oder Gruppen zuweisen, erhalten Ihre Benutzer eine Fehlermeldung, wenn sie versuchen, sich bei Ihrer Web-App anzumelden.

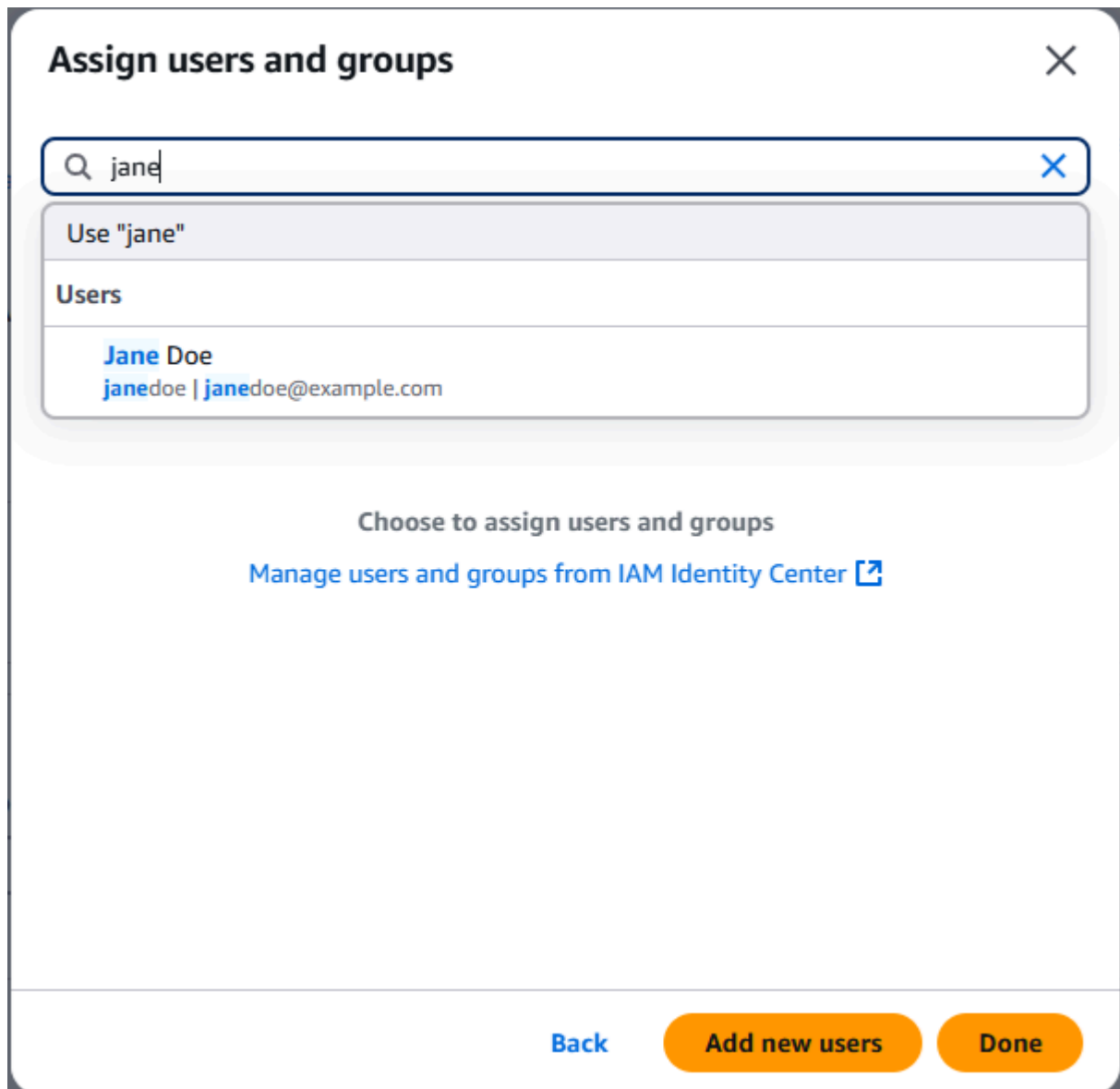
- Wenn Sie einen neuen Benutzer erstellen, müssen Sie diesem Benutzer auch eine S3-Zugriffsberechtigung gewähren, damit er auf Daten in Ihrer Web-App zugreifen kann.
- Nachdem Sie einen neuen Benutzer erstellt haben, erhält dieser Benutzer vom IAM Identity Center eine Onboarding-E-Mail mit Anweisungen zum weiteren Vorgehen.

So weisen Sie Benutzer einer Transfer Family Family-Web-App zu

1. Navigieren Sie zu Ihrer Web-App-Liste und wählen Sie die aus, die Sie bearbeiten möchten.
2. Wählen Sie Benutzer und Gruppen zuweisen aus.

The screenshot shows the AWS IAM Identity Center console interface for a web application. At the top, there's a header with the application name 'webapp-' followed by a redacted ID. Action buttons include 'Assign users and groups' (orange), 'Clear customization', and 'Delete'. Below this is the 'Web app details' section, which includes an 'Access endpoint' (a URL to a transfer-webapp instance), 'Web app endpoint' (another URL), 'Web app units' (1), 'Identity provider' (AWS IAM Identity Center), 'IAM role' (a redacted role), and 'Instance ARN' (arn:aws:sso:::instance/ssoins- followed by a redacted ID). An 'Edit' button is in the top right of this section. Below the details is a tabbed interface with 'Users' selected. The 'Users (2)' section shows a search bar and a table with two columns: 'Display name' and 'User ID'. Two users are listed, each with a checkbox, a display name, a user ID, and a username. A 'Delete' button is in the top right of the users section.

3. Um Benutzer zuzuweisen, die Sie zuvor in IAM Identity Center erstellt haben, wählen Sie Bestehende Benutzer und Gruppen zuweisen. Um neue Benutzer zu erstellen, fahren Sie mit Schritt 4 fort.
 - a. Ein Informationsbildschirm wird angezeigt. Wählen Sie Erste Schritte, um fortzufahren.
 - b. Suchen Sie nach dem Benutzer. Beachten Sie, dass keine Benutzer angezeigt werden, bis Sie mit der Eingabe Ihrer Suchkriterien beginnen. Sie müssen nach dem Anzeigenamen suchen, nicht nach dem Benutzernamen, falls es sich um einen anderen handelt. Es werden nur exakte Treffer zurückgegeben. Wenn Sie Ihren Benutzer nicht finden können, navigieren Sie zur IAM Identity Center-Managementkonsole, suchen Sie den Benutzer, kopieren Sie seinen Anzeigenamen und fügen Sie ihn hier ein.



- c. Wählen Sie die Benutzer und Gruppen aus, die Sie hinzufügen möchten, und wählen Sie dann Zuweisen.
4. Um einen neuen Benutzer zu erstellen, wählen Sie Hinzufügen und weisen Sie neue Benutzer zu.
 - a. Ein Informationsbildschirm wird angezeigt. Wählen Sie Erste Schritte, um fortzufahren.
 - b. Wählen Sie Neue Benutzer hinzufügen aus.
 - c. Geben Sie die folgenden Benutzerdetails in das Dialogfeld ein: Benutzername, Vor- und Nachname sowie eine E-Mail-Adresse.

Add new users

Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#)

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

johnstiles

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +, -, @, _

First name	Last name
John	Stiles
Email address	Confirm email address
johnstiles@example.com	johnstiles@example.com
Display name This is typically the full name of the user (first and last name) and appears in the users list.	
John Stiles	

[Cancel](#)[Next](#)

- d. Wählen Sie Weiter und dann Hinzufügen, um den Benutzer hinzuzufügen und das Dialogfeld zu schließen, oder klicken Sie auf Neuen Benutzer hinzufügen, um einen weiteren Benutzer zu erstellen.

Richten Sie Cross-origin Resource Sharing (CORS) für Ihren Bucket ein

Sie müssen Cross-Origin Resource Sharing (CORS) für alle Buckets einrichten, die von Ihrer Web-App verwendet werden. Eine CORS-Konfiguration ist ein Dokument, das Regeln definiert, die die Ursprünge identifizieren, denen Sie den Zugriff auf Ihren Bucket gewähren. Weitere Informationen zu CORS finden Sie unter [Konfiguration von Cross-Origin Resource Sharing \(CORS\)](#).

 Important

Wenn Sie CORS nicht einrichten, erhalten Ihre Endbenutzer eine Fehlermeldung, wenn sie versuchen, auf einen Standort in Ihrer Web-App zuzugreifen.

So richten Sie Cross-origin Resource Sharing (CORS) für Ihren Amazon S3 S3-Bucket ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie im linken Navigationsbereich Buckets aus, suchen Sie im Suchdialogfeld nach Ihrem Bucket und wählen Sie dann den Tab Permissions.
3. Wählen Sie unter Cross-origin Resource Sharing (CORS) die Option Bearbeiten aus und fügen Sie den folgenden Code ein. *WebAppEndpoint* Ersetzen Sie es durch den tatsächlichen Zugriffsendpunkt für Ihre Web-App. Dies kann entweder der VPC-gehostete Endpunkt oder der öffentliche Zugriffsendpunkt sein, der bei der Erstellung der Web-App erstellt wird, oder ein benutzerdefinierter Zugriffsendpunkt, falls Sie einen erstellen. Achten Sie darauf, keine abschließenden Schrägstriche einzugeben, da dies zu Fehlern führt, wenn Benutzer versuchen, sich bei Ihrer Web-App anzumelden.
 - Falsches Beispiel: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Richtige Beispiele:
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Wenn Sie einen Bucket für mehrere Web-Apps wiederverwenden, fügen Sie deren Endpunkte an die Liste an. `AllowedOrigins`

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
```

```
    "PUT",
    "POST",
    "DELETE",
    "HEAD"
  ],
  "AllowedOrigins": [
    "https://WebAppEndpoint"
  ],
  "ExposeHeaders": [
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
```

4. Wählen Sie Änderungen speichern, um das CORS zu aktualisieren.

Informationen zum Testen Ihrer CORS-Konfiguration finden Sie unter CORS [testen](#).

Amazon S3 S3-Zugriffsberechtigungen für Transfer Family Family-Web-Apps konfigurieren

In diesem Thema wird beschrieben, wie Sie mithilfe von Amazon S3 Access Grants eine Zugriffsberechtigung hinzufügen. Diese Zugriffsberechtigung definiert den direkten Zugriff auf Ihre Daten für Ihre Benutzer und Gruppen in Ihrem Unternehmensverzeichnis und gewährt temporäre Zugangsdaten auf der Grundlage von Zuschüssen nach dem Prinzip „Just-in-Time“ mit den geringsten Rechten. Eine individuelle Erteilung in einer S3 Access Grants-Instanz ermöglicht es einem bestimmten Benutzer oder einer bestimmten Gruppe in einem Unternehmensverzeichnis, Zugriff von einem Standort aus zu erhalten, der in Ihrer S3 Access Grants-Instanz registriert

ist. Weitere Informationen finden Sie unter [Konzepte von S3 Access Grants](#) im Amazon S3 S3-Benutzerhandbuch.

 Note

Sie können das IAM Identity Center-Verzeichnis mit S3 Access Grants nur mit Transfer Family Family-Web-Apps verwenden.

Sie müssen eine Amazon S3-Zugriffsberechtigung für die Weitergabe von Identitäten angeben. Eine Amazon S3 S3-Zugriffserteilung speichert die Daten, auf die Ihre Endbenutzer zugreifen müssen. Wenn sich Ihre Endbenutzer bei Ihrer Transfer Family Family-Web-App anmelden, gibt S3 Access Grants die Identität eines Benutzers an die vertrauenswürdige Anwendung weiter. In diesem Abschnitt wird beschrieben, wie Sie eine Amazon S3 S3-Zugriffs-Grant-Instance und anschließend eine Zugriffsgewährung für einen Amazon S3 S3-Bucket hinzufügen und konfigurieren.

 Note

Halten Sie den [ARN und die Benutzer- oder Gruppen-ID Ihrer IAM Identity Center-Instanz](#) bereit, da Sie sie benötigen, um die Einrichtung Ihrer Zugriffsgewährung abzuschließen.

So erstellen Sie einen Zuschuss mithilfe von Amazon S3 Access Grants

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Erstellen Sie einen Bucket oder notieren Sie sich einen vorhandenen Bucket, den Sie mit Ihrer Web-App verwenden möchten. Informationen zum Erstellen von Buckets finden Sie im [Amazon S3 S3-Benutzerhandbuch](#).
3. Wählen Sie im linken Navigationsbereich Access Grants aus.
4. Wählen Sie Create S3 Access Grants-Instanz aus und geben Sie die folgenden Informationen ein.
 - Wählen Sie IAM Identity Center-Instanz hinzufügen aus **your-Region**, in der sich Ihre **your-Region** AWS-Region befindet. Lassen Sie dieses Feld deaktiviert, wenn Sie IAM Identity Center nicht als Identitätsanbieter verwenden.
 - Fügen Sie den ARN Ihrer IAM Identity Center-Instanz ein.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
☒ **Create S3 Access Grants instance**
- Step 2
☐ Register S3 Buckets or prefixes as locations
- Step 3
☐ Create grant
- Step 4
☐ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoin-

Format: arn:aws:sso::instance/<instanceidentifier>

Wählen Sie Next (Weiter), um fortzufahren.

- Registrieren Sie S3-Buckets oder -Präfixe als Standorte. Wir empfehlen, den Standardstandort zu registrieren und ihn einer IAM-Rolle zuzuordnen. `s3://` Der Speicherort an diesem Standardpfad deckt den Zugriff auf all Ihre Amazon S3 S3-Buckets in Ihrem Konto ab. AWS-Region Wenn Sie eine Zugriffsberechtigung erstellen, können Sie den Bereich auf einen Bucket, ein Präfix oder ein Objekt innerhalb des Standardspeicherorts einschränken.

Geben Sie die folgenden Informationen ein:

- Suchen Sie für den Bereich nach einem Bucket oder geben Sie den Namen Ihres Buckets und optional ein Präfix ein.
- Wählen Sie für die IAM-Rolle die Option Neue Rolle erstellen aus, damit der Service eine Rolle erstellt.

Alternativ können Sie die Rolle selbst erstellen, wie unter beschrieben [Konfiguration von IAM-Rollen für Transfer Family Family-Web-Apps](#), und dann ihren ARN hier eingeben.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
 Format for bucket: s3://<bucket>
 Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

Permissions

To ensure the role has proper permissions to access the location scope, consult the [list of permissions](#).

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Wählen Sie Next (Weiter), um fortzufahren.

6. Geben Sie auf dem Bildschirm „Grant erstellen“ die folgenden Details an.

- Wählen Sie für Berechtigungen die Option Lesen und Schreiben aus. Die Zugriffsberechtigungen können entweder schreibgeschützt oder lesend und schreibgeschützt sein, Schreibzugriff wird jedoch nicht unterstützt.
- Wählen Sie als Typ des Empfängers die Option Verzeichnisidentität aus dem IAM Identity Center aus.
- Wählen Sie als Identitätstyp des Verzeichnisses die Option Benutzer oder Gruppe aus, je nachdem, welchen Typ Sie jetzt registrieren möchten.
- Fügen Sie in IAM Identity Center user/group ID die ID für Ihren Benutzer oder Ihre Gruppe ein. Diese ID ist in der IAM Identity Center-Konsole und in Ihrer Transfer Family Family-Web-App in Ihrer Benutzer- und Gruppentabelle verfügbar.

Create Grant [Info](#)

Grant [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)

IAM role [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Wählen Sie Weiter aus.

- Überprüfen Sie die Einstellungen auf dem Bildschirm. Wenn alles korrekt ist, wählen Sie Fertig stellen, um die Zugriffsgewährung zu erstellen. Sie können auch Abbrechen oder Zurück wählen, um Änderungen vorzunehmen.

- Step 1
Create S3 Access Grants instance
- Step 2
Register S3 Buckets or prefixes as locations
- Step 3
Create grant
- Step 4
Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region
You can create one S3 Access Grants instance per AWS Region per account.
US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional
You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.
arn:aws:sso:::application/ssoinstance:/apl

Successfully created S3 Access Grants instance
Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the [Resource Access Management console](#)

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope
s3://

IAM role
web-app-beta-access-grants

Successfully registered location
Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope
s3:///*

IAM role
web-app-beta-access-grants

Location ID

Permissions and access

Access Type READWRITE	Grantee type Directory identity user	Grantee ID	Application - optional

Successfully created grant
Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel Previous Finish

Amazon S3 S3-Zugriffsberechtigungen konfigurieren

330

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)
arn:aws:s3:us-east-2:access-grants/default

Creation date
October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

IAM Identity Center

DeregisterAdd

IAM Identity Center instance ARN
arn:aws:sso:application/ssoins/apl

GrantsLocations

Grants (1)

DeleteCreate Grant

Find by grant scope or grantee

Grant scope	Grant ID	Permission	Grantee type	Grantee ID	Creation date	Location ID	Application ARN
s3:///*		Read, Write	Directory identity user		October 25, 2024, 11:57:30 (UTC-04:00)		ALL

Damit ist die Einrichtung für Ihre Web-App abgeschlossen. Die Benutzer und Gruppen, die Sie konfiguriert haben, können die Web-App am Access Point aufrufen, sich anmelden und Dateien hoch- und herunterladen.

Aktualisieren Sie Ihren Zugriffsendpunkt mit einer benutzerdefinierten URL

Der Standardzugriffsendpunkt, der mit Ihrer Web-App erstellt wird, enthält vom Dienst generierte Identifikatoren. Um ein Markenerlebnis zu bieten, möchten Sie möglicherweise eine benutzerdefinierte URL angeben, über die Ihre Transfer Family-Web-App auf Ihre Transfer Family Family-Web-App zugreifen können. In diesem Thema wird beschrieben, wie Sie Ihren Zugriffsendpunkt mit einer benutzerdefinierten URL aktualisieren.

Note

Der Zugriffsendpunkt kann nicht für VPC-Endpunkte angepasst werden. Verwenden Sie den öffentlichen Endpunkt, um eine benutzerdefinierte URL hinzuzufügen.

 Note

Das folgende Verfahren setzt voraus, dass Sie die empfohlene [CloudFormation Stack-Vorlage](#) verwenden. Sie müssen die Vorlage nicht verwenden: Sie können die Distribution direkt über die [CloudFront Konsole](#) erstellen.

Die mitgelieferte Vorlage vereinfacht jedoch den Prozess und macht es einfacher, Fehlkonfigurationen zu vermeiden. Wenn Sie die CloudFormation Vorlage nicht verwenden, beachten Sie unbedingt die folgenden Richtlinien:

- Die [Origin-Anforderungsrichtlinie](#) sollte Abfragezeichenfolgen und Cookies an den Ursprung weiterleiten und sollte den Host Header nicht an den Ursprung weiterleiten.
- Die [Cache-Richtlinie](#) sollte den Host Header nicht im Cache-Schlüssel enthalten.

So passen Sie die URL Ihrer Web-App an

1. Erstellen Sie eine CloudFront Verteilung mithilfe der von Transfer Family bereitgestellten AWS CloudFormation Vorlage, der [CloudFormation Stapelvorlage](#).
 - a. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
 - b. Wählen Sie Create Stack und geben Sie Folgendes an.
 - Wählen Sie im Abschnitt Voraussetzung — Vorlage vorbereiten die Option Vorhandene Vorlage auswählen aus.
 - Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagendatei hochladen) aus.
 - Speichern Sie die [CloudFormation Stack-Vorlagendatei](#) und laden Sie sie dann hier hoch.
 - c. Wählen Sie Weiter und geben Sie die folgenden Informationen ein.
 - WebAppEndpoint: kopiere den Wert aus deiner Web-App
 - AccessEndpoint: Geben Sie den benutzerdefinierten Domainnamen an, den Sie verwenden möchten
 - AcmCertificateArn: Geben Sie den ARN für ein öffentliches oder privates SSL/TLS Zertifikat an, das gespeichert ist in AWS Certificate Manager
 - d. Schließen Sie den CloudFormation Assistenten ab, bis Ihr neuer Stack erstellt ist.

2. Bearbeiten Sie in Ihrer Web-App den Access-Endpunkt und aktualisieren Sie die benutzerdefinierte URL auf die URL, die Sie verwenden möchten.

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

`https://my-custom-url`

[Create a new distribution](#)

3. Erstellen Sie DNS-Einträge, um den Datenverkehr für Ihren benutzerdefinierten Domainnamen an die CloudFront Distribution weiterzuleiten. Wenn Sie Route 53 für die Zone verwenden, können Sie einen Alias- oder CNAME-Eintrag für den CloudFront Distributionsnamen erstellen (z. B. xxxx.cloudfront.net). Informationen zur Verwendung von Amazon Route 53 mit CloudFront finden Sie unter [Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an eine CloudFront Verteilung](#).
4. Aktualisieren Sie Ihre ursprungsübergreifende Richtlinie zur gemeinsamen Nutzung von Ressourcen, indem Sie den Standardzugriffsendpunkt durch die folgende Zeile im AllowedOrigins Codeblock ersetzen:

```
"https://custom-url"
```

Sie müssen diese Änderung für jeden Bucket vornehmen, der von Ihrer Web-App verwendet wird.

Nachdem Sie Ihr Update vorgenommen haben, sollte der AllowedOrigins Abschnitt Ihrer CORS-Richtlinie wie folgt aussehen:


```
"AllowedOrigins": [  
    "https://custom-url"],
```

Sie benötigen nur einen einzigen AllowedOrigins Eintrag für jede Transfer Family Family-Web-App.

Weitere Informationen finden [Sie im Verfahren zur Einrichtung von Cross-origin Resource Sharing \(CORS\) für Ihren Amazon S3 S3-Bucket](#).

Sie können jetzt Ihren benutzerdefinierten Zugriffsendpunkt aufrufen und diesen Link mit Ihren Endbenutzern teilen.

CloudTrail Protokollierung für Transfer Family Family-Web-Apps

CloudTrail ist eine AWS-Service , die eine Aufzeichnung der Aktionen erstellt, die in Ihrem ausgeführt wurden AWS-Konto. Es überwacht und zeichnet kontinuierlich API-Operationen für Aktivitäten wie Konsolenanmeldungen, AWS Command Line Interface Befehle und SDK/API Operationen auf. Auf diese Weise können Sie protokollieren, wer wann und von wo aus welche Maßnahmen ergriffen hat. CloudTrail hilft bei der Prüfung, beim Zugriffsmanagement und bei der Einhaltung gesetzlicher Vorschriften, indem es einen Verlauf aller Aktivitäten in Ihrer AWS Umgebung bereitstellt.

Bei Transfer Family Family-Web-Apps können Sie sowohl Authentifizierungsereignisse als auch Datenzugriffsvorgänge Ihrer Benutzer verfolgen. Um eine umfassende Protokollierung zu aktivieren, müssen Sie:

1. Konfigurieren Sie CloudTrail die Konfiguration so, dass Verwaltungsereignisse zur Nachverfolgung von Authentifizierungsaktivitäten protokolliert werden.
2. Aktivieren Sie Amazon S3 S3-Datenereignisse, um Dateioperationen zu verfolgen, die über Ihre Web-App ausgeführt werden.

Informationen finden Sie auch unter:

- [CloudTrail Anwendungsfälle für IAM Identity Center](#)
- [Grundlegendes zu den Anmeldeereignissen im IAM Identity Center](#)
- [CloudTrail UserIdentity-Element](#)
- [Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte](#)

- [Amazon S3 CloudTrail S3-Ereignisse](#)

Amazon S3 S3-Datenereignisse aktivieren

Um Dateioperationen zu verfolgen, die über Transfer Family Family-Web-Apps auf Ihren Amazon S3 S3-Buckets ausgeführt werden, müssen Sie Datenereignisse für diese Buckets aktivieren. Datenereignisse ermöglichen API-Aktivitäten auf Objektebene und sind besonders nützlich für die Nachverfolgung von Datei-Uploads, Downloads und anderen Vorgängen, die von Web-App-Benutzern ausgeführt werden.

So aktivieren Sie Amazon S3 S3-Datenereignisse für Ihre Transfer Family Family-Web-App:

1. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Trails aus und wählen Sie dann einen vorhandenen Trail aus, oder erstellen Sie einen neuen.
3. Wählen Sie unter Erweiterte Event-Selektoren die Option Bearbeiten aus.
4. Wählen Sie Erweiterte Eventauswahl hinzufügen aus.
5. Für die erste Felddauswahl:
 - Setzen Sie das Feld auf `eventCategory`
 - Setzen Sie Operator auf Gleich
 - Setzen Sie den Wert auf `Data`
6. Wählen Sie Feld hinzufügen und für die zweite Felddauswahl:
 - Setzen Sie Feld auf `resources.type`
 - Setzen Sie Operator auf Gleich
 - Setzen Sie den Wert auf `AWS::S3::Object`
7. (Optional) Um Ereignisse nur für bestimmte Buckets zu protokollieren, wählen Sie Feld hinzufügen und fügen Sie Folgendes hinzu:
 - Setzen Sie Feld auf `resources.ARN`
 - Setzen Sie den Operator auf Beginnt mit
 - Setzen Sie den Wert auf `arn:aws:s3:::your-bucket-name/`
8. Wählen Sie Änderungen speichern aus.

Alternativ können Sie die Konfiguration für ältere Datenereignisse verwenden:

1. Wählen Sie unter Datenereignisse die Option Bearbeiten aus.
2. Wählen Sie als Datenereignistyp die Option S3-Bucket- und Objektereignisse aus.
3. Wählen Sie die Amazon S3 S3-Buckets aus, für die Datenereignisse protokolliert werden sollen.
Sie können Alle aktuellen und future S3-Buckets auswählen oder einzelne Buckets angeben.
4. Wählen Sie aus, ob Leseereignisse, Schreibereignisse oder beides protokolliert werden sollen.
5. Wählen Sie Änderungen speichern aus.

Nachdem Sie Datenereignisse aktiviert haben, können Sie auf diese Protokolle in dem Amazon S3 S3-Bucket zugreifen, für den Sie konfiguriert sind CloudTrail. Die Protokolle enthalten Details wie den Benutzer, der die Aktion ausgeführt hat, den Zeitstempel der Aktion, das betroffene Objekt und das `onBehalfOf` Feld, mit dem die vier Aktionen verfolgt werden können, die über die `userId` Transfer Family Family-Web-Apps ausgeführt wurden.

Ihre Logs finden und einsehen

Es gibt verschiedene Möglichkeiten, CloudTrail Protokolle für Ihre Transfer Family Family-Web-App zu finden und anzuzeigen:

Verwenden der CloudTrail Konsole

Der schnellste Weg, sich aktuelle Ereignisse anzusehen:

1. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie Eventverlauf aus.
3. Ereignisse filtern nach:
 - Ereignisquelle: `signin.amazonaws.com` für Web-App-Ereignisse
 - Ereignisquelle: `s3.amazonaws.com` für Dateioperationen
4. Klicken Sie auf ein Ereignis, um detaillierte Informationen anzuzeigen.

Zugreifen auf Protokolle in Amazon S3

So greifen Sie auf die vollständigen Protokolldateien zu, die in Amazon S3 gespeichert sind:

1. Identifizieren Sie den Amazon S3 S3-Bucket Ihres CloudTrail Trails:

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Navigieren Sie zu den Protokolldateien in Amazon S3:

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Laden Sie die Protokolldateien für Ihre Web-App-ID herunter und durchsuchen Sie sie:

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Wird AWS CLI zur Suche nach Ereignissen verwendet

Suchen Sie mithilfe der folgenden Optionen nach bestimmten Web-App-Ereignissen AWS CLI:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

Oder suchen Sie nach Authentifizierungsereignissen:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Beispiele für Authentifizierungsprotokolle

CloudTrail protokolliert Authentifizierungsereignisse für Transfer Family Family-Web-Apps, sodass Sie erfolgreiche und fehlgeschlagene Anmeldeversuche verfolgen können. Diese Protokolle sind besonders nützlich für Sicherheitsüberwachungs- und Compliance-Zwecke.

Themen

- [Beispiel für einen Protokolleintrag zur Überprüfung der Anmeldeinformationen](#)
- [Beispiel für einen Protokolleintrag für die Anmeldeauthentifizierung](#)
- [Beispiel für einen Protokolleintrag für ListCallerAccessGrants](#)

- [Beispiel für einen Protokolleintrag für ein GetDataAccess Ereignis](#)

Beispiel für einen Protokolleintrag zur Überprüfung der Anmeldeinformationen

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für ein Ereignis zur Überprüfung der Anmeldeinformationen, das während des Authentifizierungsprozesses auftritt.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
  },
  "eventTime": "2025-08-08T15:29:30Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.224",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
    "CredentialType": "PASSWORD"
  },
  "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
  "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
```

```

    "CredentialVerification": "Success"
  },
  "eventCategory": "Management"
}

```

Dieses Ereignis bietet zusätzliche Informationen über den Schritt zur Überprüfung der Anmeldeinformationen im Authentifizierungsprozess und zeigt die spezifische Anmeldeinformations-ID und die verwendete Authentifizierungsworkflow-ID an.

Beispiel für einen Protokolleintrag für die Anmeldeauthentifizierung

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für ein erfolgreiches Benutzerauthentifizierungsereignis bei der Web-App-Anmeldung mit IAM Identity Center.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  }
}

```

```

    },
    "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
    "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "UserAuthentication": "Success"
    },
    "eventCategory": "Management"
}

```

Beachten Sie in diesem Beispiel die folgenden wichtigen Felder:

- `eventSource`: Zeigt „signin.amazonaws.com“ an, was darauf hinweist, dass es sich um ein IAM Identity Center-Authentifizierungsereignis handelt.
- `userIdentity.onBehalfOf`: Enthält die Benutzer-ID und den Identitätsspeicher-ARN für den Web-App-Benutzer.
- `additionalEventData.LoginTo`: Zeigt die URL der IAM Identity Center-Anwendung an, auf die zugegriffen wird.
- `additionalEventData.CredentialType`: Gibt die verwendete Authentifizierungsmethode an (PASSWORD).
- `serviceEventDetails`: Zeigt das Authentifizierungsergebnis an (Erfolg).

Beispiel für einen Protokolleintrag für ListCallerAccessGrants

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für ein ListCallerAccessGrants Ereignis, das auftritt, wenn die Transfer Family Family-Web-App verfügbare Zugriffsberechtigungen für einen Benutzer abfragt.

```

{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROEXAMPLEID:aws-transfer",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
        "accountId": "123456789012",
        "accessKeyId": "ASIAEXAMPLEKEY",

```

```

    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
        "accountId": "123456789012",
        "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
      },
      "attributes": {
        "creationDate": "2025-08-08T15:29:34Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
    },
    "eventTime": "2025-08-08T15:29:35Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "ListCallerAccessGrants",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
      "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
      "allowedByApplication": "true",
      "maxResults": "100"
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "CipherSuite": "TLS_AES_128_GCM_SHA256",
      "bytesTransferredIn": 0,
      "AuthenticationMethod": "AuthHeader",
      "x-amz-id-2": "1g34AaAELn/
fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
      "bytesTransferredOut": 462
    },
    "requestID": "48485MTZEDWT0ANT",
    "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",

```



```
"readOnly": true,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS:S3::AccessGrantsInstance",
    "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
  }
],
"eventType": "AWS ApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

Beachten Sie in diesem Beispiel die folgenden wichtigen Felder:

- `eventName`: Zeigt, dass es sich um ein `ListCallerAccessGrants` Ereignis handelt, das verfügbare S3-Zugriffsberechtigungen abfragt.
- `requestParameters.allowedByApplication`: Zeigt an, dass die Abfrage nach den von der Anwendung zugelassenen Berechtigungen gefiltert wurde.
- `requestParameters.maxResults`: Zeigt die maximale Anzahl von Zuschüssen an, die in der Antwort zurückgegeben werden können.
- `userIdentity.onBehalfOf`: Verknüpft die Anfrage mit dem spezifischen Web-App-Benutzer.

Dieses Ereignis hilft dabei, nachzuverfolgen, wann die Transfer Family Family-Web-App abfragt, auf welche S3-Ressourcen ein Benutzer Zugriff hat, und bietet so Einblick in die Vorgänge zur Ermittlung von Zugriffsberechtigungen.

Beispiel für einen Protokolleintrag für ein `GetDataAccess` Ereignis

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für ein `GetDataAccess` Ereignis, das auftritt, wenn die Transfer Family Family-Web-App im Namen eines Benutzers Zugriffsberechtigungen für S3-Ressourcen anfordert.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
```

```

    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },
      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
      "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
    }
  },
  "eventTime": "2025-05-08T16:10:25Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetDataAccess",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
  },
  "responseElements": null,
  "additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2244,

```

```

    "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNC0RFWlTYNE7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
  },
  "requestID": "BXGSKKQXCWS5RAHB",
  "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS:S3::AccessGrantsInstance",
      "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
      "accountId": "123456789012"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}

```

Beachten Sie in diesem Beispiel die folgenden wichtigen Felder:

- `eventName`: Zeigt, dass dies ein `GetDataAccess` Ereignis ist, das auftritt, wenn Transfer Family Zugriffsberechtigungen für S3-Ressourcen anfordert.
- `userIdentity.onBehalfOf`: Enthält den ARN und die Benutzer-ID des Identitätsspeichers und verknüpft die Zugriffsanforderung mit dem spezifischen Web-App-Benutzer.
- `requestParameters.target`: Zeigt das S3-Pfadmuster an, für das der Zugriff angefordert wurde.
- `requestParameters.permission`: Gibt die Art des angeforderten Zugriffs an (READWRITE, READ oder WRITE).
- `requestParameters.durationSeconds`: Zeigt an, wie lange die Zugriffsgewährung gültig ist (normalerweise 900 seconds/15 Minuten).
- `sourceIPAddress` und `userAgent`: Beide zeigen „transfer.amazonaws.com“ an, was darauf hinweist, dass es sich um eine interne Serviceanfrage handelt.

`GetDataAccess` Ereignisse sind besonders nützlich, um nachzuverfolgen, wann Benutzern der Transfer Family Family-Web-App Zugriff auf bestimmte S3-Ressourcen gewährt wird. So können Sie die Zugriffsmuster überwachen und die ordnungsgemäße Autorisierung sicherstellen.

CloudTrail Protokolleinträge anzeigen

Es gibt verschiedene Möglichkeiten, CloudTrail Protokolleinträge für Ihre Transfer Family Family-Web-App anzuzeigen und zu analysieren:

Verwenden der CloudTrail Konsole

Die CloudTrail Konsole bietet eine benutzerfreundliche Oberfläche zum Anzeigen und Filtern von Protokolleinträgen:

1. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Ereignisverlauf aus.
3. Verwenden Sie die Filteroptionen, um die Ereignisse einzugrenzen:
 - Stellen Sie Eventquelle auf `transfer.amazonaws.com`, um nur Transfer Family Family-Ereignisse anzuzeigen.
 - Filtern Sie nach dem Namen des Ereignisses, um bestimmte Operationen wie `anzeigenUserAuthentication`.
 - Verwenden Sie den Zeitraum, um sich auf Ereignisse innerhalb eines bestimmten Zeitraums zu konzentrieren.
4. Klicken Sie auf ein Ereignis, um detaillierte Informationen zu erhalten.

Zugreifen auf Protokolle in Amazon S3

Wenn Sie einen CloudTrail Trail für die Übermittlung von Protokollen an einen Amazon S3 S3-Bucket konfiguriert haben, können Sie direkt auf die Rohprotokolldateien zugreifen:

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Navigieren Sie zu dem Bucket und dem Präfix, in dem Ihre CloudTrail Logs gespeichert sind.
3. Die Protokolle sind nach Jahr, Monat, Tag und Region geordnet. Navigieren Sie zum entsprechenden Verzeichnis.
4. Laden Sie die Protokolldateien im JSON-Format herunter und öffnen Sie sie.

Fehlerbehebung bei Ihren Web-Apps

Note

Diese Tipps zur Fehlerbehebung richten sich eher an den Administrator der Web-App als an den Endbenutzer. Wenn Endbenutzer auf Probleme stoßen, wenden Sie sich an Ihren Web-App-Administrator. Alle Fälle von Ihnen in den folgenden Abschnitten beziehen sich auf den Web-App-Administrator.

Beheben Sie Netzwerkfehler

Beschreibung

Ihrem Endbenutzer wird beim Laden des Web-App-Endpunkts ein Netzwerkbanner Netzwerkfehler angezeigt.

Ursache

Die häufigsten Probleme lauten wie folgt:

- Der Administrator hat dem Benutzer, der versucht, sich bei der neuen Anwendung anzumelden, nicht zugewiesen.
- Der Administrator hat Ihren IAM-Rollen nicht die erforderlichen Aktionen hinzugefügt.
- Sie sehen eine Liste von S3 Access Grants, die Ihrem Benutzer zugewiesen wurden, aber CORS ist für Ihren Amazon S3-Bucket oder Ihre Amazon S3-Buckets nicht richtig konfiguriert.

Lösung

- Stellen Sie im IAM Identity Center sicher, dass Sie den Benutzer der richtigen Anwendung zuweisen. Oder, falls Ihnen eine Gruppe zugewiesen wurde, stellen Sie sicher, dass der Benutzer, der versucht, sich anzumelden, zur richtigen Gruppe gehört. Dieser Vorgang wird unter [Weisen Sie einer Transfer Family Family-Web-App Benutzer oder Gruppen zu oder fügen Sie sie hinzu](#) beschrieben.
- Prüfen Sie, ob Ihre Rollen die erforderlichen Aktionen in der benutzerdefinierten Vertrauensrichtlinie für beide `sts:AssumeRole` `sts:SetContext` Aktionen enthalten. Dieser Vorgang wird unter [Konfiguration von IAM-Rollen für Transfer Family Family-Web-Apps](#) beschrieben.

- Überprüfen Sie die CORS-Richtlinie für alle Buckets, die von Ihrer Web-App verwendet werden. Dies wird unter [Cross-origin Resource Sharing \(CORS\) für Ihren Amazon S3 S3-Bucket einrichten](#) beschrieben.

Fehlerbehebung: Der konfigurierte Bucket wird nicht angezeigt

Beschreibung

Alles scheint korrekt konfiguriert zu sein, aber der Amazon S3 S3-Bucket erscheint nicht in der Web-App.

Ursache

Eine mögliche Ursache ist, dass sich der Amazon S3 S3-Bucket nicht im selben Konto wie die Web-App befindet.

Lösung

Stellen Sie sicher, dass sich der Amazon S3 S3-Bucket im selben Konto wie die Web-App befindet. Cross-account Buckets werden derzeit nicht unterstützt.

Beheben Sie Fehler mit benutzerdefinierten URLs

Beschreibung

Wenn sich Ihr Endbenutzer bei der Web-App anmeldet, erhält er die Fehlermeldung Authorization failed: missing authorization code.

Ursache

Wenn Sie die Vorlage CloudFront direkt und nicht die mitgelieferte CloudFormation Vorlage verwendet haben, haben Sie wahrscheinlich die ursprüngliche Anforderungsrichtlinie falsch konfiguriert, sodass Abfragezeichenfolgen nicht weitergeleitet werden.

Lösung

Aktualisieren Sie Ihre Quellenforderungsrichtlinie, um Abfragezeichenfolgen und Cookies an den Ursprung weiterzuleiten.

Beschreibung

Wenn Ihr Endbenutzer versucht, auf eine Transfer Family Family-Web-App zuzugreifen, erhält er eine 404-Antwort.

Ursache

Wenn Sie die Vorlage CloudFront direkt und nicht die bereitgestellte CloudFormation Vorlage verwendet haben, haben Sie wahrscheinlich die Cache-Richtlinie falsch konfiguriert, um den Host Header in den Cache-Schlüssel aufzunehmen, oder die ursprüngliche Anforderungsrichtlinie falsch konfiguriert, um den Header weiterzuleiten. Host

Lösung

- Stellen Sie sicher, dass Ihre Cache-Richtlinie den Host Header nicht in den Cache-Schlüssel einbezieht
- Stellen Sie sicher, dass Ihre Origin-Anforderungsrichtlinie den Host Header nicht weiterleitet.

Beheben Sie verschiedene Fehler

Beschreibung

Ihr Endbenutzer kann sich nicht anmelden oder keine Buckets oder Dateien anzeigen, oder Sie erhalten eine weitere Fehlermeldung.

Ursache

Eine mögliche Ursache ist, dass der ARN der IAM Identity Center-Instanz nicht mit dem Wert für Ihren Grants-ARN oder den ARN Ihrer Web-App-IAM Identity Center-Instanz übereinstimmt.

Lösung

Überprüfen Sie die folgenden Punkte, um festzustellen, ob sie übereinstimmen.

- Navigieren Sie im IAM Identity Center zu Einstellungen und sehen Sie sich den Instanz-ARN an.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- Navigieren Sie in Amazon S3 zu Access Grants und sehen Sie sich Ihren IAM Identity Center-Instance-ARN an.

```
arn:aws:sso::account-id:application/ssoins-instance-identifier/ap1-1234567890abcdef0
```

- Navigieren Sie in Transfer Family zur Detailseite Ihrer Web-App und sehen Sie sich deren Instanz-ARN an.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

Der *instance-identifier* Wert muss an allen drei Stellen derselbe sein.

Doppelte S3-Buckets werden in der Web-App angezeigt

Beschreibung

Benutzern wird derselbe S3-Bucket in der Transfer Family Family-Web-App-Oberfläche mehrfach aufgeführt.

Ursache

Dies ist der Fall, wenn ein Benutzer Teil mehrerer Active Directory-Gruppen ist, die über doppelte Berechtigungen für denselben S3-Bucket verfügen. Die Web-App listet alle Zuweisungen auf oberster Ebene auf, die dem Benutzer zugeordnet sind (UID oder GID), unabhängig davon, ob dem Benutzer mehrere Grants demselben Bucket-Standort zugewiesen sind.

Lösung

Um dieses Problem zu beheben, sollten Administratoren die Zuweisungen deduplizieren, sodass jedem Benutzer nur ein Grant für jeden S3-Standort zur Verfügung steht. Überprüfen Sie Ihre Konfiguration für S3 Access Grants und konsolidieren Sie doppelte Zuweisungen für denselben Bucket in verschiedenen Active Directory-Gruppen.

Anweisungen für Endbenutzer für Transfer Family Family-Web-Apps

Note

In diesem Thema richten sich die Informationen an die Endbenutzer, die mit der Web-App interagieren. Alle Beispiele von Ihnen in diesem Thema beziehen sich auf Endbenutzer.

In diesem Thema wird beschrieben, wie Sie auf eine AWS Transfer Family Web-App zugreifen, zu deren Nutzung Sie berechtigt sind, und wie Sie mit ihr interagieren können.

Kontingente für Web-Apps

Beachten Sie die folgenden Einschränkungen bei der Verwendung von Web-Apps.

- Maximale Anzahl von Suchergebnissen pro Abfrage: 10.000
- Die Amazon S3 S3-Buckets, die von der Transfer Family Family-Web-App verwendet werden, müssen sich auf demselben Konto wie die Web-App selbst befinden. Cross-account Buckets werden derzeit nicht unterstützt.
- Maximale Suchbreite pro Abfrage: 10.000 durchsuchte Dateien
- Maximale Upload-Größe pro Datei: 160 GB (149 GiB)
- Maximale Größe der Datei zum Kopieren: 5,36 GB (5 GiB)
- Ordernamen, die mit Punkten (.) beginnen oder enden, werden nicht unterstützt

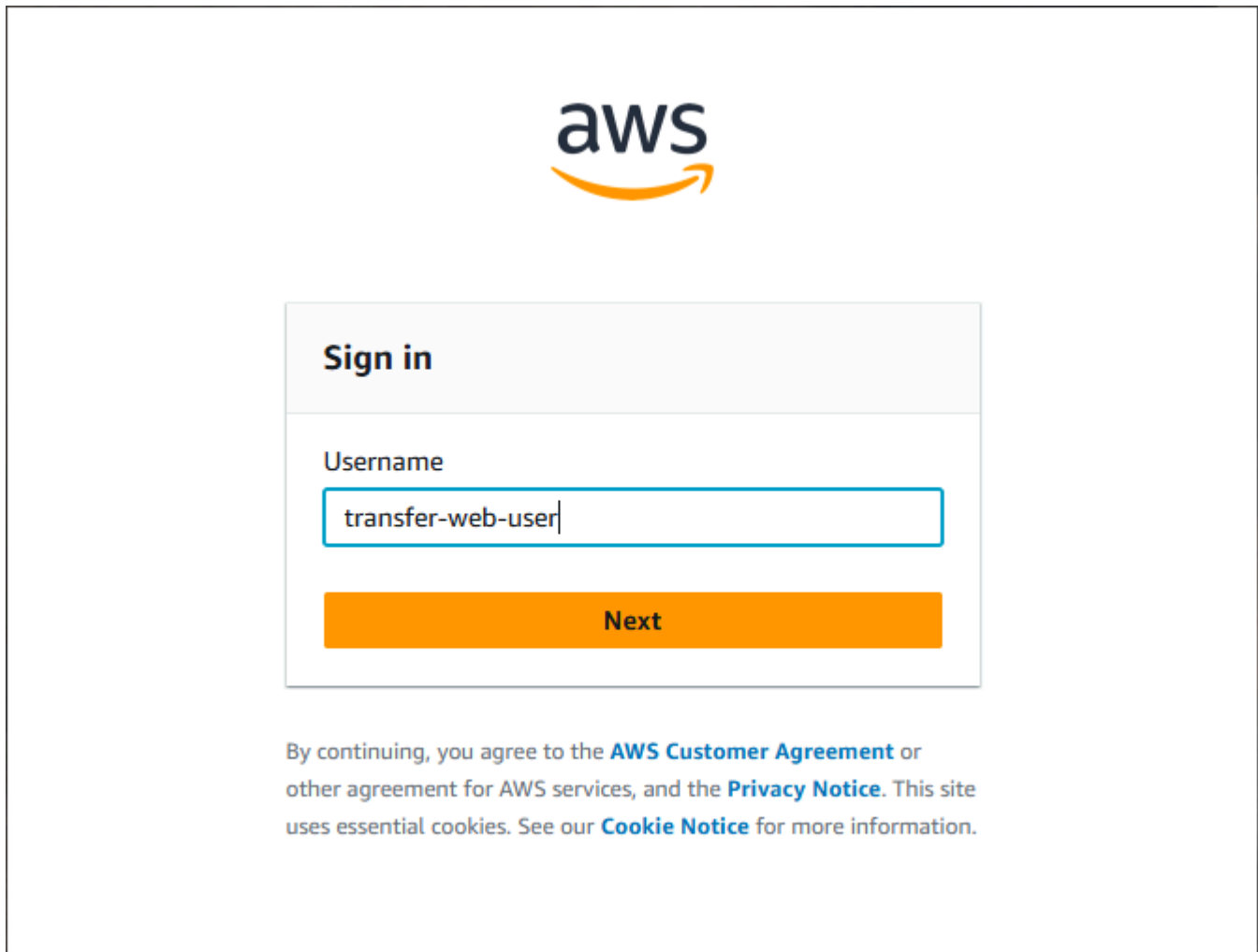
Benutzererfahrung für IAM Identity Center-Benutzer

In diesem Abschnitt wird die Benutzererfahrung beschrieben, wenn Ihr Unternehmen IAM Identity Center zur Konfiguration seiner Benutzer verwendet hat.

So greifen Sie auf eine Transfer Family Family-Web-App zu

1. Sie sollten von no-reply@login.awsapps.com eine E-Mail mit dem Titel „Einladung zum Beitritt“ erhalten AWS IAM Identity Center. Nehmen Sie die Einladung zur Aktivierung Ihres Benutzerkontos an.
2. Wählen Sie in der Nachricht die URL unter Ihrer AWS Zugangs-Portal-URL aus.

Dadurch gelangen Sie zum AWS Anmeldebildschirm.



aws

Sign in

Username

transfer-web-user

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

3. Geben Sie Ihre Anmeldedaten ein und wählen Sie Anmelden.

Dadurch gelangen Sie zu der AWS-Zugangsportale, in der eine Liste Ihrer verfügbaren Anwendungen angezeigt wird.

4. Wählen Sie die Anwendung für Ihre Transfer Family Family-Web-App.

Benutzererfahrung für Benutzer von Identitätsanbietern von Drittanbietern

Wenn Ihre Organisation ihre Benutzer nicht AWS IAM Identity Center zur Konfiguration verwendet hat, hängt Ihr Onboarding-Erlebnis von der Identity Provider-Anwendung ab, mit der sie ihre Endbenutzer konfiguriert haben. Nachdem Sie sich authentifiziert und angemeldet haben, entspricht Ihre Web-App-Oberfläche der im nächsten Abschnitt beschriebenen.

 Note

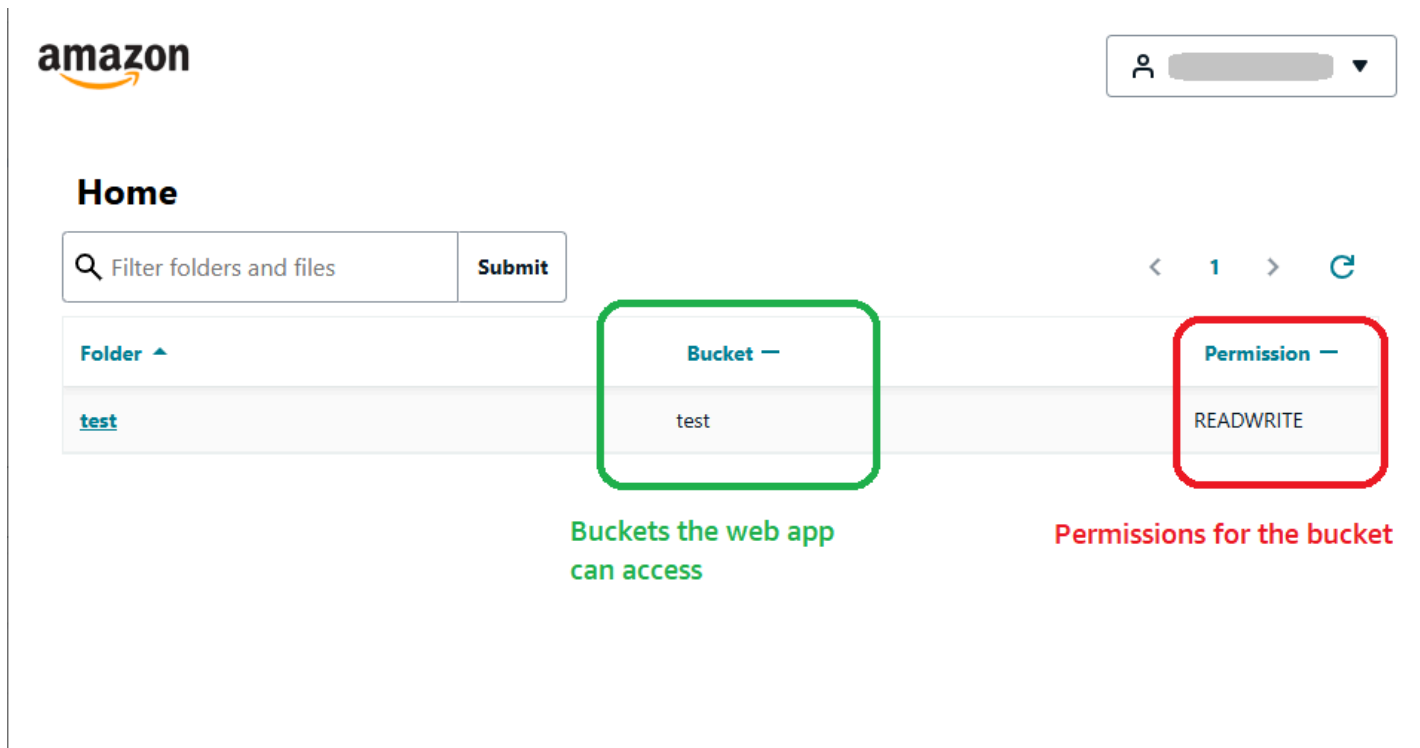
Wenn ein Benutzer mehreren Active Directory-Gruppen angehört, die Berechtigungen für denselben Amazon S3 S3-Bucket haben, wird der Bucket mehrfach in der Web-App-Oberfläche angezeigt. Dies liegt daran, dass die Web-App alle Grants auf oberster Ebene auflistet, die mit der UID oder GID des Benutzers verknüpft sind, einschließlich doppelter Zuschüsse für denselben Bucket. Um doppelte Angebote zu vermeiden, können Administratoren mehrere Zuschüsse zusammenfassen, sodass jeder Benutzer nur über einen Zuschuss pro Amazon S3 S3-Standort verfügt.

Endbenutzeroberfläche von Transfer Family

Nachdem Sie sich authentifiziert und angemeldet haben, können Sie mit der Web-App interagieren.

Es gibt vier Hauptansichten.

- **Startseite:** Auf Ihrer Startseite sind die S3-Standorte, auf die Sie zugreifen können, sowie die jeweiligen Berechtigungen aufgeführt. Ein S3-Standort ist ein S3-Bucket oder -Präfix, den Sie definieren können, wenn Sie S3 Access Grants verwenden. Dies ist die erste Ansicht für Benutzer, in der die S3-Ressourcen auf Root-Ebene, auf die Ihre Endbenutzer Zugriff haben, sowie die Berechtigungen für jeden S3-Standort angezeigt werden.



- Standortdetails: In dieser Ansicht können Benutzer Dateien und Ordner in S3 durchsuchen und Dateien hoch- oder herunterladen.
- Standortaktion: Nachdem Sie eine Aktion (z. B. Hochladen) ausgewählt haben, wird eine weitere Ansicht des Dateispeicherorts geöffnet.
- Vertikale Ellipse: Das vertikale Ellipsensymbol öffnet das Aktionsmenü.

Verfügbare Aktionen

Die meisten Aktionen sind im Aktionsmenü verfügbar. Für die andere Hauptaktion, das Herunterladen von Dateien, verwenden Sie das Download-Symbol, nachdem Sie eine Datei ausgewählt haben (derzeit können Sie jeweils nur eine Datei herunterladen).

Transfer Web App

Scott

Home / test2 / Testing-01

Testing-01/

Submit ☐ Include subfolders < 1 > ↺ ⋮

☐	Name ▲	Type —	Last Modified —	Size —	
☐	scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	
☐	Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	
☐	Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	

Download icon

Verwenden Sie in einem Ordner das Aktionsmenü, um eine der folgenden Aufgaben auszuführen:

- Kopieren Sie eine oder mehrere Dateien an einen anderen Speicherort.
- Erstellen Sie einen Ordner.
- Löschen Sie eine oder mehrere Dateien.
- Laden Sie eine oder mehrere Dateien hoch.
- Laden Sie einen ganzen Ordner hoch (einschließlich Unterordnern, falls vorhanden).
- Wählen Sie einen Ordner aus und navigieren Sie zu ihm. Sie können dann jede der zuvor aufgelisteten Aktionen ausführen.
- Nach Seite sortieren.
- Filtern Sie nach Datei- oder Ordnernamen pro Ordner und Unterordnern.

amazon

Home / test

test

🔍 Search current folder

Submit

☐ Include subfolders

< 1 > ↺ ⋮

📄 Copy files

📁 Create folder

🗑 Delete files

📁 Upload files

📁 Upload folder

Name ▲	Type —	Last Modified —
📁 My First Folder/	Folder	
📁 My Second Folder/	Folder	
📁 Testing-01/	Folder	
📁 Testing-02/	Folder	

AWS Transfer Family SFTP-Anschlüsse

Ein AWS Transfer Family SFTP-Connector stellt mithilfe des SFTP-Protokolls eine Verbindung mit einem Remote-SFTP-Server her, um Dateien zwischen Amazon-Speicher und einem Remote-Server zu übertragen. Sie können Dateien von Amazon S3 an einen externen, partnereigenen SFTP-Server senden, Dateien vom SFTP-Server eines Partners auf Amazon S3 abrufen oder Dateien auf dem Remote-Server auflisten, löschen, umbenennen oder verschieben. SFTP-Konnektoren unterstützen zwei Ausgangstypen: Service Managed (mit AWS verwalteter Infrastruktur) und VPC (Routing durch Ihre VPC mit Amazon VPC Lattice). Mithilfe von SFTP-Konnektoren können Sie automatisierte, ereignisgesteuerte Workflows für die Dateiübertragung in erstellen. AWS

Unter [AWS Transfer Family SFTP-Konnektoren finden](#) Sie eine kurze Einführung in die SFTP-Konnektoren der Transfer Family.

Themen

- [SFTP-Konnektoren erstellen](#)
- [VPC-Konnektivität für SFTP-Anschlüsse](#)
- [Verwenden von SFTP-Anschlüssen](#)
- [Überwachung von SFTP-Anschlüssen](#)
- [Verwaltung von SFTP-Konnektoren](#)
- [Skalierung und Kontingente für SFTP-Konnektoren](#)
- [Referenzarchitekturen, die SFTP-Konnektoren verwenden](#)

SFTP-Konnektoren erstellen

In diesem Thema wird beschrieben, wie SFTP-Konnektoren erstellt werden. Jeder Connector bietet die Möglichkeit, eine Verbindung mit einem Remote-SFTP-Server herzustellen. Sie führen die folgenden allgemeinen Aufgaben aus, um einen SFTP-Connector zu konfigurieren.

Note

Informationen zu VPC-based Connectoren, die den Datenverkehr durch Ihre Virtual Private Cloud weiterleiten, finden Sie unter [Erstellen Sie einen SFTP-Connector mit Egress VPC-based](#).

1. Speichern Sie die Authentifizierungsdaten für den Connector in AWS Secrets Manager.
2. Erstellen Sie den Connector, indem Sie den geheimen ARN, die URL oder den ARN für die Ressourcenkonfiguration des Remoteservers, die Sicherheitsrichtlinie mit den Algorithmen, die vom Connector unterstützt werden, und andere Konfigurationseinstellungen angeben.
3. Nachdem Sie den Connector erstellt haben, können Sie ihn testen, um sicherzustellen, dass er Verbindungen mit dem Remote-SFTP-Server herstellen kann.

Wählen Sie den Ausgangstyp des SFTP-Connectors

Wenn Sie einen SFTP-Connector erstellen, wählen Sie den Ausgangstyp zwischen „Service managed“ und „VPC Lattice“.

- **Service managed (Standard):** Der Connector verwendet NAT-Gateways und IP-Adressen, die Eigentum von sind, AWS Transfer Family um Verbindungen über das öffentliche Internet weiterzuleiten. Der Dienst stellt 3 statische IP-Adressen für Ihre Connectoren bereit, die auf den Remoteservern auf die Zulassungsliste gesetzt werden müssen, um Verbindungen herzustellen.
- **VPC Lattice:** Der Connector leitet den Datenverkehr mithilfe von Amazon VPC Lattice durch Ihre VPC-Umgebung. Verwenden Sie VPC-Konnektivität für SFTP-Connectors in diesen Szenarien:
 - **Private SFTP-Server:** Connect zu SFTP-Servern her, auf die nur von Ihrer VPC aus zugegriffen werden kann
 - **On-premises Konnektivität:** Stellen Sie über Oder-Verbindungen eine Verbindung zu lokalen SFTP-Servern her AWS Direct Connect AWS Virtual Private Network
 - **Benutzerdefinierte IP-Adressen:** Präsentieren Sie dem Remote-Server Ihre eigenen NAT-Gateways und Elastic IP-Adressen
 - **Zentralisierte Sicherheitskontrollen:** Leiten Sie Dateiübertragungen über die zentralen Kontrollen Ihres Unternehmens weiter ingress/egress

Die folgende Matrix hilft Ihnen bei der Auswahl des richtigen Steckertyps für Ihre Anwendungsfälle.

Matrix für den Ausgangstyp des SFTP-Anschlusses

Funktion	Ausgangstyp = Verwalteter Dienst	Ausgangstyp = VPC-Gitter
Konnektivität zu öffentlich gehosteten (über das Internet zugänglichen) SFTP-Servern	Unterstützt	Unterstützt 1
Konnektivität zu privat gehosteten (lokalen) SFTP-Servern	Nicht unterstützt	Unterstützt 2
Konnektivität zu privat gehosteten (In-VPC) SFTP-Servern	Nicht unterstützt	Unterstützt
Statische IP-Adressen, die dem Remote-SFTP-Server präsentiert werden	Wird über vom Dienst bereitgestellte statische IP-Adressen unterstützt	Wird über statische IP-Adressen unterstützt, die sich im Besitz des Kunden befinden
Verfügbare Bandbreite	50 MBIT/S pro Konto	Höhere Bandbreite, je nach Verfügbarkeit über Resource Gateway und NAT Gateway im Kundenbesitz
Weiterleitung des Datenverkehrs zum Internet über kundeneigene NAT-Gateways und Netzwerk-Firewalls	Nicht unterstützt NAT-Gateways gehören dem Transfer Family Service und werden von diesem verwaltet.	Unterstützt

¹ Mit Egress Type = VPC Lattice wird die Konnektivität zu öffentlich gehosteten Servern mithilfe der Egress-Infrastruktur (NAT-Gateways) in Ihren Ausgangs-VPCs unterstützt.

² Mit Egress Type = VPC Lattice wird die Konnektivität zu privat gehosteten Servern unter Verwendung vorhandener Netzwerke in Ihrer VPC unterstützt, z. B. VPN. AWS Direct Connect

Wählen Sie den IP-Adressierungsmodus

Wenn Sie einen SFTP-Connector mit serviceverwaltetem Ausgang erstellen, können Sie zwischen zwei IP-Adressierungsmodi wählen:

- **Nur IPv4 (Standard):** Der Connector verwendet ausschließlich IPv4-Adressen, um eine Verbindung zum Remote-SFTP-Server herzustellen. Dies ist der Standardmodus beim Erstellen von Connectoren über die Konsole, AWS CLI oder API.
- **Dual-stack:** Der Connector unterstützt sowohl IPv6- als auch IPv4-Adressen. Im Dual-Stack-Modus bevorzugt der Connector IPv6, wenn die DNS-Auflösung IPv6-Ergebnisse zurückgibt, und verwendet IPv4, wenn nur IPv4-DNS-Ergebnisse zurückgegeben werden.

Note

Der IP-Adressierungsmodus gilt nur für Connectors mit vom Dienst verwaltetem Ausgangstyp. Connectoren, die VPC Lattice Egress verwenden, unterstützen diese Einstellung nicht.

Themen

- [Speichern Sie Authentifizierungsdaten für SFTP-Konnektoren in Secrets Manager](#)
- [Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang](#)
- [Erstellen Sie einen SFTP-Connector mit Egress VPC-based](#)
- [Testen Sie einen SFTP-Connector](#)

Speichern Sie Authentifizierungsdaten für SFTP-Konnektoren in Secrets Manager

Sie können Secrets Manager verwenden, um Benutzeranmeldeinformationen für Ihre SFTP-Konnektoren zu speichern. Wenn Sie Ihr Geheimnis erstellen, müssen Sie einen Benutzernamen angeben. Darüber hinaus können Sie entweder ein Passwort, einen privaten Schlüssel oder beides angeben. Details hierzu finden Sie unter [Kontingente für SFTP-Anschlüsse](#).

 Note

Wenn Sie Geheimnisse im Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu den Preisen erhalten Sie unter [AWS Secrets Manager Preise](#).

Um Benutzeranmeldeinformationen in Secrets Manager für einen SFTP-Connector zu speichern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Secrets Manager Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie im linken Navigationsbereich Secrets aus.
3. Wählen Sie auf der Seite Secrets die Option Neues Geheimnis speichern aus.
4. Wählen Sie auf der Seite Geheimtyp auswählen für Geheimtyp die Option Anderer Geheimtyp aus.
5. Geben Sie die key/value Informationen für Ihr Geheimnis ein: Sie müssen den Benutzernamen und entweder einen privaten Schlüssel oder ein Passwort angeben.
 - a. Wählen Sie im Bereich Key/value Paare die Key/valueRegisterkarte aus.
 - Schlüssel — Enter**Username**.
 - Wert — Geben Sie den Namen des Benutzers ein, der berechtigt ist, eine Verbindung zum Server des Partners herzustellen.
 - b. Wenn Sie ein key pair angeben möchten, wählen Sie Zeile hinzufügen und wählen Sie im Abschnitt Key/value Paare die Key/valueRegisterkarte aus.
 - Schlüssel — Geben Sie ein**PrivateKey**.
 - Wert — fügen Sie Ihren privaten Schlüssel ein.

Tipp: Die von Ihnen eingegebenen privaten Schlüsseldaten müssen dem öffentlichen Schlüssel entsprechen, der für diesen Benutzer auf dem Remote-SFTP-Server gespeichert ist.

 Note

Es ist nicht möglich, einen passwortgeschützten privaten Schlüssel für die Authentifizierung mit einem SFTP-Connector zu verwenden. AWS Transfer Family

Einzelheiten zum Generieren eines public/private key pair finden Sie unter [SSH-Schlüssel auf macOS, Linux oder Unix erstellen](#).

- c. Wenn Sie ein Passwort angeben möchten, wählen Sie Zeile hinzufügen und wählen Sie im Abschnitt Key/value Paare die Key/value Registerkarte aus.
 - Schlüssel — Geben Sie ein **Password**.
 - Wert — Geben Sie das Passwort für den Benutzer ein.
6. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite Geheim konfigurieren einen Namen und eine Beschreibung für Ihr Geheimnis ein. Wir empfehlen, dass Sie **aws/transfer/** für den Namen das Präfix von verwenden. Sie könnten beispielsweise Ihr Geheimnis benennen **aws/transfer/connector-1**.
8. Wählen Sie Weiter und akzeptieren Sie dann die Standardeinstellungen auf der Seite Rotation konfigurieren. Klicken Sie anschließend auf Weiter.
9. Wählen Sie auf der Seite „Überprüfen“ die Option Speichern aus, um das Geheimnis zu erstellen und zu speichern.

Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang

In diesem Verfahren wird erklärt, wie Sie SFTP-Konnektoren mithilfe der AWS Transfer Family Konsole oder erstellen. AWS CLI

Console

Um einen SFTP-Connector zu erstellen

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich SFTP-Connectors und anschließend Create SFTP-Connector aus.
3. Wählen Sie im Abschnitt Connector-Konfiguration für Egress type die Option Service managed aus. Diese Option verwendet eine AWS Transfer Family verwaltete Ausgangsinfrastruktur. Der Transfer Family Family-Dienst stellt statische IP-Adressen für jeden SFTP-Connector bereit und verwaltet sie.

4. Geben Sie im Abschnitt Connector-Konfiguration die folgenden Informationen an:

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

- Geben Sie für die URL die URL für einen Remote-SFTP-Server ein. Diese URL muss beispielsweise als `sftp://partner-SFTP-server-url` formatiert sein. `sftp://AnyCompany.com`

Note

Optional können Sie in Ihrer URL eine Portnummer angeben. Das Format ist `sftp://partner-SFTP-server-url:port-number`. Die Standard-Portnummer (wenn kein Port angegeben ist) ist Port 22.

- Wählen Sie für die Access-Rolle den Amazon-Ressourcennamen (ARN) der zu verwendenden AWS Identity and Access Management (IAM) -Rolle aus.
 - Stellen Sie sicher, dass diese Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis des Dateispeicherorts bietet, der in der StartFileTransfer Anfrage verwendet wird.
 - Stellen Sie sicher, dass diese Rolle die Berechtigung **secretsmanager:GetSecretValue** zum Zugriff auf den geheimen Schlüssel gewährt.

Note

In der Richtlinie müssen Sie den ARN für das Geheimnis angeben. Der ARN enthält den geheimen Namen, fügt dem Namen jedoch sechs zufällige

alphanumerische Zeichen hinzu. Ein ARN für ein Geheimnis hat das folgende Format.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Stellen Sie sicher, dass diese Rolle eine Vertrauensstellung enthält, die es dem Connector ermöglicht, auf Ihre Ressourcen zuzugreifen, wenn er Übertragungsanfragen Ihrer Benutzer bearbeitet. Einzelheiten zum Aufbau einer Vertrauensbeziehung finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
```

```

    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}

```

Note

Für die Zugriffsrolle gewährt das Beispiel Zugriff auf ein einzelnes Geheimnis. Sie können jedoch ein Platzhalterzeichen verwenden, was Ihnen Arbeit ersparen kann, wenn Sie dieselbe IAM-Rolle für mehrere Benutzer und Geheimnisse wiederverwenden möchten. Die folgende Ressourcenanweisung gewährt beispielsweise Berechtigungen für alle Geheimnisse, deren Namen mit beginnen. `aws/transfer`

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/*"

```

Sie können Geheimnisse, die Ihre SFTP-Anmeldeinformationen enthalten, auch in einem anderen AWS-Konto speichern. Einzelheiten zur Aktivierung des kontoübergreifenden geheimen Zugriffs finden Sie unter [Berechtigungen für AWS Secrets Manager geheime Daten für Benutzer in einem anderen Konto](#).

5. Vervollständigen Sie die Connector-Konfiguration:

- (Optional) Wählen Sie für die Logging-Rolle die IAM-Rolle aus, die der Connector verwenden soll, um Ereignisse in Ihre CloudWatch Logs zu übertragen. In der folgenden Beispielrichtlinie sind die erforderlichen Berechtigungen für die Protokollierung von Ereignissen für SFTP-Konnektoren aufgeführt.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",

```

```

    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
  }
]
}

```

6. Geben Sie im Abschnitt SFTP-Konfiguration die folgenden Informationen ein:

SFTP configuration Info

Connector credentials Info
 Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

↻
Store a new secret ↗

Trusted host keys - optional Info
 Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

ⓘ Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

Remove

Add trusted host key

Maximum concurrent connections Info
 Select the maximum number of concurrent connections that your connector can create to the remote server

- Wählen Sie für Connector-Anmeldeinformationen aus der Dropdownliste den Namen eines Geheimnisses aus, das den privaten Schlüssel AWS Secrets Manager oder das Passwort des SFTP-Benutzers enthält. Sie müssen ein Geheimnis erstellen und es auf eine bestimmte Weise speichern. Details hierzu finden Sie unter [Speichern Sie Authentifizierungsdaten für SFTP-Konnektoren in Secrets Manager](#).
- (Optional) Sie haben die Möglichkeit, Ihren Connector zu erstellen und dabei den TrustedHostKeys Parameter leer zu lassen. Ihr Connector kann jedoch keine Dateien mit dem Remoteserver übertragen, bis Sie diesen Parameter in der Konfiguration Ihres Connectors angeben. Sie können den oder die vertrauenswürdigen Hostschlüssel bei der Erstellung Ihres Connectors eingeben oder Ihren Connector später aktualisieren, indem Sie die Host-Schlüsselinformationen verwenden, die von der TestConnection

Konsolenaktion oder dem API-Befehl zurückgegeben wurden. Das heißt, für das Textfeld Vertrauenswürdige Hostschlüssel können Sie einen der folgenden Schritte ausführen:

- Geben Sie bei der Erstellung Ihres Connectors den/die Trusted Host Key (s) an. Fügen Sie den öffentlichen Teil des Hostschlüssels ein, der zur Identifizierung des externen Servers verwendet wird. Sie können mehr als einen Schlüssel hinzufügen, indem Sie Vertrauenswürdigen Hostschlüssel hinzufügen wählen, um einen zusätzlichen Schlüssel hinzuzufügen. Sie können den `ssh-keyscan` Befehl für den SFTP-Server verwenden, um den erforderlichen Schlüssel abzurufen. Einzelheiten zum Format und Typ der vertrauenswürdigen Hostschlüssel, die Transfer Family unterstützt, finden Sie unter [SFTPConnectorConfig](#).
- Lassen Sie das Textfeld Vertrauenswürdige Hostschlüssel leer, wenn Sie Ihren Connector erstellen, und aktualisieren Sie Ihren Connector zu einem späteren Zeitpunkt mit diesen Informationen. Wenn Sie zum Zeitpunkt der Erstellung Ihres Connectors nicht über die Informationen zum Hostschlüssel verfügen, können Sie diesen Parameter vorerst leer lassen und mit der Erstellung Ihres Connectors fortfahren. Nachdem der Connector erstellt wurde, verwenden Sie die ID des neuen Connectors, um den `TestConnection` Befehl entweder auf der AWS CLI oder auf der Detailseite des Connectors auszuführen. Bei Erfolg `TestConnection` werden die erforderlichen Host-Schlüsselinformationen zurückgegeben. Anschließend können Sie Ihren Connector mithilfe der Konsole (oder durch Ausführen des `UpdateConnector` AWS CLI Befehls) bearbeiten und die Hostschlüsselinformationen hinzufügen, die bei der Ausführung zurückgegeben wurden `TestConnection`.

 Important

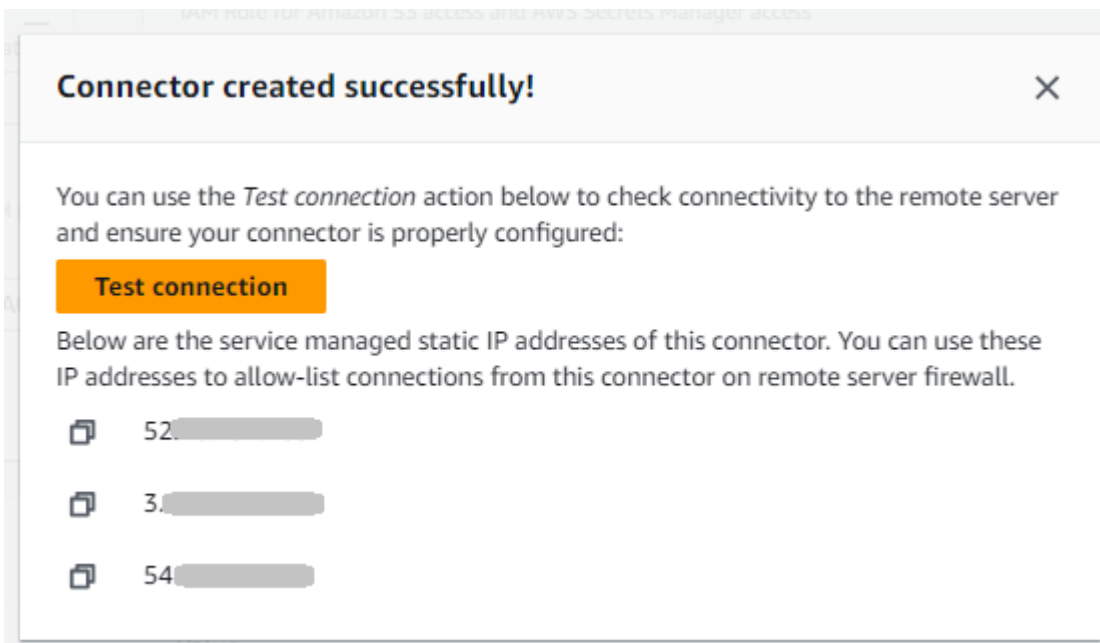
Wenn Sie den Hostschlüssel des Remoteservers durch Ausführen `abrufenTestConnection`, stellen Sie sicher, dass Sie für den zurückgegebenen Schlüssel eine Out-of-Band-Validierung durchführen.

Sie müssen den neuen Schlüssel als vertrauenswürdig akzeptieren oder den angezeigten Fingerabdruck mit einem bereits bekannten Fingerabdruck verifizieren, den Sie vom Besitzer des Remote-SFTP-Servers erhalten haben, zu dem Sie eine Verbindung herstellen.

- (Optional) Wählen Sie für Maximale Anzahl gleichzeitiger Verbindungen aus der Dropdownliste die Anzahl der gleichzeitigen Verbindungen aus, die Ihr Connector zum Remoteserver herstellt. Die Standardauswahl auf der Konsole ist 5.

Diese Einstellung gibt die Anzahl der aktiven Verbindungen an, die Ihr Connector gleichzeitig mit dem Remoteserver herstellen kann. Durch das Erstellen gleichzeitiger Verbindungen kann die Leistung des Connectors verbessert werden, indem parallel Operationen ermöglicht werden.

7. Wählen Sie im Abschnitt Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus der Dropdownliste im Feld Sicherheitsrichtlinie aus. Mit der Sicherheitsrichtlinie können Sie die kryptografischen Algorithmen auswählen, die Ihr Connector unterstützt. Einzelheiten zu den verfügbaren Sicherheitsrichtlinien und Algorithmen finden Sie unter [Sicherheitsrichtlinien für SFTP-Konnektoren AWS Transfer Family](#).
8. (Optional) Geben Sie im Abschnitt Tags für Schlüssel und Wert ein oder mehrere Tags als Schlüssel-Wert-Paare ein.
9. Nachdem Sie alle Ihre Einstellungen bestätigt haben, wählen Sie „SFTP-Connector erstellen“, um den SFTP-Connector zu erstellen. Wenn der Connector erfolgreich erstellt wurde, erscheint ein Bildschirm mit einer Liste der zugewiesenen statischen IP-Adressen und der Schaltfläche Verbindung testen. Verwenden Sie die Schaltfläche, um die Konfiguration für Ihren neuen Connector zu testen.



Die Seite Connectors wird angezeigt, auf der die ID Ihres neuen SFTP-Connectors zur Liste hinzugefügt wurde. Einzelheiten zu Ihren Konnektoren finden Sie unter [Details zum SFTP-Connector anzeigen](#).

CLI

Sie verwenden den [create-connector](#) Befehl, um einen Konnektor zu erstellen. Um mit diesem Befehl einen SFTP-Connector zu erstellen, müssen Sie die folgenden Informationen angeben.

- Die URL für einen Remote-SFTP-Server. Diese URL muss beispielsweise als `sftp://partner-SFTP-server-url` formatiert sein. `sftp://AnyCompany.com`
- Die Zugriffsrolle. Wählen Sie den Amazon-Ressourcennamen (ARN) der zu AWS Identity and Access Management verwendenden (IAM) -Rolle aus.
- Stellen Sie sicher, dass diese Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis des Dateispeicherorts bietet, der in der `StartFileTransfer` Anfrage verwendet wird.
- Stellen Sie sicher, dass diese Rolle die Berechtigung **`secretsmanager:GetSecretValue`** zum Zugriff auf den geheimen Schlüssel gewährt.

 Note

In der Richtlinie müssen Sie den ARN für das Geheimnis angeben. Der ARN enthält den geheimen Namen, fügt dem Namen jedoch sechs zufällige alphanumerische Zeichen hinzu. Ein ARN für ein Geheimnis hat das folgende Format.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Stellen Sie sicher, dass diese Rolle eine Vertrauensstellung enthält, die es dem Connector ermöglicht, auf Ihre Ressourcen zuzugreifen, wenn er Übertragungsanfragen Ihrer Benutzer bearbeitet. Einzelheiten zum Aufbau einer Vertrauensbeziehung finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
    },
  ],
}
```

```

    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ],
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
]
}

```

Note

Für die Zugriffsrolle gewährt das Beispiel Zugriff auf ein einzelnes Geheimnis. Sie können jedoch ein Platzhalterzeichen verwenden, was Ihnen Arbeit ersparen kann, wenn Sie dieselbe IAM-Rolle für mehrere Benutzer und Geheimnisse wiederverwenden möchten. Die folgende Ressourcenanweisung gewährt beispielsweise Berechtigungen für alle Geheimnisse, deren Namen mit beginnen. `aws/transfer`

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"

```

Sie können Geheimnisse, die Ihre SFTP-Anmeldeinformationen enthalten, auch in einem anderen AWS-Konto speichern. Einzelheiten zur Aktivierung des kontoübergreifenden geheimen Zugriffs finden Sie unter [Berechtigungen für AWS Secrets Manager geheime Daten für Benutzer in einem anderen](#) Konto.

- (Optional) Wählen Sie die IAM-Rolle aus, die der Connector verwenden soll, um Ereignisse in Ihre CloudWatch Logs zu übertragen. In der folgenden Beispielrichtlinie sind die erforderlichen Berechtigungen für die Protokollierung von Ereignissen für SFTP-Konnektoren aufgeführt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

- Geben Sie die folgenden SFTP-Konfigurationsinformationen an.
 - Der ARN eines Geheimnisses AWS Secrets Manager, das den privaten Schlüssel oder das Passwort des SFTP-Benutzers enthält.
 - Der öffentliche Teil des Hostschlüssels, der zur Identifizierung des externen Servers verwendet wird. Sie können mehrere vertrauenswürdige Hostschlüssel angeben, wenn Sie möchten.

Der einfachste Weg, die SFTP-Informationen bereitzustellen, besteht darin, sie in einer Datei zu speichern. Kopieren Sie beispielsweise den folgenden Beispieltext in eine Datei mit dem Namen `testSFTPConfig.json`.

```
// Listing for testSFTPConfig.json
{
```

```

    "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/
transfer/example-username-key",
    "TrustedHostKeys": [
        "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
    ]
}

```

- Geben Sie eine Sicherheitsrichtlinie für Ihren Connector an und geben Sie den Namen der Sicherheitsrichtlinie ein.

Note

Das SecretId kann entweder der gesamte ARN oder der Name des Geheimnisses (*example-username-key* in der vorherigen Liste) sein.

Führen Sie dann den folgenden Befehl aus, um den Connector zu erstellen:

```

aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5

```

Wenn Sie einen VPC-Ausgangsconnector beschreiben, enthält die Antwort die neuen Felder:

```

{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/
c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    }
  }
}

```

```
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/connector-secret"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Beachten Sie, dass dieser Wert für VPC-Ausgangs-Connectors Null `ServiceManagedEgressIpAddresses` ist, da der Datenverkehr über Ihre VPC und nicht über die verwaltete Infrastruktur geleitet wird. AWS

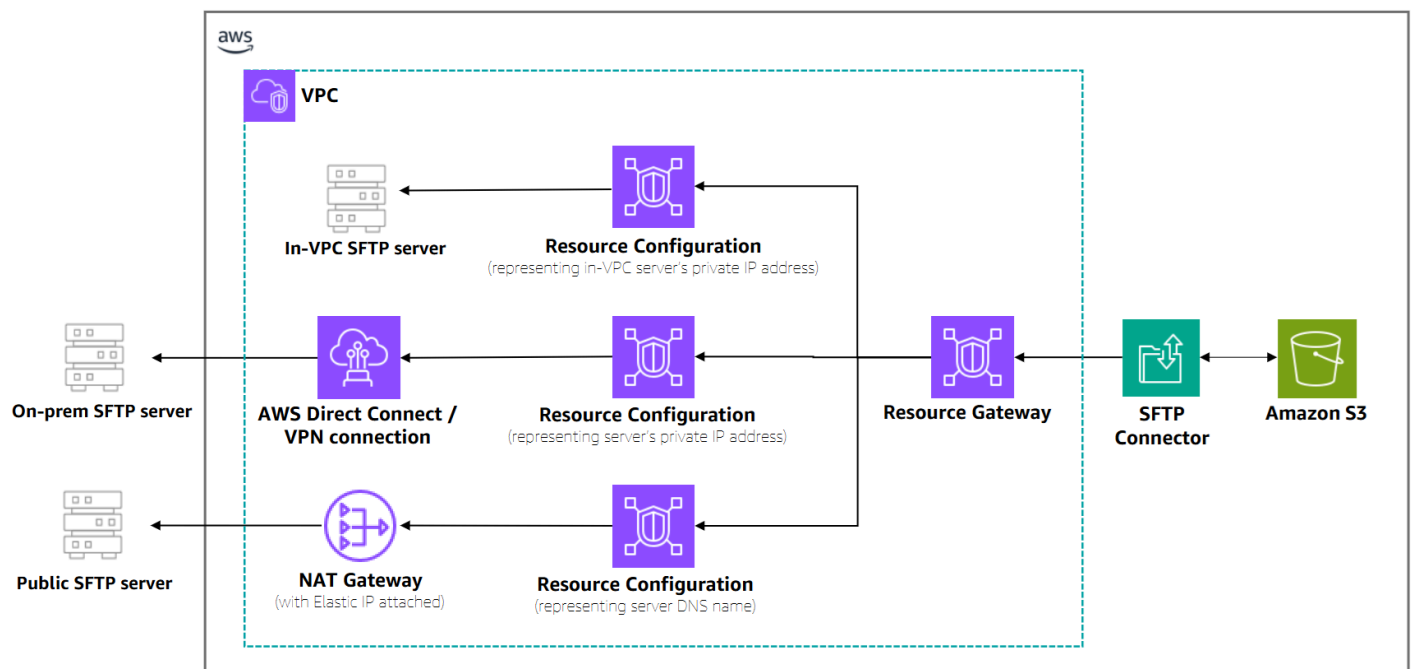
Erstellen Sie einen SFTP-Connector mit Egress VPC-based

Dieses Thema enthält schrittweise Anweisungen zum Erstellen von SFTP-Connectors mit VPC-Konnektivität. VPC_LATTICE-enabled Connectors verwenden Amazon VPC Lattice, um den Datenverkehr durch Ihre Virtual Private Cloud zu leiten und so sichere Verbindungen zu privaten Endpunkten zu ermöglichen oder Ihre eigenen NAT-Gateways für den Internetzugang zu verwenden.

Wann sollte VPC-Konnektivität verwendet werden

Verwenden Sie VPC-Konnektivität für SFTP-Connectors in diesen Szenarien:

- Private SFTP-Server: Connect zu SFTP-Servern her, auf die nur von Ihrer VPC aus zugegriffen werden kann.
- On-premises Konnektivität: Stellen Sie über AWS Direct Connect- oder AWS Site-to-Site VPN-Verbindungen Connect zu lokalen SFTP-Servern her.
- Benutzerdefinierte IP-Adressen: Verwenden Sie Ihre eigenen NAT-Gateways und Elastic IP-Adressen, einschließlich BYOIP-Szenarien.
- Zentralisierte Sicherheitskontrollen: Leiten Sie Dateiübertragungen über die zentralen Kontrollen Ihres Unternehmens weiter. ingress/egress



Voraussetzungen für VPC_-SFTP-Konnektoren LATTICE-enabled

Bevor Sie einen LATTICE-enabled VPC_-SFTP-Connector erstellen, müssen Sie die folgenden Voraussetzungen erfüllen:

Wie funktioniert Konnektivität VPC-based

Mit VPC Lattice können Sie VPC-Ressourcen sicher mit anderen Diensten teilen. AWS Transfer Family verwendet ein Servicenetzwerk, um den Prozess der gemeinsamen Nutzung von Ressourcen zu vereinfachen. Die wichtigsten Komponenten sind:

- **Resource Gateway:** Dient als Zugangspunkt zu Ihrer VPC. Sie erstellen dies in Ihrer VPC mit mindestens zwei Availability Zones.
- **Ressourcenkonfiguration:** Enthält die private IP-Adresse oder den öffentlichen DNS-Namen des SFTP-Servers, zu dem Sie eine Verbindung herstellen möchten.

Wenn Sie einen LATTICE-enabled VPC_-Connector erstellen, AWS Transfer Family verwendet er Forward Access Session (FAS), um vorübergehend Ihre Anmeldeinformationen abzurufen und Ihre Ressourcenkonfiguration mit unserem Servicenetzwerk zu verknüpfen.

Erforderliche Einrichtungsschritte

1. VPC-Infrastruktur: Stellen Sie sicher, dass Sie über eine ordnungsgemäß konfigurierte VPC mit den erforderlichen Subnetzen, Routing-Tabellen und Sicherheitsgruppen für Ihre Anforderungen an die SFTP-Serverkonnektivität verfügen.
2. Resource Gateway: Erstellen Sie mit dem Befehl `VPC create-resource-gateway` Lattice ein Resource Gateway in Ihrer VPC. Das Resource Gateway muss Subnetzen in mindestens zwei Availability Zones zugeordnet sein. Weitere Informationen finden Sie unter [Resource Gateways](#) im Amazon VPC Lattice-Benutzerhandbuch.
3. Ressourcenkonfiguration: Erstellen Sie mit dem Befehl `VPC create-resource-configuration` Lattice eine Ressourcenkonfiguration, die den Ziel-SFTP-Server darstellt. Sie können entweder angeben:
 - Eine private IP-Adresse für private Endpunkte
 - Ein öffentlicher DNS-Name für öffentliche Endpunkte (IP-Adressen werden für öffentliche Endpunkte nicht unterstützt)
4. Authentifizierungsdaten: Speichern Sie die SFTP-Benutzeranmeldedaten AWS Secrets Manager wie unter beschrieben. [Speichern Sie Authentifizierungsdaten für SFTP-Konnektoren in Secrets Manager](#)

 Important

Das Resource Gateway und die Ressourcenkonfiguration müssen im selben AWS Konto erstellt werden. Wenn Sie eine Ressourcenkonfiguration erstellen, müssen Sie zunächst über ein Resource Gateway verfügen.

Weitere Informationen zu VPC-Ressourcenkonfigurationen finden Sie unter [Ressourcenkonfigurationen](#) im Amazon VPC Lattice-Benutzerhandbuch.

 Note

VPC-Konnektivität für SFTP-Konnektoren ist dort verfügbar, AWS-Regionen wo Amazon VPC Lattice-Ressourcen verfügbar sind. Weitere Informationen finden Sie unter Häufig gestellte Fragen zu [VPC Lattice](#). Die Availability Zone-Unterstützung ist je nach Region unterschiedlich, und Resource Gateways erfordern mindestens zwei Availability Zones.

Erstellen Sie einen LATTICE-enabled VPC_-SFTP-Connector

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie mithilfe der AWS Management Console oder AWS SDKs einen SFTP-Connector mit VPC-Konnektivität erstellen. AWS CLI

Console

So erstellen Sie einen VPC_-SFTP-Connector LATTICE-enabled

1. Öffnen Sie die Konsole unter AWS Transfer Family . <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich SFTP-Connectors und anschließend Create SFTP-Connector aus.
3. Wählen Sie im Abschnitt Connector-Konfiguration für Egress type die Option VPC Lattice aus.

Diese Option leitet den Datenverkehr mithilfe von Amazon VPC Lattice für den VPC-übergreifenden Ressourcenzugriff über Ihre VPC weiter. Sie können diese Option verwenden, um eine Verbindung zu privat gehosteten Serverendpunkten herzustellen, den Datenverkehr über die Sicherheitskontrollen Ihrer VPC weiterzuleiten oder Ihre eigenen NAT-Gateways und Elastic IP-Adressen zu verwenden. Die Adresse des Remote-SFTP-Servers wird in Ihrer VPC als Ressourcenkonfiguration dargestellt. Weitere Informationen zu Ressourcenkonfigurationen finden Sie unter [Ressourcenkonfigurationen für VPC-Ressourcen](#) im Amazon VPC Lattice-Benutzerhandbuch.

4. Vervollständigen Sie die Connector-Konfiguration:
 - Wählen Sie für die Access-Rolle den Amazon-Ressourcennamen (ARN) der zu verwendenden AWS Identity and Access Management (IAM) -Rolle aus.
 - Stellen Sie sicher, dass diese Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis des Dateispeicherorts bietet, der in der StartFileTransfer Anfrage verwendet wird.
 - Stellen Sie sicher, dass diese Rolle die Berechtigung **secretsmanager:GetSecretValue** zum Zugriff auf den geheimen Schlüssel gewährt.

Note

In der Richtlinie müssen Sie den ARN für das Geheimnis angeben. Der ARN enthält den geheimen Namen, fügt dem Namen jedoch sechs zufällige

alphanumerische Zeichen hinzu. Ein ARN für ein Geheimnis hat das folgende Format.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Stellen Sie sicher, dass diese Rolle eine Vertrauensstellung enthält, die es dem Connector ermöglicht, auf Ihre Ressourcen zuzugreifen, wenn er Übertragungsanfragen Ihrer Benutzer bearbeitet. Einzelheiten zum Aufbau einer Vertrauensbeziehung finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
```

```

    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}

```

Note

Für die Zugriffsrolle gewährt das Beispiel Zugriff auf ein einzelnes Geheimnis. Sie können jedoch ein Platzhalterzeichen verwenden, was Ihnen Arbeit ersparen kann, wenn Sie dieselbe IAM-Rolle für mehrere Benutzer und Geheimnisse wiederverwenden möchten. Die folgende Ressourcenanweisung gewährt beispielsweise Berechtigungen für alle Geheimnisse, deren Namen mit beginnen. `aws/transfer`

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/*"

```

Sie können Geheimnisse, die Ihre SFTP-Anmeldeinformationen enthalten, auch in einem anderen AWS-Konto speichern. Einzelheiten zur Aktivierung des kontoübergreifenden geheimen Zugriffs finden Sie unter [Berechtigungen für AWS Secrets Manager geheime Daten für Benutzer in einem anderen](#) Konto.

- Geben Sie für Resource Configuration ARN den ARN der VPC Lattice Resource Configuration ein, der auf Ihren SFTP-Server verweist:

```

arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678

```

- (Optional) Wählen Sie für die Logging-Rolle die IAM-Rolle aus, die der Connector verwenden soll, um Ereignisse in Ihre Logs zu übertragen. CloudWatch

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
}

```

5. Geben Sie im Abschnitt SFTP-Konfiguration die folgenden Informationen ein:

- Wählen Sie für Connector-Anmeldeinformationen den Namen eines Geheimnisses AWS Secrets Manager, das den privaten Schlüssel oder das Passwort des SFTP-Benutzers enthält.
- Fügen Sie für vertrauenswürdige Hostschlüssel den öffentlichen Teil des Hostschlüssels ein, der zur Identifizierung des externen Servers verwendet wird, oder lassen Sie das Feld leer, um es später mit dem TestConnection Befehl zu konfigurieren.

Da dieser Hostschlüssel für einen VPC_LATTICE-Connector bestimmt ist, entfernen Sie den Hostnamen aus dem Schlüssel

- (Optional) Wählen Sie unter Maximale Anzahl gleichzeitiger Verbindungen die Anzahl der gleichzeitigen Verbindungen aus, die Ihr Connector zum Remoteserver herstellt (Standard ist 5).
6. Wählen Sie im Abschnitt Optionen für kryptografische Algorithmen eine Sicherheitsrichtlinie aus der Dropdownliste aus.
7. (Optional) Fügen Sie im Abschnitt „Tags“ Tags als Schlüssel-Wert-Paare hinzu.
8. Wählen Sie „SFTP-Connector erstellen“, um den LATTICE-enabled VPC_-SFTP-Connector zu erstellen.

Der Connector wird mit dem Status „PENDING“ während der Bereitstellung der Ressourcenzuordnung“ erstellt, was in der Regel mehrere Minuten dauert. Sobald sich der Status auf „ACTIVE“ ändert, ist der Connector einsatzbereit.

CLI

Verwenden Sie den folgenden Befehl, um einen LATTICE-enabled VPC_-SFTP-Connector zu erstellen:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

Der Schlüsselparameter für die VPC-Konnektivität ist `--egress-config`, der den ARN für die Ressourcenkonfiguration angibt, der Ihr SFTP-Serverziel definiert.

Überwachung des VPC-Connectorstatus

LATTICE-enabled VPC_-Konnektoren haben einen asynchronen Einrichtungsprozess. Überwachen Sie nach der Erstellung den Status des Connectors:

- **AUSSTEHEND:** Der Connector wird bereitgestellt. Die Bereitstellung des Servicenetzwerks ist im Gange, was in der Regel mehrere Minuten dauert.
- **AKTIV:** Der Connector ist einsatzbereit und kann Dateien übertragen.
- **FEHLER:** Der Connector konnte nicht bereitgestellt werden. Informationen zur Problembehandlung finden Sie in den Fehlerdetails.

Überprüfen Sie den Status des Connectors mit dem `describe-connector` folgenden Befehl:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Im Status **PENDING** gibt die `test-connection` API „Connector not available“ zurück, bis die Bereitstellung abgeschlossen ist.

Einschränkungen und Überlegungen

- **Öffentliche Endpunkte:** Wenn Sie über VPC eine Verbindung zu öffentlichen Endpunkten herstellen, müssen Sie in der Ressourcenkonfiguration einen DNS-Namen angeben. Öffentliche IP-Adressen werden nicht unterstützt.
- **Regionale Verfügbarkeit:** VPC-Konnektivität ist in ausgewählten AWS-Regionen Fällen verfügbar. Cross-region Die gemeinsame Nutzung von Ressourcen wird nicht unterstützt.
- **Anforderungen an die Availability Zone:** Resource Gateways müssen Subnetzen in mindestens zwei Availability Zones zugeordnet sein. Nicht alle Availability Zones unterstützen VPC Lattice in jeder Region.
- **Verbindungslimits:** Maximal 350 Verbindungen pro Ressource mit einem Leerlaufzeitlimit von 350 Sekunden für TCP-Verbindungen.

Kostenüberlegungen

Es fallen keine zusätzlichen Gebühren an, die über die regulären Servicegebühren AWS Transfer Family hinausgehen. Für Kunden können jedoch zusätzliche Gebühren von Amazon VPC Lattice im Zusammenhang mit der gemeinsamen Nutzung ihrer Amazon Virtual Private Cloud Cloud-Ressourcen sowie NAT-Gateway-Gebühren anfallen, wenn sie ihre eigenen NAT-Gateways für den Internetzugang verwenden.

[Vollständige AWS Transfer Family Preisinformationen finden Sie auf der Preisseite.AWS Transfer Family](#)

Beispiele für VPC-Konnektivität für SFTP-Konnektoren

Dieser Abschnitt enthält Beispiele für die Erstellung von SFTP-Connectors mit VPC-Konnektivität für verschiedene Szenarien. Bevor Sie diese Beispiele verwenden, stellen Sie sicher, dass Sie die Einrichtung der VPC-Infrastruktur abgeschlossen haben, wie in der VPC-Konnektivitätsdokumentation beschrieben.

Beispiel: Private Endpunktverbindung

Dieses Beispiel zeigt, wie Sie einen SFTP-Connector erstellen, der eine Verbindung zu einem privaten SFTP-Server herstellt, auf den nur von Ihrer VPC aus zugegriffen werden kann.

Voraussetzungen

1. Erstellen Sie ein Resource Gateway in Ihrer VPC:

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifier vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Erstellen Sie eine Ressourcenkonfiguration für Ihren privaten SFTP-Server:

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
  --port-ranges 22
```

Erstellen Sie den VPC_Connector LATTICE-enabled

1. Erstellen Sie den SFTP-Connector mit VPC-Konnektivität:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Überwachen Sie den Status des Connectors, bis er wie folgt aussieht: ACTIVE

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Der Remote-SFTP-Server erkennt Verbindungen, die von der IP-Adresse des Resource Gateways innerhalb Ihres VPC-CIDR-Bereichs kommen.

Beispiel: Öffentlicher Endpunkt über VPC

Dieses Beispiel zeigt, wie Sie Verbindungen zu einem öffentlichen SFTP-Server über Ihre VPC weiterleiten, um zentralisierte Sicherheitskontrollen zu nutzen und Ihre eigenen NAT-Gateway-IP-Adressen zu verwenden.

Voraussetzungen

1. Erstellen Sie ein Resource Gateway in Ihrer VPC (wie im Beispiel für einen privaten Endpunkt).
2. Erstellen Sie eine Ressourcenkonfiguration für den öffentlichen SFTP-Server unter Verwendung seines DNS-Namens:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Für öffentliche Endpunkte müssen Sie einen DNS-Namen verwenden, keine IP-Adresse.

Erstellen Sie den Connector

- Erstellen Sie den SFTP-Connector:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

Der Datenverkehr fließt vom Connector zu Ihrem Resource Gateway und dann über Ihr NAT-Gateway zum öffentlichen SFTP-Server. Der Remoteserver sieht die Elastic IP-Adresse Ihres NAT-Gateways als Quelle.

Beispiel: Cross-account privater Endpunkt

Dieses Beispiel zeigt, wie Sie mithilfe von Resource Sharing eine Verbindung zu einem privaten SFTP-Server in einem anderen AWS Konto herstellen.

 Note

Wenn Sie die VPC-übergreifende Ressourcenfreigabe bereits über andere Mechanismen aktiviert haben, z. B. AWS Transit Gateway, müssen Sie die hier beschriebene Ressourcenfreigabe nicht konfigurieren. Die vorhandenen Routingmechanismen, wie Transit Gateway Gateway-Routentabellen, werden automatisch von SFTP-Konnektoren verwendet. Sie müssen nur eine Ressourcenkonfiguration in demselben Konto erstellen, in dem Sie den SFTP-Connector erstellen.

Konto A (Ressourcenanbieter) — Teilen Sie die Ressourcenkonfiguration

1. Erstellen Sie das Ressourcen-Gateway und die Ressourcenkonfiguration in Konto A (wie in den vorherigen Beispielen).
2. Teilen Sie die Ressourcenkonfiguration mithilfe von AWS Resource Access Manager mit Konto B:

```
aws ram create-resource-share \  
    --name cross-account-sftp-share \  
    --resource-arns arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
    --principals 222222222222
```

Konto B (Ressourcennutzer) — Den Share akzeptieren und verwenden

1. Nehmen Sie die Einladung zur gemeinsamen Nutzung von Ressourcen an:

```
aws ram accept-resource-share-invitation \  
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-  
share-invitation/invitation-id
```

2. Erstellen Sie den SFTP-Connector in Konto B:

```
aws transfer create-connector \  
    --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \  
    --sftp-config UserSecretId=cross-account-server-  
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \  

```

```
--egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

Der Connector in Konto B kann jetzt über die gemeinsame Ressourcenkonfiguration auf den privaten SFTP-Server in Konto A zugreifen.

Allgemeine Problembehandlungsszenarien

Hier finden Sie Lösungen für häufig auftretende Probleme bei der Erstellung von LATTICE-enabled VPC_-Konnektoren:

- Der Connector bleibt im Status AUSSTEHEND hängen: Überprüfen Sie, ob Ihr Resource Gateway AKTIV ist und Subnetze in unterstützten Availability Zones hat. Wenn der Connector immer noch den Status PENDING hat, rufen Sie `UpdateConnector` ihn mit denselben Konfigurationsparametern auf, die Sie ursprünglich verwendet haben. Dadurch wird ein neues Statusereignis ausgelöst, das das Problem möglicherweise behebt.
- Verbindungstimeouts: Stellen Sie sicher, dass die Sicherheitsgruppenregeln den Verkehr auf Port 22 zulassen und dass Ihr VPC-Routing korrekt ist.
- Probleme mit der DNS-Auflösung: Stellen Sie bei öffentlichen Endpunkten sicher, dass Ihre VPC über ein NAT-Gateway oder ein Internet Gateway mit dem Internet verbunden ist.
- Cross-account Zugriff verweigert: Stellen Sie sicher, dass die Ressourcenfreigabe akzeptiert wurde und der ARN für die Ressourcenkonfiguration korrekt ist. Wenn der Ressourcenkonfiguration bei der Erstellung der Ressourcenfreigabe durch das Ursprungskonto die richtige Berechtigungsrichtlinie zugewiesen wurde, sind die folgenden Berechtigungen erforderlich: `vpc-lattice:AssociateViaAWSService`, `vpc-lattice:AssociateViaAWSService-EventsAndStates`, `vpc-lattice:CreateServiceNetworkResourceAssociation`, `vpc-lattice:GetResourceConfiguration`.

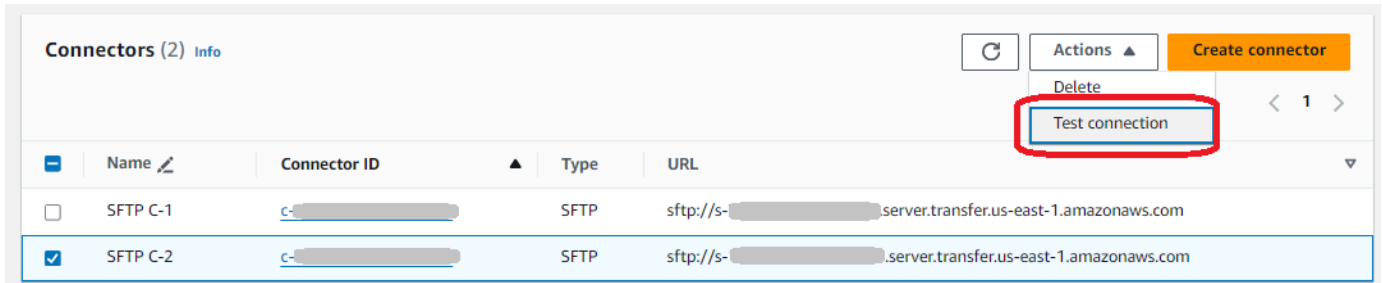
Testen Sie einen SFTP-Connector

Nachdem Sie einen SFTP-Connector erstellt haben, empfehlen wir Ihnen, ihn zu testen, bevor Sie versuchen, Dateien mit Ihrem neuen Connector zu übertragen.

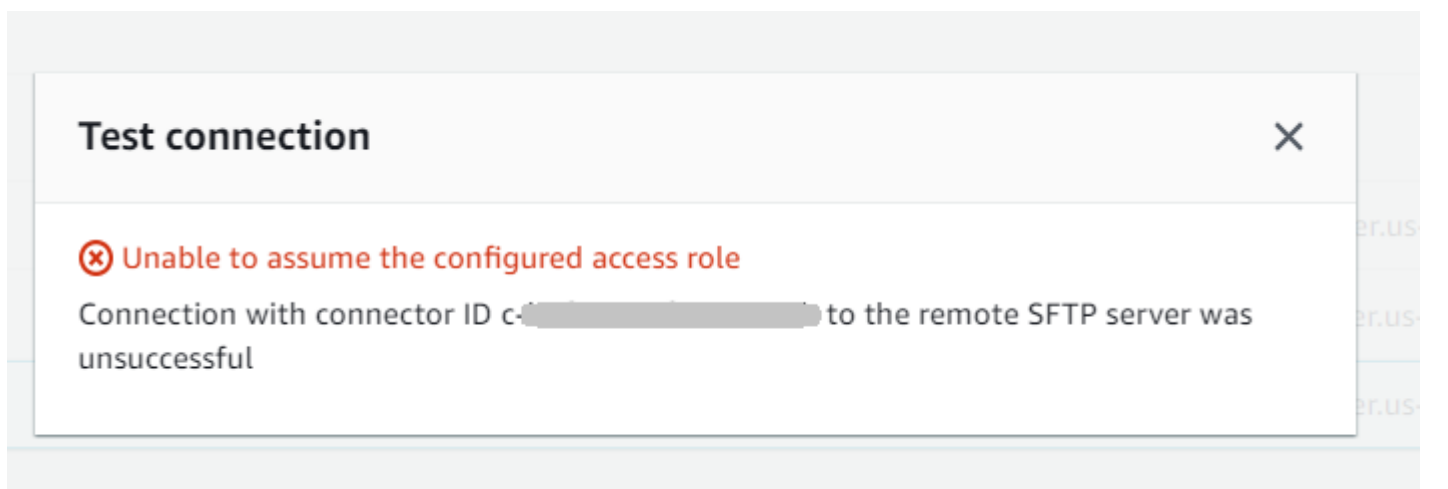
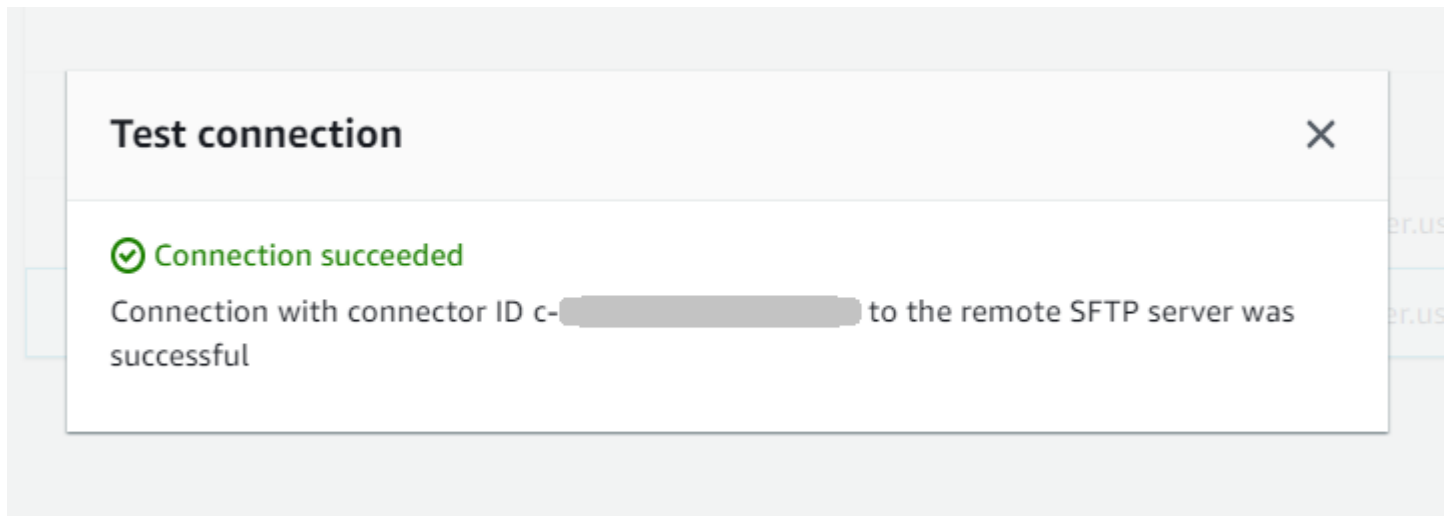
Um einen SFTP-Connector zu testen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>

2. Wählen Sie im linken Navigationsbereich SFTP-Konnektoren und wählen Sie einen Connector aus.
3. Wählen Sie im Menü Aktionen die Option Verbindung testen aus.



Das System gibt eine Meldung zurück, die angibt, ob der Test erfolgreich war oder nicht. Wenn der Test fehlschlägt, gibt das System eine Fehlermeldung aus, die auf dem Grund basiert, warum der Test fehlgeschlagen ist.



 Note

Informationen zum Testen Ihres Connectors mithilfe der API finden Sie in der [TestConnection](#) API-Dokumentation.

VPC-Konnektivität für SFTP-Anschlüsse

AWS Transfer Family SFTP-Konnektoren unterstützen mithilfe von Amazon VPC Lattice Konnektivität zu Remote-SFTP-Servern über Ihre VPC-Umgebungen. Auf diese Weise können Sie eine Verbindung zu privat gehosteten SFTP-Servern herstellen oder den Internetverkehr über die Sicherheitskontrollen Ihrer VPC weiterleiten und Ihre eigenen NAT-Gateways und Elastic IP-Adressen verwenden.

Arten von Ausgängen

SFTP-Anschlüsse können einen von zwei Ausgangstypen verwenden:

- **Service Managed (Standard):** Der Connector verwendet NAT-Gateways und IP-Adressen, die Eigentum von sind AWS Transfer Family , um Verbindungen über das öffentliche Internet weiterzuleiten.
- **VPC_LATTICE:** Der Connector leitet den Datenverkehr mithilfe von Resource Access durch Ihre VPC-Umgebung. Cross-VPC

Wann sollte VPC-Konnektivität verwendet werden?

Verwenden Sie VPC-Konnektivität für SFTP-Connectors in diesen Szenarien:

- **Private SFTP-Server:** Connect zu SFTP-Servern her, auf die nur von Ihrer VPC aus zugegriffen werden kann.
- **On-premises Konnektivität:** Stellen Sie über AWS Direct Connect- oder AWS Site-to-Site VPN-Verbindungen Connect zu lokalen SFTP-Servern her.
- **Benutzerdefinierte IP-Adressen:** Verwenden Sie Ihre eigenen NAT-Gateways und Elastic IP-Adressen, einschließlich BYOIP-Szenarien.
- **Zentralisierte Sicherheitskontrollen:** Leiten Sie Dateiübertragungen über die zentralen Kontrollen Ihres Unternehmens weiter. ingress/egress

Voraussetzungen

Bevor Sie einen LATTICE-enabled VPC_-SFTP-Connector erstellen, benötigen Sie:

- VPC und zugehörige Infrastruktur (Subnetze, Routing-Tabellen, Sicherheitsgruppen)
- Resource Gateway in Ihrer VPC (mindestens zwei Availability Zones)
- Ressourcenkonfiguration unter Angabe des Ziel-SFTP-Servers

Ausführliche Anweisungen zur Einrichtung finden Sie unter [Erstellen Sie einen LATTICE-enabled VPC_-SFTP-Connector](#). Und Beispiele finden Sie unter [Beispiele für VPC-Konnektivität für SFTP-Konnektoren](#).

Verwenden von SFTP-Anschlüssen

In diesem Thema wird beschrieben, wie Sie die unterstützten Dateioperationen mit Ihrem SFTP-Connector ausführen. Sie finden auch Beispielbefehle zur Ausführung dieser Operationen, indem Sie die Details Ihres Connectors auf der AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> auswählen.

Nachdem Sie einen SFTP-Connector erstellt haben, können Sie ihn verwenden, um die folgenden Dateioperationen auf dem Remote-SFTP-Server auszuführen, dem er zugeordnet ist.

- Senden Sie Dateien von Amazon S3 an den Remote-SFTP-Server.
- Rufen Sie Dateien vom Remote-SFTP-Server auf Amazon S3 ab.
- Listet Dateien und Unterordner aus einem Verzeichnis auf dem Remote-SFTP-Server auf.
- Dateien und Verzeichnisse auf dem Remote-SFTP-Server löschen, umbenennen oder verschieben.

Einzelheiten zum Erstellen von Konnektoren finden Sie unter [SFTP-Konnektoren erstellen](#).

Themen

- [Übertragen von Dateien](#)
- [Inhalt eines Remote-Verzeichnisses auflisten](#)
- [Dateien oder Verzeichnisse auf dem Remoteserver verschieben, umbenennen oder löschen](#)

Übertragen von Dateien

Themen

- [Senden und Abrufen von Dateien mithilfe eines SFTP-Connectors](#)

Senden und Abrufen von Dateien mithilfe eines SFTP-Connectors

Um Dateien mithilfe eines SFTP-Connectors zu senden und abzurufen, verwenden Sie den [StartFileTransfer](#) API-Vorgang und geben die folgenden Parameter an, je nachdem, ob Sie Dateien senden (ausgehende Übertragungen) oder Dateien empfangen (eingehende Übertragungen). Beachten Sie, dass jede `StartFileTransfer` Anfrage 10 verschiedene Pfade enthalten kann.

Note

Standardmäßig verarbeiten SFTP-Konnektoren jeweils eine Datei nach der anderen und übertragen Dateien sequentiell. Sie haben die Möglichkeit, die Übertragungsleistung zu beschleunigen, indem Ihre Connectoren gleichzeitige Sitzungen mit Remoteservern erstellen, die gleichzeitige Sitzungen desselben Benutzers unterstützen, und bis zu 5 Dateien parallel verarbeiten.

Um gleichzeitige Verbindungen für jeden Connector zu aktivieren, können Sie die Einstellung `Maximale Anzahl gleichzeitiger Verbindungen` bearbeiten, wenn Sie einen Connector erstellen oder aktualisieren. Details hierzu finden Sie unter [Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang](#).

- **Ausgehende Übertragungen**
 - `send-file-paths` enthält einen bis zehn Quelldateipfade für Dateien, die auf den SFTP-Server des Partners übertragen werden sollen.
 - `remote-directory-path` ist der Remote-Pfad, an den eine Datei auf dem SFTP-Server des Kunden gesendet werden soll.
- **Eingehende Übertragungen**
 - `retrieve-file-paths` enthält einen bis zehn Remote-Pfade. Jeder Pfad gibt einen Speicherort für die Übertragung von Dateien vom SFTP-Server des Partners auf Ihren Transfer Family Family-Server an.
 - `local-directory-path` ist der Amazon S3 S3-Speicherort (Bucket und optionales Präfix), an dem Ihre Dateien gespeichert sind.

Um Dateien zu senden, geben Sie die `remote-directory-path` Parameter `send-file-paths` und an. Sie können bis zu 10 Dateien für den `send-file-paths` Parameter angeben. Der folgende Beispielbefehl sendet die Dateien `/amzn-s3-demo-source-bucket/file2.txt`, die benannt sind `/amzn-s3-demo-source-bucket/file1.txt` und sich im Amazon S3 S3-Speicher befinden, an das `/tmp` Verzeichnis auf dem SFTP-Server Ihres Partners. Um diesen Beispielbefehl zu verwenden, ersetzen Sie den *amzn-s3-demo-source-bucket* durch Ihren eigenen Bucket.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Um Dateien abzurufen, geben Sie die `local-directory-path` Parameter `retrieve-file-paths` und an. Das folgende Beispiel ruft die Dateien `/my/remote/file2.txt` auf dem SFTP-Server des Partners ab `/my/remote/file1.txt` und platziert sie am Amazon S3 S3-Speicherort `/amzn-s3-demo-bucket/`. *prefix* Wenn Sie diese Beispielbefehl verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/
remote/file2.txt \
  --local-directory-path /amzn-s3-demo-bucket/prefix --connector-id
c-2222BBBB3333CCCC4 --region us-east-2
```

Die vorherigen Beispiele spezifizieren absolute Pfade auf dem SFTP-Server. Sie können auch relative Pfade verwenden, d. h. Pfade, die relativ zum Home-Verzeichnis des SFTP-Benutzers sind. Wenn der SFTP-Benutzer beispielsweise `marymajor` und sein Home-Verzeichnis auf dem SFTP-Server sind `/users/marymajor/`, sendet der folgende Befehl an `/amzn-s3-demo-source-bucket/file1.txt /users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

Inhalt eines Remote-Verzeichnisses auflisten

Bevor Sie Dateien von einem Remote-SFTP-Server abrufen, können Sie den Inhalt eines Verzeichnisses auf dem Remote-SFTP-Server abrufen. Dazu verwenden Sie die [StartDirectoryListing](#) API-Operation.

Das folgende Beispiel listet den Inhalt des home Ordners auf dem Remote-SFTP-Server auf, der in der Konfiguration des Connectors angegeben ist. Die Ergebnisse werden am Amazon S3 S3-Speicherort `/amzn-s3-demo-bucket/connector-files` und in einer Datei mit dem Namen `abgelegt-c-AAAA1111BBBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`.

```
aws transfer start-directory-listing \
  --connector-id c-AAAA1111BBBBB2222C \
  --output-directory-path /amzn-s3-demo-bucket/example/connector-files \
  --remote-directory-path /home
```

Dieser AWS CLI Befehl gibt eine Listing-ID und den Namen der Datei zurück, die die Ergebnisse enthält.

```
{
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
  "OutputFileName": "c-AAAA1111BBBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

 Note

Die Benennungskonvention für die Ausgabedatei lautet *connector-ID-listing-ID*.json.

Die JSON-Datei enthält die folgenden Informationen:

- **filePath**: Der vollständige Pfad einer Remote-Datei, relativ zum Verzeichnis der Listing-Anfrage für Ihren SFTP-Connector auf dem Remoteserver.
- **modifiedTimestamp**: das letzte Mal, als die Datei geändert wurde, in Sekunden, UTC-Format (Coordinated Universal Time). Dies ist ein optionales Feld. Wenn die Attribute der Remote-Datei keinen Zeitstempel enthalten, wird dieser in der Dateiliste weggelassen.
- **size**: Die Größe der Datei in Byte. Dies ist ein optionales Feld. Wenn die Remote-Dateiattribute keine Dateigröße enthalten, wird sie in der Dateiliste weggelassen.
- **path**: der vollständige Pfad eines Remote-Verzeichnisses, relativ zum Verzeichnis der Listing-Anfrage für Ihren SFTP-Connector auf dem Remoteserver.
- **truncated**: ein Flag, das angibt, ob die Listenausgabe alle im Remote-Verzeichnis enthaltenen Elemente enthält oder nicht. Wenn Ihr **truncated** Ausgabewert wahr ist, können Sie den im optionalen **max-items** Eingabeattribut angegebenen Wert erhöhen, um mehr Elemente auflisten zu können (bis zur maximal zulässigen Listengröße von 200.000 Elementen).

Das Folgende ist ein Beispiel für den Inhalt der Ausgabedatei (c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json), wobei das Remote-Verzeichnis zwei Dateien und zwei Unterverzeichnisse (Pfade) enthält.

```
{
  "files": [
    {
      "filePath": "/home/what.txt",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 2323
    },
    {
      "filePath": "/home/how.pgp",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 4691
    }
  ],
  "paths": [
    {
      "path": "/home/magic"
    },
    {
      "path": "/home/aws"
    }
  ],
  "truncated": "false"
}
```

Dateien oder Verzeichnisse auf dem Remoteserver verschieben, umbenennen oder löschen

Themen

- [Dateien oder Verzeichnisse auf dem Remote-SFTP-Server verschieben oder umbenennen](#)
- [Löschen Sie Dateien oder Verzeichnisse auf dem Remote-SFTP-Server](#)

Dateien oder Verzeichnisse auf dem Remote-SFTP-Server verschieben oder umbenennen

Sie können einen SFTP-Connector verwenden, um Dateien und Verzeichnisse auf einem Remote-SFTP-Server zu verschieben oder umzubenennen. Beachten Sie, dass der Remoteserver diese Vorgänge für eine erfolgreiche Verarbeitung mithilfe von Konnektoren unterstützen muss.

Einige häufige Anwendungsfälle sind wie folgt.

- Ein Remoteserver generiert oder empfängt jede Stunde eine neue Datei mit demselben Dateinamen, aber einem anderen Zeitstempel. Um den Hauptordner auf dem neuesten Stand zu halten (sodass er nur die neueste Datei enthält), können Sie ältere Dateien mithilfe eines Konnektors in einen archivierten Ordner verschieben.
- Sie verwenden einen Connector, um alle Dateien in einem Remote-Verzeichnis aufzulisten und dann alle Dateien in Ihren lokalen Speicher zu übertragen. Sie können dann einen Connector verwenden, um die Dateien in einen archivierten Ordner auf dem Remoteserver zu verschieben.

Sie müssen für jede Datei oder jedes Verzeichnis, das Sie verarbeiten möchten, einen `StartRemoteMove` Aufruf verwenden, da der Befehl nur eine Quell- und eine Zielfeile oder ein Verzeichnis als Argumente verwendet. Sie können die Leistung jedoch beschleunigen, indem Sie Ihre Connectoren gleichzeitige Sitzungen mit Remoteservern erstellen lassen, die gleichzeitige Sitzungen desselben Benutzers und `move/rename` bis zu 5 Dateien parallel unterstützen.

Im folgenden Beispiel wird eine Datei auf dem Remote-SFTP-Server von `/source/folder/sourceFile` nach `/destination/targetFile` verschoben und eine eindeutige Kennung für den Vorgang zurückgegeben.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
  --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

Note

Für die `move/rename` Operationen verwendet Transfer Family den SFTP `SSH_FXP_RENAME` Standardbefehl, um den `move/rename` Vorgang auszuführen.

Löschen Sie Dateien oder Verzeichnisse auf dem Remote-SFTP-Server

Sie können einen SFTP-Connector verwenden, um Dateien oder Verzeichnisse auf einem Remote-SFTP-Server zu löschen. Beachten Sie, dass der Remoteserver diese Vorgänge für eine erfolgreiche Verarbeitung mithilfe von Konnektoren unterstützen muss.

Note

Löschvorgänge für Remote-Verzeichnisse werden nur für leere Verzeichnisse unterstützt.

Einige häufige Anwendungsfälle sind wie folgt.

- Sie verwenden einen Connector, um eine Datei von einem Remote-SFTP-Server abzurufen, sie in Ihrem Amazon S3-Bucket zu speichern und sie dann zu verschlüsseln. Schließlich können Sie einen Connector verwenden, um die unverschlüsselte Datei auf dem Remote-Server zu löschen.
- Sie verwenden einen Connector, um alle Dateien in einem Remote-Verzeichnis aufzulisten und dann alle Dateien in Ihren lokalen Speicher zu übertragen. Anschließend können Sie einen Connector verwenden, um alle Dateien zu löschen, die Sie übertragen haben. Sie können das Remote-Verzeichnis auch löschen, wenn Sie es vorziehen.

Sie müssen für jede Datei oder jedes Verzeichnis, das Sie löschen möchten, einen `StartRemoteDelete` Aufruf verwenden, da der Befehl eine einzelne Datei oder ein einzelnes Verzeichnis als Argument verwendet. Sie können die Leistung jedoch beschleunigen, indem Sie Ihre Connectoren gleichzeitige Sitzungen mit Remoteservern erstellen lassen, die gleichzeitige Sitzungen desselben Benutzers unterstützen, und bis zu 5 files/directories gleichzeitig löschen.

Im folgenden Beispiel wird eine Datei auf dem Remote-SFTP-Server im Pfad `/delete/folder/deleteFile` gelöscht und eine eindeutige Kennung für den Vorgang zurückgegeben.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \  
--delete-path /delete/folder/deleteFile
```

Note

Für den Löschvorgang verwendet Transfer Family den `SSH_FXP_REMOVE` Standardbefehl, um eine Datei und ein Verzeichnis `SSH_FXP_RMDIR` zu löschen.

Überwachung von SFTP-Anschlüssen

Sie können den Status Ihrer Connector-Operationen auf eine der folgenden Arten überwachen. Wählen Sie den Ansatz, der Ihren Anforderungen entspricht.

Verwenden Sie die Connector-API, um den Status von Dateiübertragungsanfragen abzufragen

Um den Fortschritt eines Dateiübertragungsvorgangs zu verfolgen, verwenden Sie den [ListFileTransferResults](#) API-Vorgang, bei dem Aktualisierungen und detaillierte Informationen zum Status jeder einzelnen Datei, die in einem bestimmten Dateiübertragungsvorgang übertragen wird, in Echtzeit zurückgegeben werden. Sie geben die Dateiübertragung an, indem Sie die zugehörige Connector-ID und die Transfer-ID angeben. Das folgende Beispiel gibt eine Liste von Dateien für Connector-ID a-11112222333344444 und Transfer-ID aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111 zurück.

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-id aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

Die Ergebnisse der Dateiübertragung sind bis zu 7 Tage nach dem Aufruf des `ListFileTransferResults` API-Vorgangs verfügbar.

Sie können auch Protokolle und Ereignisse für Ihre Dateiübertragungsanforderungen anzeigen, die SFTP-Konnektoren verwenden. EventBridge Amazon-Ereignisse für Transfer Family werden unter [beschrieben Ereignisse des SFTP-Connectors](#). Informationen zum Anzeigen von Transfer Family CloudWatch Family-Protokolleinträgen finden Sie unter [Protokollstreams von Transfer Family anzeigen](#).

SFTP-Connector-Ereignisse in Amazon anzeigen EventBridge

Für jeden Vorgang, der über SFTP-Konnektoren ausgeführt wird, generiert Transfer Family automatisch Ereignisse und sendet sie an den Standard-Event-Bus in Ihrem EventBridge Amazon-Konto. Die Ereignisse enthalten detaillierte Metadaten über den Vorgang, einschließlich des Vorgangsstatus. Sie können diese Ereignisse abonnieren EventBridge, Filter auf bestimmte

Ereigniskriterien wie den Betriebsstatus anwenden und basierend auf dem Status automatisch nachgelagerte Aktionen auslösen. Einzelheiten zu den Ereignissen, die durch SFTP-Connector-Operationen generiert werden, finden Sie unter [Ereignisse des SFTP-Connectors](#).

SFTP-Connector-Protokolle in Amazon anzeigen CloudWatch

Bei allen Vorgängen des SFTP-Connectors werden detaillierte Logs generiert. CloudWatch Protokolleinträge, die von SFTP-Konnektoren generiert wurden, finden Sie beispielsweise unter [Beispielprotokolleinträge für SFTP-Konnektoren](#)

Überwachung VPC VPC-Ausgangsanschlüssen

Konnektoren vom Typ VPC Egress bieten zusätzliche Überwachungsfunktionen und Überlegungen, die über standardmäßige Service Managed Connectors hinausgehen:

Überwachung des Konnektorstatus

VPC_LATTICE-Konnektoren enthalten zusätzliche Informationen, mit denen Sie den Bereitstellungs- und Betriebsstatus überwachen können:

- EgressType Feld: Wird für ausgehende Konnektoren vom Typ VPC_LATTICE angezeigt VPC
- EgressConfig Feld: Enthält die ARN- und Port-Informationen zur Ressourcenkonfiguration

Überwachen Sie den Konnektorstatus mithilfe der `describe-connector` API:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Überwachung der VPC-Lattice-Kosten

Für VPC-Ausgangsanschlüsse fallen zusätzliche VPC-Lattice-Gebühren an, die Sie überwachen sollten:

- Gebühren des Ressourcenanbieters: Ihnen werden 0 USD in Rechnung gestellt. 006/GB für die Datenverarbeitung als Ressourcenanbieter (direkt von VPC Lattice in Rechnung gestellt)
- Gebühren für Ressourcenverbraucher: AWS Transfer Family übernimmt die 0\$. 01/GB Kosten für den Ressourcenverbrauch (erstes 1 PB)
- NAT-Gateway-Gebühren: Für öffentliche Endpunkte, auf die über VPC zugegriffen wird, können zusätzliche NAT-Gateway- und Datenübertragungsgebühren anfallen

- **Familiengebühren übertragen:** Standard 0\$. 40/GB Datenverarbeitungsgebühren fallen weiterhin an

Überwachen Sie die Nutzung und die Kosten von VPC Lattice über die AWS Cost and Billing Console und filtern Sie dabei nach dem VPC Lattice-Dienst.

Netzwerküberwachung für VPC-Konnektoren

Überwachen Sie die Netzwerkaktivität und -leistung für VPC-Ausgangsanschlüsse:

- **VPC Flow Logs:** Aktivieren Sie VPC Flow Logs, um Netzwerkverkehrsmuster zwischen Resource Gateways und SFTP-Servern zu überwachen
- **VPC Lattice-Zugriffsprotokolle:** VPC Lattice bietet Zugriffsprotokolle, die source/destination IP-Adressen, Verbindungszeiten und Datenübertragungsvolumen anzeigen
- **Überwachung von Sicherheitsgruppen:** Überwachen Sie Sicherheitsgruppenregeln und Verkehrsmuster, um eine angemessene Netzwerkzugriffskontrolle sicherzustellen
- **Überwachung der DNS-Auflösung:** Überwachen Sie die Zeiten und Ausfälle der DNS-Auflösung für Dienstnetzwerkendpunkte

Beispiel für einen Eintrag im VPC Lattice-Zugriffsprotokoll:

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
  "gatewayIpPort": "10.0.1.150:1769",
  "resourceIpPort": "10.0.2.200:22"
}
```

Problembehebung durch Überwachung

Verwenden Sie Überwachungsdaten, um häufig auftretende VPC-Connector-Probleme zu beheben:

- **Status AUSSTEHEND:** Überwachen Sie den Fortschritt der DNS-Auflösung und warten Sie, bis der Status **AKTIV** ist, bevor Sie Übertragungen versuchen
- **Verbindungs-Timeouts:** Überprüfen Sie die VPC-Flow-Logs und die Sicherheitsgruppenregeln auf blockierten Datenverkehr auf Port 22
- **Übertragungsfehler:** Überprüfen Sie die CloudWatch Protokolle auf detaillierte Fehlermeldungen und die VPC Lattice-Zugriffsprotokolle auf Netzwerkebene
- **Leistungsprobleme:** Überwachen Sie die VPC-Lattice-Zugriffsprotokolle auf Verbindungszeit und Durchsatzmetriken

Verwaltung von SFTP-Konnektoren

In diesem Thema wird beschrieben, wie SFTP-Konnektoren angezeigt und aktualisiert werden.

Note

Jedem Connector werden automatisch statische IP-Adressen zugewiesen, die während der Lebensdauer des Connectors unverändert bleiben. Auf diese Weise können Sie eine Verbindung zu Remote-SFTP-Servern herstellen, die nur eingehende Verbindungen von bekannten IP-Adressen akzeptieren. Ihren Connectoren wird ein Satz statischer IP-Adressen zugewiesen, die von allen Connectoren gemeinsam genutzt werden, die dasselbe Protokoll (SFTP oder AS2) in Ihrem verwenden. AWS-Konto Diese Adressen sind nicht ausschließlich Ihrem Konto gewidmet.

Wenn Sie dedizierte, vorhersehbare IP-Adressen benötigen, konfigurieren Sie Ihre Connectors mit VPC-based Egress. Weitere Informationen finden Sie unter [the section called “Erstellen Sie einen SFTP-Connector mit Egress VPC-based”](#).

Aktualisieren Sie die SFTP-Konnektoren

Um die vorhandenen Parameterwerte für Ihre Konnektoren zu ändern, können Sie den `update-connector` Befehl ausführen. Mit dem folgenden Befehl wird das Geheimnis für den Connector *connector-id* in der Region *region-id* auf aktualisiert *secret-ARN*. Wenn Sie diesen Beispielfehl verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
```



```
--connector-id connector-id --region region-id
```

Aktualisierung der VPC-Konnektivitätseinstellungen

Sie können die VPC-Konnektivitätseinstellungen für vorhandene Connectors aktualisieren, einschließlich des Wechsels zwischen serviceverwalteten und VPC-Ausgangstypen oder der Änderung des ARN für die Ressourcenkonfiguration.

So schalten Sie einen Connector von serviceverwaltetem auf VPC-Egress um:

```
aws transfer update-connector \  
  --connector-id connector-id \  
  --egress-type VPC \  
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

So aktualisieren Sie den ARN für die Ressourcenkonfiguration für einen LATTICE-enabled VPC_-Connector:

```
aws transfer update-connector \  
  --connector-id connector-id \  
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Bei der Aktualisierung der VPC-Konnektivitätseinstellungen ändert sich der Connectorstatus PENDING während der Neukonfiguration auf. Überwachen Sie den Status des Connectors mithilfe des `describe-connector` Befehls.

Details zum SFTP-Connector anzeigen

In der Konsole finden Sie eine Liste mit Details und Eigenschaften für einen SFTP-Connector. AWS Transfer Family

Um die Connector-Details anzuzeigen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich die Option Connectors aus.

3. Wählen Sie den Bezeichner in der Spalte Connector-ID aus, um die Detailseite für den ausgewählten Connector aufzurufen.

Sie können die Eigenschaften für den SFTP-Connector ändern, indem Sie auf der Connector-Detailseite auf Bearbeiten klicken.

Überwachung des VPC-Connectorstatus

LATTICE-enabled VPC_-Konnektoren enthalten zusätzliche Statusinformationen, mit denen Sie den Bereitstellungsprozess überwachen können:

- Status: Zeigt PENDING, oder ACTIVE ERRORED
- EgressType: Zeigt VPC oder SERVICE_MANAGED
- EgressConfig: Enthält den ARN für die Ressourcenkonfiguration für VPC-Konnektoren
- Fehler: Stellt detaillierte Fehlerinformationen bereit, wenn sich der Connector im ERRORED Status befindet

Für VPC-Connectoren ist das ServiceManagedEgressIpAddresses Feld leer, da der Datenverkehr stattdessen Ihre VPC-IP-Adressen verwendet.

Note

Sie können viele dieser Informationen, wenn auch in einem anderen Format, abrufen, indem Sie den folgenden AWS Command Line Interface (AWS CLI) Befehl ausführen. Wenn Sie diesen Beispielfehl verwenden möchten, ersetzen Sie *user input placeholders* durch Ihre Informationen.

```
aws transfer describe-connector --connector-id your-connector-id
```

Weitere Informationen finden Sie [DescribeConnector](#) in der API-Referenz.

Skalierung und Kontingente für SFTP-Konnektoren

Themen

- [Kontingente für SFTP-Anschlüsse](#)

- [Skalierung Ihrer SFTP-Konnektoren](#)

Kontingente für SFTP-Anschlüsse

Die folgenden Kontingente gelten für SFTP-Konnektoren.

Note

Weitere Dienstkontingente für SFTP-Konnektoren sind unter [AWS Transfer Family Endpunkte und Kontingente](#) in der aufgeführt. Allgemeine Amazon Web Services-Referenz

Kontingente für SFTP-Konnektoren

Name	Standard	Anpassbar
Maximale Anzahl an Testverbindungstransaktionen pro Sekunde (TPS)	1 Anfrage pro Sekunde, pro Konto	Nein
Maximale Warteschlangengröße für ausstehende Dateiübertragungen	1000	Nein
Maximale Dateigröße	150 Gibibyte (GiB)	Nein
Maximale Übertragungszeit pro Datei	12 Stunden	Nein
Maximale Wartezeit für Anfragen pro Datei	12 Stunden	Nein
Maximale Bandbreite für Konnektoren pro Konto (sowohl SFTP- als auch AS2-Konnektoren tragen zu diesem Wert bei)	50 Mbit/s	Nein

Name	Standard	Anpassbar
Maximale Anzahl von Elementen für Operationen zum Auflisten von Verzeichnissen	200 000	Nein

Note

Standardmäßig verarbeiten SFTP-Konnektoren jeweils eine Datei und übertragen Dateien nacheinander. Sie haben die Möglichkeit, die Übertragungsleistung zu beschleunigen, indem Ihre Connectoren gleichzeitige Sitzungen mit Remoteservern erstellen, die gleichzeitige Sitzungen desselben Benutzers unterstützen, und bis zu 5 Dateien parallel verarbeiten. Um gleichzeitige Verbindungen für jeden Connector zu aktivieren, können Sie die Einstellung Maximale Anzahl gleichzeitiger Verbindungen bearbeiten, wenn Sie einen Connector erstellen oder aktualisieren. Details hierzu finden Sie unter [Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang](#).

Für das Speichern der Anmeldeinformationen für SFTP-Konnektoren sind mit jedem Secrets Manager Manager-Geheimnis Kontingente verknüpft. Wenn Sie dasselbe Geheimnis zum Speichern mehrerer Schlüsseltypen für verschiedene Zwecke verwenden, können Sie auf diese Kontingente stoßen.

- Gesamtlänge eines einzelnen Geheimnisses: 12.000 Zeichen
- Maximale Länge der **Password** Zeichenfolge: 1024 Zeichen
- Maximale Länge der **PrivateKey** Zeichenfolge: 8192 Zeichen
- Maximale Länge der **Username** Zeichenfolge: 100 Zeichen

Skalierung Ihrer SFTP-Konnektoren

In diesem Abschnitt werden Überlegungen zur Skalierung Ihrer AWS Transfer Family SFTP-Connector-Workloads beschrieben. Sie müssen die folgenden drei Kontingente berücksichtigen, die gelten, wenn Sie Ihre Workloads mit SFTP-Konnektoren skalieren möchten.

- Die maximale Warteschlangengröße. Dies bezieht sich auf die maximale Anzahl von ausstehenden Vorgängen in der Warteschlange eines Connectors, die angefordert wurden. Ein ausstehender Vorgang bezieht sich auf alle zuvor eingereichten Übertragungsanforderungen, die noch nicht abgeschlossen wurden, entweder erfolgreich oder erfolglos.

Die maximale Warteschlangentiefe für ausstehende Anfragen ist derzeit auf 1.000 pro Connector festgelegt (wie in den [AWS Transfer Family Dienstkontingenten](#) definiert). Ihre Workloads können dieses Servicelimit überschreiten, wenn Sie innerhalb eines kurzen Zeitraums Tausende von Übertragungsvorgängen anfordern. Sie erhalten dann eine Meldung `ThrottlingException` mit der Meldung Maximale Anzahl ausstehender Anfragen überschritten. Wenn Ihre Workloads diesem Kontingent unterliegen, wenden Sie sich an das Transfer Family Family-Serviceteam AWS Support oder an Ihr Account-Team, um Ihre Skalierbarkeitsanforderungen zu besprechen.

Sie können auch eine oder beide der folgenden Maßnahmen ergreifen.

- Verteilen Sie Ihre Dateivolumes auf mehrere Konnektoren.
- Lassen Sie Ihre Connectoren gleichzeitige Sitzungen mit dem Remoteserver erstellen, um mehrere Anfragen aus der Warteschlange parallel zu verarbeiten.
- Die Anzahl der gleichzeitigen Sitzungen. Standardmäßig überträgt ein SFTP-Connector jeweils eine Datei, wobei die Dateien nacheinander aus der Warteschlange übertragen werden.

Sie haben die Möglichkeit, die Übertragungsleistung zu beschleunigen, indem Sie Ihre Konnektoren mehrere Dateien parallel übertragen lassen. Sie können gleichzeitige Sitzungen mit Remoteservern erstellen, die gleichzeitige Sitzungen desselben Benutzers unterstützen, und bis zu 5 Dateien parallel verarbeiten. Wenn Sie einen SFTP-Connector erstellen, wählen Sie einen Wert bis zu 5 für die Einstellung Maximale Anzahl gleichzeitiger Verbindungen, wenn Sie den Connector erstellen oder aktualisieren. Details hierzu finden Sie unter [Erstellen Sie einen SFTP-Connector mit serviceverwaltetem Ausgang](#).

- Die Rate der Anfragen. **StartFileTransfer** Sie können mit jedem SFTP-Anschluss bis zu 100 Dateipfade pro Sekunde für die Übertragung anfordern. Die angeforderten Dateipfade werden der Warteschlange Ihrer Konnektoren zur Verarbeitung hinzugefügt. Sie können den `StartFileTransfer` Befehl rekursiv verwenden, um bis zu 100 Dateipfade pro Sekunde und Konnektor anzufordern, unabhängig von der Anzahl der Dateien, die in einem einzelnen Befehl bereitgestellt werden. `StartFileTransfer`

Referenzarchitekturen, die SFTP-Konnektoren verwenden

In diesem Abschnitt werden die Referenzmaterialien aufgeführt, die für die Konfiguration automatisierter Dateiübertragungsworkflows mithilfe von SFTP-Konnektoren verfügbar sind. Sie können Ihre eigenen ereignisgesteuerten Architekturen entwerfen, indem Sie die SFTP-Connector-Ereignisse in Amazon verwenden EventBridge, um zwischen Ihrer Dateiübertragungsaktion und den Vor- und Nachverarbeitungsaktionen in zu orchestrieren. AWS

Blog-Posts

Der folgende Blogbeitrag bietet eine Referenzarchitektur für die Erstellung eines MFT-Workflows mithilfe von SFTP-Konnektoren, einschließlich der Verschlüsselung von Dateien mit PGP, bevor sie mithilfe von SFTP-Konnektoren an einen Remote-SFTP-Server gesendet werden: [Architektur sicherer und richtlinienkonformer verwalteter Dateiübertragungen mit SFTP-Konnektoren und PGP-Verschlüsselung](#). AWS Transfer Family

Workshops

- Der folgende Workshop bietet praktische Übungen zur Konfiguration von SFTP-Konnektoren und zur Verwendung Ihrer Konnektoren zum Senden oder Abrufen von Dateien von Remote-SFTP-Servern: [Transfer Family — SFTP-Workshop](#).
- [Der folgende Workshop bietet praktische Übungen zur Erstellung vollautomatischer und ereignisgesteuerter Workflows, die die Übertragung von Dateien zu oder von externen SFTP-Servern zu Amazon S3 sowie die allgemeine Vor- und Nachverarbeitung dieser Dateien beinhalten: MFT-Workshop. Event-driven](#)

Dieses Video bietet einen Überblick über diesen Workshop.

Lösungen

AWS Transfer Family bietet die folgenden Lösungen:

- Die [Dateiübertragungssynchronisierungslösung bietet eine Referenzarchitektur zur Automatisierung des Synchronisierungsprozesses](#) von Remote-SFTP-Verzeichnissen — einschließlich ganzer Ordnerstrukturen — mit Ihren lokalen Amazon S3 S3-Buckets mithilfe eines SFTP-Connectors. Sie orchestriert den Prozess der Auflistung von Remote-Verzeichnissen, der Erkennung von Änderungen und der Übertragung neuer oder geänderter Dateien.

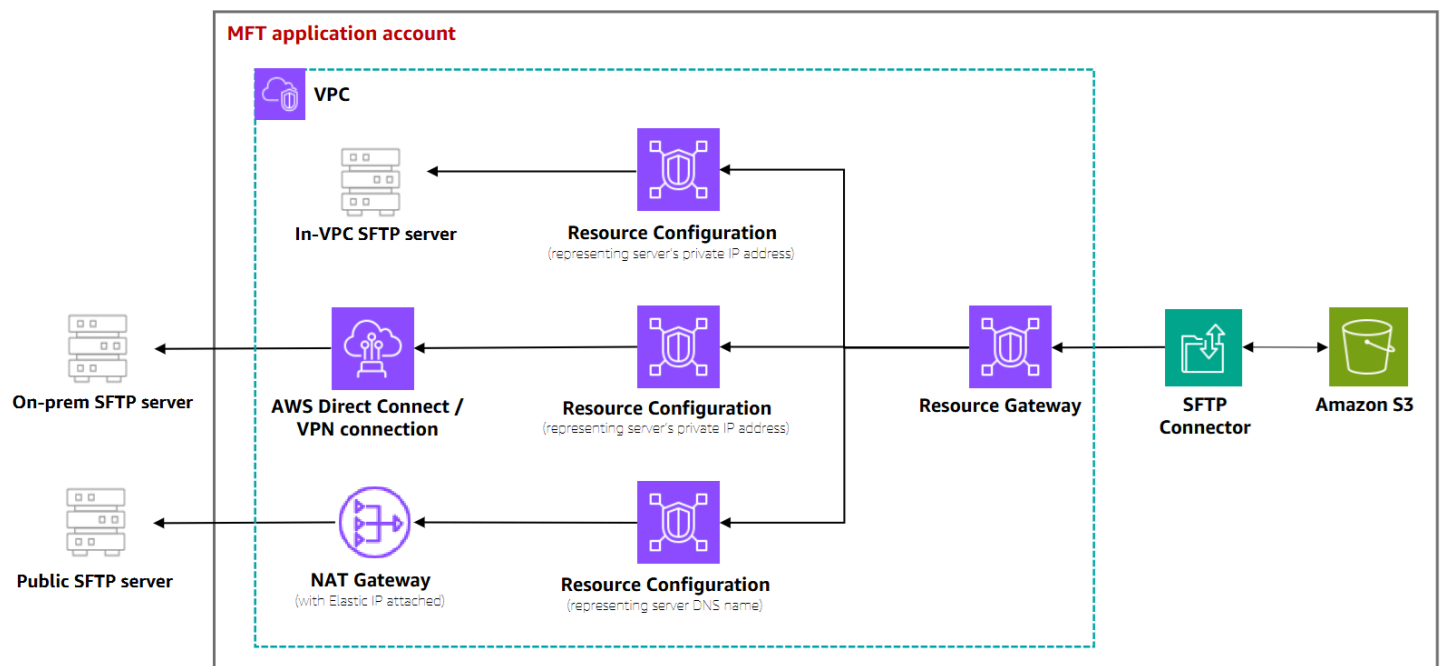
- [Serverlessland — Selektive Dateiübertragung zwischen Remote-SFTP-Server und S3; Die Verwendung AWS Transfer Family](#) bietet ein Beispielmuster für das Auflisten von Dateien, die an Remote-SFTP-Speicherorten gespeichert sind, und für die Übertragung selektiver Dateien an Amazon S3.

VPC-Referenzarchitekturen

Die folgenden Referenzarchitekturen zeigen gängige Muster für die Bereitstellung von LATTICE-enabled VPC_-SFTP-Konnektoren. Diese Beispiele helfen Ihnen zu verstehen, wo VPC Lattice-Ressourcen in Ihrer AWS Gesamtarchitektur erstellt werden müssen.

Einzelkonto mit gemeinsam genutzter Ausgangsinfrastruktur

In dieser Architektur ist die Ausgangsinfrastruktur (NAT-Gateway, VPN-Tunnel oder Direct Connect) in einer VPC innerhalb desselben Kontos wie Ihre SFTP-Konnektoren konfiguriert. Alle Connectoren können dasselbe Resource Gateway und NAT-Gateway gemeinsam nutzen.

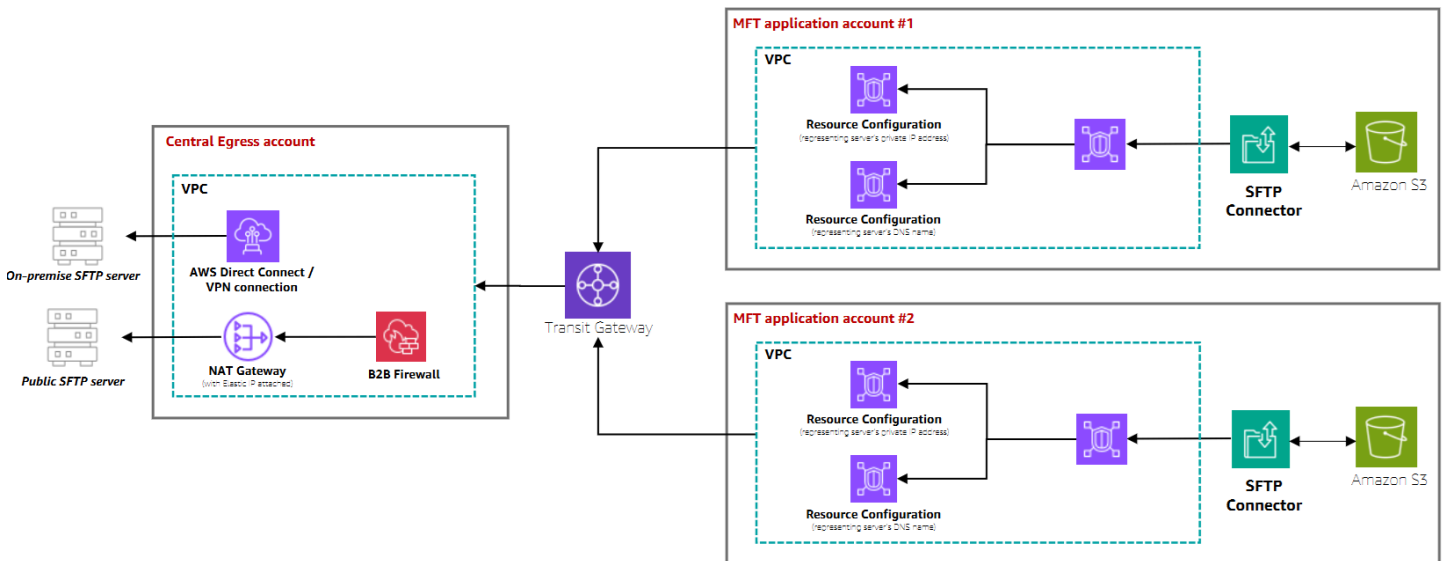


Dieses Muster ist ideal, wenn:

- Alle SFTP-Konnektoren werden in einem einzigen verwalteten AWS-Konto
- Die Ausgangsinfrastruktur wird in einer VPC innerhalb desselben Kontos wie Ihre SFTP-Konnektoren eingerichtet

Cross-account mit zentraler Ausgangsinfrastruktur

In dieser Architektur wird die Ausgangsinfrastruktur (NAT-Gateway, VPN-Tunnel, Direct Connect oder B2B-Firewalls) in einem zentralen Ausgangskonto konfiguriert, das vom Netzwerkteam verwaltet wird. SFTP-Konnektoren werden im MFT-Anwendungskonto erstellt, das vom MFT-Administrationsteam verwaltet wird. Cross-account Das Netzwerk wird mithilfe von Transit Gateway eingerichtet, um bestehende Netzwerkregeln einzuhalten.



Dieses Muster ist ideal, wenn:

- Die Netzwerkinfrastruktur von einem separaten Team in einem speziellen Konto verwaltet wird
- Sie haben bestehende Routen (z. B. AWS Transit Gateway) zwischen dem Konto, in dem SFTP-Konnektoren erstellt werden, und dem Konto, in dem die Ausgangsinfrastruktur eingerichtet ist. SFTP-Konnektoren können Ihre vorhandenen Routen nutzen, die die beiden Konten verbinden.
- Zentralisierte Sicherheitskontrollen und B2B-Firewalls sind erforderlich
- Sie müssen die Aufgabentrennung zwischen Netzwerk- und Anwendungsteams aufrechterhalten

AWS Transfer Family für AS2

Applicability Statement 2 (AS2) ist eine Spezifikation für die RFC-defined Übertragung von Dateien, die starke Mechanismen zum Schutz und zur Überprüfung von Nachrichten umfasst. Der Schutz einer AS2-Nutzlast während der Übertragung verwendet Cryptographic Message Syntax (CMS) mit Verschlüsselung und digitalen Signaturen, um Datenschutz und Peer-Authentifizierung zu gewährleisten. Eine signierte MDN-Antwortpayload (Message Disposition Notice) dient der Überprüfung (Unwiderlegbarkeit), dass eine Nachricht empfangen und erfolgreich entschlüsselt wurde.

Das AS2-Protokoll ist entscheidend für Workflows mit Compliance-Anforderungen, die darauf beruhen, dass Datenschutz- und Sicherheitsfunktionen in das Protokoll integriert sind. AWS Transfer Family AS2-Endgeräte sind [Drummond-zertifiziert](#), sodass Kunden in Branchen wie Einzelhandel, Biowissenschaften, Fertigung, Finanzdienstleistungen und Versorgungsunternehmen sichere Transaktionen mit ihren Geschäftspartnern durchführen können.

Wenn Sie AS2 mit Transfer Family verwenden, sind die Transaktionsdaten nativ zugänglich für: AWS

- Verarbeitung, Analyse und maschinelles Lernen
- Integration mit ERP-Systemen (Enterprise Resource Planning)
- Integration mit Systemen für das Kundenbeziehungsmanagement (CRM)

Um Dateien mit einem Partner auszutauschen, der über einen AS2-enabled Server verfügt, müssen Sie:

- Generieren Sie ein öffentlich-privates key pair für die Verschlüsselung
- Generieren Sie ein öffentlich-privates key pair zum Signieren
- Tauschen Sie die öffentlichen Schlüssel mit Ihrem Partner aus

Important

HTTPS AS2-Serverendpunkte werden derzeit nicht unterstützt. Sie sind für die TLS-Terminierung verantwortlich.

Transfer Family bietet einen Workshop, an dem Sie teilnehmen können, in dem Sie einen Transfer Family-Endpunkt mit aktiviertem AS2 und einen Transfer Family AS2-Connector konfigurieren können. [Die Details zu diesem Workshop finden Sie hier.](#)

Eine schrittweise Anleitung zur Konfiguration von AS2 in Transfer Family finden Sie im Folgenden:

1. [AS2-Zertifikate importieren](#)
2. [Erstellen Sie AS2-Profil](#)
3. [Erstellen Sie einen AS2-Server](#)
4. [Erstellen Sie eine AS2-Vereinbarung](#)
5. [Konfigurieren Sie AS2-Konnektoren](#)

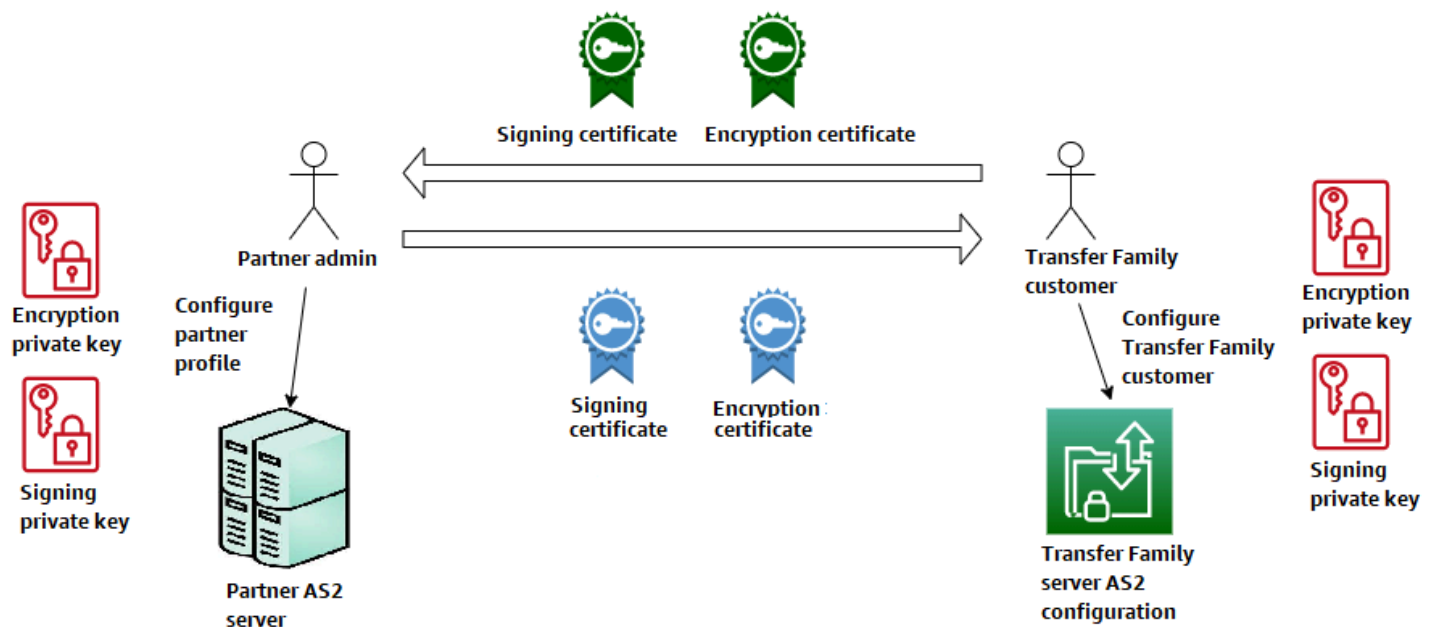
Ein vollständiges Beispiel finden Sie unter [Einrichtung einer AS2-Konfiguration](#).

Note

Um die Unterstützung für AS2-Terraform-Vorlagen anzuzeigen, fügen Sie der Funktionsanfrage für [Terraform-Vorlagen der Transfer Family](#) eine Reaktion mit dem Daumen hoch (#) hinzu. Sie können auch einen Kommentar hinzufügen, der Ihren Anwendungsfall beschreibt.

AS2-Anwendungsfälle

Wenn Sie ein AWS Transfer Family Kunde sind, der Dateien mit einem Partner austauschen möchte, der über einen AS2-enabled Server verfügt, besteht der komplexeste Teil der Einrichtung darin, ein öffentlich-privates key pair für die Verschlüsselung und ein weiteres für das Signieren und Austauschen der öffentlichen Schlüssel mit dem Partner zu generieren.



Ziehen Sie die folgenden Varianten für die Verwendung AWS Transfer Family mit AS2 in Betracht.

Note

Handelspartner ist der Partner, der mit diesem Partnerprofil verknüpft ist.
Bei allen Erwähnungen von MDN in der folgenden Tabelle wird von signierten mDNs ausgegangen.

AS2-Anwendungsfälle

Inbound-only Anwendungsfälle

- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Handelspartner auf einen Transfer Family Family-Server.

Führen Sie in diesem Fall folgende Schritte aus:

- Erstellen Sie Profile für Ihren Handelspartner und sich selbst.
- Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet.
- Erstellen Sie eine Vereinbarung und fügen Sie sie Ihrem Server hinzu.
- Importieren Sie ein Zertifikat mit einem privaten Schlüssel und fügen Sie es Ihrem Profil hinzu. Importieren Sie dann den öffentlichen Schlüssel zur Verschlüsselung in Ihr Partnerprofil.

5. Nachdem Sie diese Elemente erhalten haben, senden Sie den öffentlichen Schlüssel für Ihr Zertifikat an Ihren Handelspartner.

Jetzt kann Ihr Partner Ihnen verschlüsselte Nachrichten senden und Sie können sie entschlüsseln und in Ihrem Amazon S3 S3-Bucket speichern.

- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Handelspartner auf einen Transfer Family Family-Server und fügen Sie die Signatur hinzu.

In diesem Szenario führen Sie immer noch nur eingehende Übertragungen durch, aber jetzt möchten Sie, dass Ihr Partner die von ihm gesendeten Nachrichten signiert. Importieren Sie in diesem Fall den öffentlichen Signaturschlüssel des Handelspartners (als Signaturzertifikat, das dem Profil Ihres Partners hinzugefügt wurde).

- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Handelspartner auf einen Transfer Family Family-Server und fügen Sie das Signieren und Senden einer MDN-Antwort hinzu.

In diesem Szenario führen Sie immer noch nur eingehende Übertragungen durch, aber Ihr Handelspartner möchte jetzt nicht nur signierte Payloads empfangen, sondern auch eine signierte MDN-Antwort erhalten.

1. Importieren Sie Ihre öffentlichen und privaten Signaturschlüssel (als Signaturzertifikat in Ihr Profil).
2. Senden Sie den öffentlichen Signaturschlüssel an Ihren Handelspartner.

Outbound-only Anwendungsfälle

- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Transfer Family Family-Server an einen Handelspartner.

Dieser Fall ähnelt dem Anwendungsfall für eingehende Übertragungen, mit dem Unterschied, dass Sie, anstatt Ihrem AS2-Server eine Vereinbarung hinzuzufügen, einen Connector erstellen. In diesem Fall importieren Sie den öffentlichen Schlüssel Ihres Handelspartners in sein Profil.

- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Transfer Family Family-Server an einen Handelspartner und fügen Sie die Signatur hinzu.

Sie führen immer noch nur ausgehende Übertragungen durch, aber jetzt möchte Ihr Handelspartner, dass Sie die Nachricht, die Sie an ihn senden, signieren.

1. Importieren Sie Ihren privaten Signaturschlüssel (als Signaturzertifikat, das Ihrem Profil hinzugefügt wurde).
 2. Senden Sie Ihrem Handelspartner Ihren öffentlichen Schlüssel.
- Übertragen Sie verschlüsselte AS2-Nachrichten von einem Transfer Family Family-Server an einen Handelspartner, fügen Sie die Signatur hinzu und senden Sie eine MDN-Antwort.

Sie führen immer noch nur ausgehende Übertragungen durch, aber jetzt möchten Sie nicht nur signierte Payloads senden, sondern auch eine signierte MDN-Antwort von Ihrem Handelspartner erhalten.

1. Ihr Handelspartner sendet Ihnen seinen öffentlichen Signaturschlüssel.
2. Importieren Sie den öffentlichen Schlüssel Ihres Handelspartners (als Signaturzertifikat, das Ihrem Partnerprofil hinzugefügt wurde).

Anwendungsfälle für eingehenden und ausgehenden Datenverkehr

- Übertragen Sie verschlüsselte AS2-Nachrichten in beide Richtungen zwischen einem Transfer Family Family-Server und einem Handelspartner.

Führen Sie in diesem Fall folgende Schritte aus:

1. Erstellen Sie Profile für Ihren Handelspartner und sich selbst.
2. Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet.
3. Erstellen Sie eine Vereinbarung und fügen Sie sie Ihrem Server hinzu.
4. Erstellen Sie einen Konnektor.
5. Importieren Sie ein Zertifikat mit einem privaten Schlüssel und fügen Sie es Ihrem Profil hinzu. Importieren Sie dann den öffentlichen Schlüssel zur Verschlüsselung in Ihr Partnerprofil.
6. Erhalten Sie einen öffentlichen Schlüssel von Ihrem Handelspartner und fügen Sie ihn zur Verschlüsselung zu seinem Profil hinzu.
7. Nachdem Sie diese Artikel erhalten haben, senden Sie den öffentlichen Schlüssel für Ihr Zertifikat an Ihren Handelspartner.

Jetzt können Sie und Ihr Handelspartner verschlüsselte Nachrichten austauschen, und Sie können sie beide entschlüsseln. Sie können die Nachrichten, die Sie erhalten, in Ihrem Amazon S3 S3-Bucket speichern, und Ihr Partner kann die Nachrichten, die Sie an ihn senden, entschlüsseln und speichern.

- Übertragen Sie verschlüsselte AS2-Nachrichten in beide Richtungen zwischen einem Transfer Family Family-Server und einem Handelspartner und fügen Sie die Signatur hinzu.

Jetzt möchten Sie und Ihr Partner signierte Nachrichten.

1. Importieren Sie Ihren privaten Signaturschlüssel (als Signaturzertifikat, das Ihrem Profil hinzugefügt wurde).
 2. Senden Sie Ihrem Handelspartner Ihren öffentlichen Schlüssel.
 3. Importieren Sie den öffentlichen Signaturschlüssel Ihres Handelspartners und fügen Sie ihn seinem Profil hinzu.
- Übertragen Sie verschlüsselte AS2-Nachrichten in beide Richtungen zwischen einem Transfer Family Family-Server und einem Handelspartner, fügen Sie die Signatur hinzu und senden Sie eine MDN-Antwort.

Jetzt möchten Sie signierte Payloads austauschen, und sowohl Sie als auch Ihr Handelspartner wünschen MDN-Antworten.

1. Ihr Handelspartner sendet Ihnen seinen öffentlichen Signaturschlüssel.
2. Importieren Sie den öffentlichen Schlüssel Ihres Handelspartners (als Signaturzertifikat in Ihr Partnerprofil).
3. Senden Sie Ihren öffentlichen Schlüssel an Ihren Handelspartner.

AS2-Vorlagen CloudFormation

Dieses Thema enthält Informationen zu AWS CloudFormation Vorlagen, mit denen Sie schnell AS2-Server und -Konfigurationen bereitstellen können. AWS Transfer Family Diese Vorlagen automatisieren den Einrichtungsprozess und helfen Ihnen bei der Implementierung von Best Practices für AS2-Dateiübertragungen.

- Die grundlegende AS2-Vorlage wird unter beschrieben [Verwenden Sie eine Vorlage, um einen Demo-Stack der Transfer Family AS2 zu erstellen](#)
- Die AS2-Vorlage zum Anpassen von HTTP-Headern wird unter beschrieben. [Passen Sie HTTP-Header für AS2-Nachrichten an](#)

AS2-Vorlagen anpassen

Sie können die bereitgestellten Vorlagen an Ihre spezifischen Anforderungen anpassen:

1. Laden Sie die Vorlage von der S3-URL herunter.
2. Ändern Sie den YAML-Code, um Konfigurationen wie die folgenden anzupassen:
 - Sicherheitseinstellungen und Zertifikatkonfigurationen
 - Netzwerkarchitektur und VPC-Einstellungen
 - Speicheroptionen und Dateiverwaltung
 - Einstellungen für Überwachung und Benachrichtigung
3. Laden Sie Ihre geänderte Vorlage in Ihren eigenen S3-Bucket hoch.
4. Stellen Sie die benutzerdefinierte Vorlage mithilfe der CloudFormation Konsole bereit oder AWS CLI.

 Important

Achten Sie beim Anpassen von Vorlagen darauf, dass Sie die Abhängigkeiten zwischen den Ressourcen beibehalten und die bewährten Sicherheitsmethoden befolgen.

Testen Sie Ihre AS2-Bereitstellung

Nachdem Sie einen AS2-Server mithilfe einer Vorlage bereitgestellt haben, können Sie die Konfiguration testen:

1. In den CloudFormation Stack-Ausgaben finden Sie Beispielbefehle und Endpunktinformationen.
2. Verwenden Sie den AWS CLI , um eine Testdatei zu senden:

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt  
aws transfer start-file-transfer --connector-id your-connector-id --send-file-  
paths /your-bucket-name/test.txt
```

3. Überprüfen Sie die Dateizustellung im Ziel-S3-Bucket.
4. Überprüfen Sie die CloudWatch Protokolle auf erfolgreiche Verarbeitung und MDN-Antworten.

Für umfassendere Tests sollten Sie die Verwendung von AS2-Clients von Drittanbietern in Betracht ziehen, um Dateien an Ihren Transfer Family AS2-Server zu senden.

Bewährte Methoden für die Bereitstellung von AS2-Vorlagen

Beachten Sie bei der Verwendung von CloudFormation AS2-Vorlagen die folgenden bewährten Methoden:

Sicherheit

Verwenden Sie sichere Zertifikate und wechseln Sie diese regelmäßig ab.

Implementieren Sie IAM-Richtlinien mit den geringsten Rechten.

Beschränken Sie den Netzwerkzugriff mithilfe von Sicherheitsgruppen.

Zuverlässigkeit

Stellen Sie die Lösung in mehreren Availability Zones bereit.

Implementieren Sie Überwachung und Warnmeldungen für fehlgeschlagene Übertragungen.

Richten Sie automatische Wiederholungsversuche für fehlgeschlagene Übertragungen ein.

Leistung

Wählen Sie die geeigneten Instance-Typen für Ihr Übertragungsvolumen aus.

Implementieren Sie S3-Lebenszyklusrichtlinien für effizientes Dateimanagement.

Überwachen und optimieren Sie Netzwerkkonfigurationen.

Kostenoptimierung

Verwenden Sie die auto-scaling für variable Workloads.

Implementieren Sie S3-Speicherklassen für ältere Dateien.

Überwachen und passen Sie die Ressourcen an die tatsächliche Nutzung an.

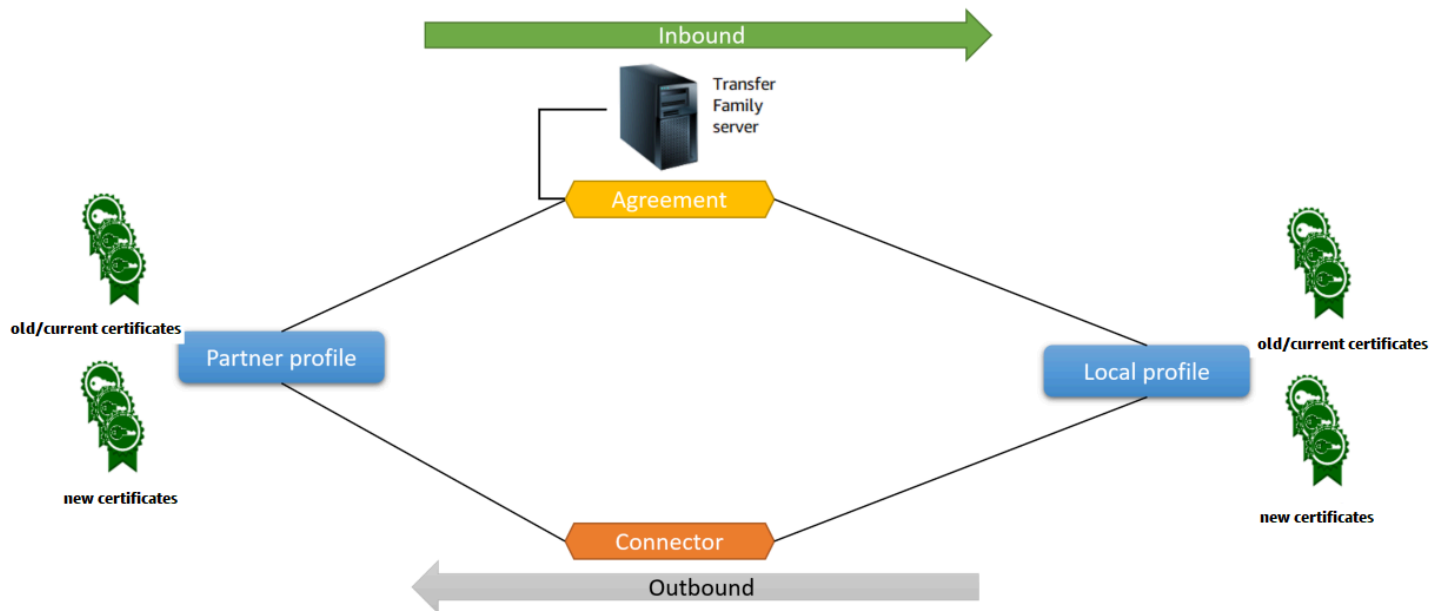
AS2 konfigurieren

Um einen AS2-enabled Server zu erstellen, müssen Sie außerdem die folgenden Komponenten angeben:

- **Abkommen** — Bilaterale Handelspartnerabkommen oder Partnerschaften definieren die Beziehung zwischen den beiden Parteien, die Nachrichten (Dateien) austauschen. Um eine Vereinbarung zu definieren, kombiniert Transfer Family Server-, lokale Profil-, Partnerprofil- und Zertifikatsinformationen. Transfer Family AS2-inbound Familienprozesse verwenden Vereinbarungen.
- **Zertifikate** — Public-Key-Zertifikate (X.509) werden in der AS2-Kommunikation zur Nachrichtenverschlüsselung und -verifizierung verwendet. Zertifikate werden auch für Connector-Endpunkte verwendet.
- **Lokale Profile und Partnerprofile** — Ein lokales Profil definiert die lokale Organisation oder „Partei“ (AS2-enabled Transfer Family Family-Server). In ähnlicher Weise definiert ein Partnerprofil die Remote-Partnerorganisation außerhalb von Transfer Family.

Obwohl nicht für alle AS2-enabled Server erforderlich, benötigen Sie für ausgehende Übertragungen einen Connector. Ein Connector erfasst die Parameter für eine ausgehende Verbindung. Der Connector ist erforderlich, um Dateien an einen externen Server eines Kunden zu senden, der kein AWS Server ist.

Das folgende Diagramm zeigt die Beziehung zwischen den AS2-Objekten, die an den eingehenden und ausgehenden Prozessen beteiligt sind.



Ein umfassendes Beispiel für eine AS2-Konfiguration finden Sie unter: [Einrichtung einer AS2-Konfiguration](#)

Themen

- [AS2-Konfigurationen](#)
- [AS2-Kontingente und Einschränkungen](#)
- [Merkmale und Fähigkeiten von AS2](#)

AS2-Konfigurationen

In diesem Thema werden die unterstützten Konfigurationen, Funktionen und Funktionen für Übertragungen beschrieben, die das AS2-Protokoll (Applicability Statement 2) verwenden, einschließlich der akzeptierten Chiffren und Digests.

Signierung, Verschlüsselung, Komprimierung, MDN

Sowohl für eingehende als auch für ausgehende Übertragungen sind die folgenden Elemente entweder erforderlich oder optional:

- Verschlüsselung — Erforderlich (für HTTP-Transport, die einzige derzeit unterstützte Transportmethode). Unverschlüsselte Nachrichten werden nur akzeptiert, wenn sie von einem TLS-

terminating Proxy wie einem Application Load Balancer (ALB) weitergeleitet werden und der X-Forwarded-Proto: https Header vorhanden ist.

- Signieren — optional
- Komprimierung — Optional (der einzige derzeit unterstützte Komprimierungsalgorithmus ist ZLIB)
- Hinweis zur Disposition von Nachrichten (MDN) — Optional

Chiffren

Die folgenden Verschlüsselungen werden sowohl für eingehende als auch für ausgehende Übertragungen unterstützt:

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES (nur aus Gründen der Abwärtskompatibilität)

Übersichten

Die folgenden Digests werden unterstützt:

- Eingehendes Signieren und MDN — SHA1, SHA256, SHA384, SHA512
- Ausgehendes Signieren und MDN — SHA1, SHA256, SHA384, SHA512

MDN

Für MDN-Antworten werden bestimmte Typen wie folgt unterstützt:

- Eingehende Übertragungen — Synchron und asynchron
- Ausgehende Übertragungen — Synchron und asynchron
- Simple Mail Transfer Protocol (SMTP) (E-Mail MDN) — Nicht unterstützt

Transporte

- Eingehende Übertragungen — HTTP ist der einzige derzeit unterstützte Transport, und Sie müssen ihn explizit angeben.

Note

Wenn Sie HTTPS für eingehende Übertragungen verwenden müssen, können Sie TLS auf einem Application Load Balancer oder einem Network Load Balancer beenden. Dieser Vorgang wird unter [Empfangen Sie AS2-Nachrichten über HTTPS](#) beschrieben.

- **Ausgehende Übertragungen** — Wenn Sie eine HTTP-URL angeben, müssen Sie auch einen Verschlüsselungsalgorithmus angeben. Wenn Sie eine HTTPS-URL angeben, haben Sie die Möglichkeit, NONE für Ihren Verschlüsselungsalgorithmus anzugeben.

AS2-Kontingente und Einschränkungen

In diesem Abschnitt werden Kontingente und Einschränkungen für AS2 beschrieben

Themen

- [AS2-Kontingente](#)
- [Kontingente für den Umgang mit Geheimnissen](#)
- [Bekannte Beschränkungen](#)

AS2-Kontingente

Die folgenden Kontingente gelten für AS2-Dateiübertragungen. Informationen zur Beantragung einer Erhöhung für ein anpassbares Kontingent finden Sie unter [AWS-Service Kontingente](#) im Allgemeine AWS-Referenz.

AS2-Kontingente

Name	Standard	Anpassbar
Maximale Anzahl von Dateien pro ausgehender Anfrage	10	Nein
Maximale Anzahl ausgehender Anfragen pro Sekunde	100	Nein
Maximale Anzahl eingehender Anfragen pro Sekunde	100	Nein

Name	Standard	Anpassbar
Maximale ausgehende Bandbreite pro Konto (ausgehende SFTP- und AS2-Anfragen tragen beide zu diesem Wert bei)	50 MB pro Sekunde	Nein

Kontingente für den Umgang mit Geheimnissen

AWS Transfer Family ruft im Namen von AS2-Kunden AWS Secrets Manager an, die die Standardauthentifizierung verwenden. Zusätzlich ruft Secrets Manager auf AWS KMS.

Note

Diese Kontingente sind nicht spezifisch für Ihre Verwendung von Geheimnissen für Transfer Family: Sie werden von allen Diensten in Ihrem gemeinsam genutzt AWS-Konto.

Für Secrets Manager `GetSecretValue` gilt das Kontingent Kombinierte Rate von Anfragen `DescribeSecret` und `GetSecretValue` API-Anfragen, wie unter [AWS Secrets Manager Kontingente](#) beschrieben.

Secrets Manager **GetSecretValue**

Name	Wert	Description
Kombinierte Rate von <code>DescribeSecret</code> und <code>GetSecretValue</code> API-Anfragen	Jede unterstützte Region: 10 000 pro Sekunde	Die maximale Anzahl an Transaktionen pro Sekunde für <code>DescribeSecret</code> <code>GetSecretValue</code> API-Operationen zusammen.

Für gelten AWS KMS die folgenden Kontingente für `Decrypt`. Einzelheiten finden Sie unter [Kontingente für jeden AWS KMS API-Vorgang anfordern](#)

AWS KMS **Decrypt**

Kontingentsname	Standardwert (Anforderungen pro Sekunde)
Anforderungsrate für kryptografische Operationen (symmetrisch)	Diese gemeinsamen Kontingente variieren je nach dem AWS-Region und der Art des in der Anfrage verwendeten AWS KMS Schlüssels. Jedes Kontingent wird separat berechnet. • 5 500 (freigegeben) • 10 000 (gemeinsam) in den folgenden Regionen: • USA Ost (Ohio), us-east-2 • Asien-Pazifik (Singapur), ap-southeast-1 • Asien-Pazifik (Sydney), ap-southeast-2 • Asien-Pazifik (Tokio), ap-northeast-1 • Europa (Frankfurt) eu-central-1 • Europa (London) eu-west-2 • 50 000 (gemeinsam) in den folgenden Regionen: • USA Ost (Nord-Virginia), us-east-1 • USA West (Oregon), us-west-2 • Europa (Irland), eu-west-1
Anforderungskontingente für benutzerdefinierte Schlüsselspeicher  Note Dieses Kontingent gilt nur, wenn Sie einen externen Schlüsselspeicher verwenden.	Kontingente für benutzerdefinierte Schlüsselspeicher-Anfragen werden für jeden benutzerdefinierten Schlüsselspeicher separat berechnet. • 1.800 (gemeinsam genutzt) für jeden AWS CloudHSM Schlüsselspeicher • 1 800 (freigegeben) für jeden externen Schlüsselspeicher.

Bekannte Beschränkungen

- Server-side TCP-Keep-Alive wird nicht unterstützt. Die Verbindung wird nach 350 Sekunden Inaktivität unterbrochen, es sei denn, der Client sendet Keep-Alive-Pakete.
- Damit eine aktive Vereinbarung vom Service akzeptiert wird und in den CloudWatch Amazon-Protokollen erscheint, müssen Nachrichten gültige AS2-Header enthalten.
- [Der Server, der Nachrichten AWS Transfer Family für AS2 empfängt, muss das Schutzattribut des Algorithmus Cryptographic Message Syntax \(CMS\) zur Validierung von Nachrichtensignaturen unterstützen, wie in RFC 6211 definiert.](#) Dieses Attribut wird in einigen älteren IBM Sterling-Produkten nicht unterstützt.
- Doppelte Nachrichten-IDs führen zu einer processed/Warning: Nachricht mit doppeltem Dokument.
- Die Schlüssellänge für AS2-Zertifikate muss mindestens 2048 Bit und höchstens 4096 Bit betragen.
- Wenn AS2-Nachrichten oder asynchrone mDNS an den HTTPS-Endpunkt eines Handelspartners gesendet werden, müssen die Nachrichten oder mDNS ein gültiges SSL-Zertifikat verwenden, das von einer öffentlich vertrauenswürdigen Zertifizierungsstelle (CA) signiert ist. Self-signed Zertifikate werden derzeit nur für ausgehende Übertragungen unterstützt.
- Der Endpunkt muss das TLS-Protokoll der Version 1.2 und einen kryptografischen Algorithmus unterstützen, der gemäß der Sicherheitsrichtlinie zulässig ist (wie unter beschrieben).
[Sicherheitsrichtlinien für Server AWS Transfer Family](#)
- Mehrere Anlagen und Certificate Exchange Messaging (CEM) aus AS2 Version 1.2 werden derzeit nicht unterstützt.
- Die Standardauthentifizierung wird derzeit nur für ausgehende Nachrichten unterstützt.
- Sie können einen Dateiverarbeitungs-Workflow an einen Transfer Family Family-Server anhängen, der das AS2-Protokoll verwendet. AS2-Nachrichten führen jedoch keine Workflows aus, die an den Server angehängt sind.

Merkmale und Fähigkeiten von AS2

In den folgenden Tabellen sind die Funktionen und Fähigkeiten aufgeführt, die für Transfer Family Family-Ressourcen verfügbar sind, die AS2 verwenden.

AS2-Funktionen

Transfer Family bietet die folgenden Funktionen für AS2.

Feature	Unterstützt von AWS Transfer Family
Drummond-Zertifizierung	Ja
AWS CloudFormation Unterstützung	Ja
CloudWatchAmazon-Metriken	Ja
SHA-2 kryptografische Algorithmen	Ja
Support für Amazon S3	Ja
Support für Amazon EFS	Nein
Geplante Nachrichten	Ja ¹
AWS Transfer Family Verwaltete Workflows	Nein
Zertifikatsaustausch-Messaging (CEM)	Nein
Gegenseitiges TLS (mTLS)	Nein
Support für selbstsignierte Zertifikate	Ja

1. Ausgehende geplante Nachrichten sind [über AWS Lambda Planungsfunktionen](#) von Amazon verfügbar EventBridge

AS2-Sende- und Empfangsfunktionen

Die folgende Tabelle enthält eine Liste der AWS Transfer Family AS2-Sende- und Empfangsfunktionen.

Funktion	Eingehend: Empfang mit dem Server	Ausgehend: Senden mit Connector
TLS-verschlüsselter Transport (HTTPS)	Ja ¹	Ja
Non-TLS Verkehr (HTTP)	Ja	Ja ²

Funktion	Eingehend: Empfang mit dem Server	Ausgehend: Senden mit Connector
Synchrones MDN	Ja	Ja
Komprimierung von Nachrichten	Ja	Ja
Asynchrones MDN	Ja	Ja
Statische IP-Adresse	Ja	Ja
Bringen Sie Ihre eigene IP-Adresse mit	Ja	Nein
Mehrere Dateianhänge	Nein	Nein
Gggrundlegende Authentifizierung	Nein	Ja
AS2 neu starten	Nicht zutreffend	Nein
AS2-Zuverlässigkeit	Nein	Nein
Benutzerdefinierter Betreff pro Nachricht	Nicht zutreffend	Nein

1. Eingehender TLS-verschlüsselter Transport mit Network Load Balancer (NLB) oder Application Load Balancer (ALB) verfügbar

2. Ausgehender Transport ohne TLS ist nur verfügbar, wenn die Verschlüsselung aktiviert ist

AS2-Zertifikate verwalten

In diesem Thema wird beschrieben, wie AS2-Zertifikate importiert und verwaltet werden. Das Importieren von Zertifikaten ist der erste Schritt im AS2-Prozess für Transfer Family.

1. Importieren des Zertifikats

2. [Erstellen Sie AS2-Profile](#)

3. [Erstellen Sie einen AS2-Server](#)
4. [Erstellen Sie eine AS2-Vereinbarung](#)
5. [Konfigurieren Sie AS2-Konnektoren](#)

AS2-Zertifikate importieren

Der Transfer Family AS2-Prozess verwendet Zertifikatsschlüssel sowohl für die Verschlüsselung als auch für die Signierung der übertragenen Informationen. Partner können für beide Zwecke denselben Schlüssel oder für jeden einen separaten Schlüssel verwenden. Wenn Sie über gemeinsame Verschlüsselungsschlüssel verfügen, die von einem vertrauenswürdigen Drittanbieter treuhänderisch aufbewahrt werden, sodass Daten im Notfall oder bei einer Sicherheitsverletzung entschlüsselt werden können, empfehlen wir, separate Signaturschlüssel zu verwenden. Durch die Verwendung separater Signaturschlüssel (die Sie nicht hinterlegen) gefährden Sie nicht die Funktionen Ihrer digitalen Signaturen, die nicht zurückgewiesen werden können.

Note

Die Schlüssellänge für AS2-Zertifikate muss mindestens 2048 Bit und höchstens 4096 Bit betragen.

In den folgenden Punkten wird detailliert beschrieben, wie AS2-Zertifikate während des Prozesses verwendet werden.

- **Eingehend AS2**
 - Der Handelspartner sendet seinen öffentlichen Schlüssel für das Signaturzertifikat, und dieser Schlüssel wird in das Partnerprofil importiert.
 - Die lokale Partei sendet den öffentlichen Schlüssel für ihre Verschlüsselungs- und Signaturzertifikate. Der Partner importiert dann den oder die privaten Schlüssel. Die lokale Partei kann separate Zertifikatsschlüssel zum Signieren und Verschlüsseln senden oder denselben Schlüssel für beide Zwecke verwenden.
- **Ausgehender AS2**
 - Der Partner sendet den öffentlichen Schlüssel für sein Verschlüsselungszertifikat, und dieser Schlüssel wird in das Partnerprofil importiert.
 - Die lokale Partei sendet den öffentlichen Schlüssel für das Zertifikat zum Signieren und importiert den privaten Schlüssel des Zertifikats zum Signieren.

- Wenn Sie HTTPS verwenden, können Sie ein selbstsigniertes Transport Layer Security (TLS) - Zertifikat importieren.

Einzelheiten zum Erstellen von Zertifikaten finden Sie unter [the section called “Schritt 1: Zertifikate für AS2 erstellen”](#).

In diesem Verfahren wird erklärt, wie Zertifikate mithilfe der Transfer Family Family-Konsole importiert werden. Wenn Sie AWS CLI stattdessen das verwenden möchten, finden Sie weitere Informationen unter [the section called “Schritt 2: Zertifikate als Transfer Family Family-Zertifikatsressourcen importieren”](#).

So geben Sie ein AS2-enabled Zertifikat an

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich unter AS2 Trading Partners die Option Certificates aus.
3. Wählen Sie Import certificate (Zertifikat importieren).
4. Geben Sie im Abschnitt Zertifikatkonfiguration unter Beschreibung des Zertifikats einen leicht identifizierbaren Namen für das Zertifikat ein. Stellen Sie sicher, dass Sie den Zweck des Zertifikats anhand seiner Beschreibung identifizieren können. Wählen Sie außerdem die Rolle für das Zertifikat aus.
5. Wählen Sie im Abschnitt Verwendung des Zertifikats den Zweck für dieses Zertifikat aus. Es kann zur Verschlüsselung, Signierung oder für beides verwendet werden.

Tipp: Wenn Sie Verschlüsselung und Signierung für die Verwendung wählen, erstellt Transfer Family zwei identische Zertifikate (jedes hat seine eigene ID): eines mit einem Nutzungswert von ENCRYPTION und eines mit einem Nutzungswert von SIGNING.

6. Geben Sie im Abschnitt Inhalt des Zertifikats ein öffentliches Zertifikat eines Handelspartners oder die öffentlichen und privaten Schlüssel für ein lokales Zertifikat an.

Füllen Sie den Abschnitt Inhalt des Zertifikats mit den entsprechenden Details aus.

- Wenn Sie sich für Self-signed ein Zertifikat entscheiden, geben Sie die Zertifikatskette nicht an.
- Fügen Sie den Zertifikatstext und die Kette in das Feld Zertifikat und Zertifikatskette ein.
- Wenn es sich bei diesem Zertifikat um ein lokales Zertifikat handelt, fügen Sie seinen privaten Schlüssel ein.

7. Wählen Sie Zertifikat importieren, um den Vorgang abzuschließen und die Details für das importierte Zertifikat zu speichern.

Note

TLS-Zertifikate können nur als öffentliches Zertifikat eines Partners importiert werden. Wenn Sie Öffentliches Zertifikat von einem Partner und dann Transport Layer Security (TLS) für die Verwendung auswählen, erhalten Sie eine Warnung. Außerdem müssen TLS-Zertifikate selbstsigniert sein (d. h. Sie müssen Self Signed Certificate auswählen, um ein TLS-Zertifikat zu importieren).

Rotation der AS2-Zertifikate

Oft sind Zertifikate für einen Zeitraum von sechs Monaten bis zu einem Jahr gültig. Möglicherweise haben Sie Profile eingerichtet, die Sie für einen längeren Zeitraum beibehalten möchten. Um dies zu erleichtern, bietet Transfer Family eine Zertifikatsrotation. Sie können mehrere Zertifikate für ein Profil angeben, sodass Sie das Profil mehrere Jahre lang verwenden können. Transfer Family verwendet Zertifikate zum Signieren (optional) und Verschlüsseln (verpflichtend). Sie können ein einzelnes Zertifikat für beide Zwecke angeben, wenn Sie möchten.

Bei der Zertifikatsrotation wird ein altes, ablaufendes Zertifikat durch ein neueres Zertifikat ersetzt. Die Umstellung erfolgt schrittweise, um zu vermeiden, dass Übertragungen unterbrochen werden, wenn ein Vertragspartner noch kein neues Zertifikat für ausgehende Übertragungen konfiguriert hat oder während eines Zeitraums, in dem möglicherweise auch ein neueres Zertifikat verwendet wird, Payloads sendet, die mit einem alten Zertifikat signiert oder verschlüsselt sind. Die Zwischenzeit, in der sowohl alte als auch neue Zertifikate gültig sind, wird als Karenzzeit bezeichnet.

X.509 Zertifikate haben `Not Before` ein `Not After` Datum. Diese Parameter bieten Administratoren jedoch möglicherweise nicht genügend Kontrolle. Transfer Family bietet `Active Date` `Inactive Date` Einstellungen, mit denen gesteuert werden kann, welches Zertifikat für ausgehende Payloads verwendet und welches für eingehende Payloads akzeptiert wird.

Überwachung des Ablaufs von Zertifikaten

Transfer Family veröffentlicht `DaysUntilExpiry` nach dem Import eines Zertifikats eine CloudWatch Amazon-Metrik. Die Metrik gibt die Anzahl der Tage zwischen dem aktuellen Datum und

dem `InactiveDate` auf dem Zertifikat angegebenen Datum aus. Die Metrik befindet sich unter dem `Transfer AWS Namespace` im CloudWatch Metrik-Dashboard.

Diese Metrik hat immer eine Metrikdimension für `CertificateId` und enthält optional eine Beschreibungsdimension, sofern sie vom Kunden auf dem Zertifikat angegeben wird. Weitere Informationen zu CloudWatch metrischen Dimensionen finden Sie unter [Dimension](#) in der CloudWatch API-Referenz.

 Note

Nach dem Import eines Zertifikats für Transfer Family kann es bis zu einem ganzen Tag dauern, bis diese Metrik an das Kundenkonto gesendet wird.

Sie können diese Metrik verwenden, um CloudWatch Alarme zu erstellen, die Sie benachrichtigen, wenn Zertifikate bald ablaufen.

Bei der Auswahl ausgehender Zertifikate wird der Höchstwert verwendet, der vor dem Datum der Übertragung liegt. `Inactive Date` Eingehende Prozesse akzeptieren Zertifikate im Bereich von `Not Before` `Not After` und `und`. `Active Date` `Inactive Date`

Beispiel für die Zertifikatsrotation

In der folgenden Tabelle wird eine Möglichkeit beschrieben, zwei Zertifikate für ein einzelnes Profil zu konfigurieren.

Zwei Zertifikate im Wechsel

Name	NOT BEFORE(wird von der Zertifizierungsstelle kontrolliert)	ACTIVE DATE(gesetzt von Transfer Family)	INACTIVE DATE(gesetzt von Transfer Family)	NOT AFTER(von der Zertifizierungsstelle festgelegt)
Cert1 (älteres Zertifikat)	2019-11-01	01.01.2020	31.12.2020	2024-01-01
Cert2 (neueres Zertifikat)	01.11.2020	2020-06-01	01.06.2021	01.01.2025

Beachten Sie Folgendes:

- Wenn Sie ein `Active Date` und `Inactive Date` für ein Zertifikat angeben, muss der Bereich innerhalb des Bereichs zwischen und liegen. `Not Before` `Not After`
- Es wird empfohlen, mehrere Zertifikate für jedes Profil zu konfigurieren und dabei sicherzustellen, dass der aktive Datumsbereich für alle Zertifikate zusammen den Zeitraum abdeckt, für den Sie das Profil verwenden möchten.
- Wir empfehlen Ihnen, eine Übergangszeit zwischen dem Zeitpunkt, zu dem Ihr älteres Zertifikat inaktiv wird, und dem Zeitpunkt, zu dem Ihr neueres Zertifikat aktiv wird, festzulegen. Im vorherigen Beispiel wird das erste Zertifikat erst am 31.12.2020 inaktiv, während das zweite Zertifikat am 01.06.2020 aktiv wird, was eine Kulanzzeit von 6 Monaten bietet. Im Zeitraum vom 01.06.2020 bis 31.12.2020 sind beide Zertifikate aktiv.

Erstellen Sie AS2-Profil

In diesem Thema wird beschrieben, wie Profile für den AS2-Prozess erstellt werden. Ein lokales Profil definiert die lokale Organisation oder „Partei“ (AS2-enabledTransfer Family Server). In ähnlicher Weise definiert ein Partnerprofil die Remote-Partnerorganisation außerhalb von Transfer Family.

1. [AS2-Zertifikate importieren](#)
2. AS2-Profil erstellen
3. [Erstellen Sie einen AS2-Server](#)
4. [Erstellen Sie eine AS2-Vereinbarung](#)
5. [Konfigurieren Sie AS2-Konnektoren](#)

Gehen Sie wie folgt vor, um sowohl lokale Profile als auch Partnerprofile zu erstellen. In diesem Verfahren wird erklärt, wie AS2-Profil mithilfe der Transfer Family Family-Konsole erstellt werden. Wenn Sie AWS CLI stattdessen das verwenden möchten, finden Sie weitere Informationen unter [the section called “Schritt 3: Erstellen Sie Profile für Sie und Ihren Handelspartner”](#).

So erstellen Sie ein AS2-Profil

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich unter AS2 Trading Partners die Option Profile und dann Create profile aus.

3. Geben Sie im Abschnitt Profilkonfiguration die AS2-ID für das Profil ein. Dieser Wert wird für die für das AS2-Protokoll spezifischen HTTP-Header `as2-from` und `as2-to` zur Identifizierung der Handelspartnerschaft verwendet, die bestimmt, welche Zertifikate verwendet werden sollen, usw.
4. Wählen Sie im Abschnitt Profiltyp die Option Lokales Profil oder Partnerprofil aus.
5. Wählen Sie im Abschnitt Zertifikate ein oder mehrere Zertifikate aus dem Drop-down-Menü aus.

Tipp: Wenn Sie ein Zertifikat importieren möchten, das nicht im Drop-down-Menü aufgeführt ist, wählen Sie Neues Zertifikat importieren aus. Dadurch wird ein neues Browserfenster auf dem Bildschirm Zertifikat importieren geöffnet. Informationen zum Importieren von Zertifikaten finden Sie unter [AS2-Zertifikate importieren](#).

6. (Optional) Geben Sie im Abschnitt Tags ein oder mehrere Schlüssel-Wert-Paare an, um dieses Profil leichter identifizieren zu können.
7. Wählen Sie Profil erstellen, um den Vorgang abzuschließen und das neue Profil zu speichern.

Erstellen Sie einen AS2-Server

Dieses Thema enthält Anweisungen zum Erstellen eines AS2-enabled Transfer Family Family-Servers mithilfe der Konsole oder einer CloudFormation Vorlage. Ein umfassendes Beispiel für eine AS2-Konfiguration finden Sie unter [Einrichtung einer AS2-Konfiguration](#). Nachdem Sie einen AS2-Server erstellt haben, können Sie dem Server eine Vereinbarung hinzufügen.

1. [AS2-Zertifikate importieren](#)
2. [Erstellen Sie AS2-Profile](#)
3. Erstellen Sie einen AS2-Server
4. [Erstellen Sie eine AS2-Vereinbarung](#)
5. [Konfigurieren Sie AS2-Konnektoren](#)

Themen

- [Erstellen Sie einen AS2-Server mit der Transfer Family Family-Konsole](#)
- [Verwenden Sie eine Vorlage, um einen Demo-Stack der Transfer Family AS2 zu erstellen](#)
- [Erstellen Sie eine AS2-Vereinbarung](#)

Erstellen Sie einen AS2-Server mit der Transfer Family Family-Konsole

In diesem Verfahren wird erklärt, wie Sie mithilfe der Transfer Family Family-Konsole einen AS2-enabled Server erstellen. Wenn Sie AWS CLI stattdessen verwenden möchten, finden Sie weitere Informationen unter [the section called “Schritt 4: Erstellen Sie einen Transfer Family Family-Server, der das AS2-Protokoll verwendet”](#).

Note

Sie können einen Dateiverarbeitungs-Workflow an einen Transfer Family Family-Server anhängen, der das AS2-Protokoll verwendet. AS2-Nachrichten führen jedoch keine Workflows aus, die an den Server angehängt sind.

Um einen Server zu erstellen AS2-enabled

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann Server erstellen aus.
3. Wählen Sie auf der Seite „Protokolle auswählen“ die Option AS2 (Applicability Statement 2) und dann Weiter aus.
4. Wählen Sie auf der Seite „Identitätsanbieter auswählen“ die Option Weiter aus.

Note

Für AS2 können Sie keinen Identitätsanbieter auswählen, da die Standardauthentifizierung für das AS2-Protokoll nicht unterstützt wird. Stattdessen kontrollieren Sie den Zugriff über Virtual Private Cloud (VPC) -Sicherheitsgruppen.

5. Gehen Sie auf der Seite „Endpunkt auswählen“ wie folgt vor:

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

- a. Wählen Sie als Endpunkttyp die Option VPC Hosted aus, um den Endpunkt Ihres Servers zu hosten. Informationen zur Einrichtung Ihres VPC-hosted Endpunkts finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).

 Note

Öffentlich zugängliche Endpunkte werden für das AS2-Protokoll nicht unterstützt. Um Ihren VPC-Endpunkt über das Internet zugänglich zu machen, wählen Sie Internet Facing unter Access und geben Sie dann Ihre Elastic IP-Adressen ein.

- b. Wählen Sie für Access eine der folgenden Optionen:

- Intern — Wählen Sie diese Option, um den Zugriff von Ihrer VPC und Ihren VPC-connected Umgebungen aus zu ermöglichen, z. B. über ein lokales Rechenzentrum Direct Connect oder VPN.
- Internet Facing — Wählen Sie diese Option, um den Zugriff über das Internet und von Ihrer VPC und Ihren VPC-connected Umgebungen aus zu ermöglichen, z. B. über ein lokales Rechenzentrum Direct Connect oder VPN.

Wenn Sie sich für Internet Facing entscheiden, geben Sie Ihre Elastic IP-Adressen ein, wenn Sie dazu aufgefordert werden.

- c. Wählen Sie für VPC entweder eine vorhandene VPC aus oder wählen Sie Create VPC, um eine neue VPC zu erstellen.
- d. Lassen Sie für FIPS Enabled das Kontrollkästchen FIPS Enabled Endpoint deaktiviert.

 Note

FIPS-enabled Endpunkte werden für das AS2-Protokoll nicht unterstützt.

- e. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite „Domain auswählen“ Amazon S3 aus, um Ihre Dateien mithilfe des ausgewählten Protokolls als Objekte zu speichern und darauf zuzugreifen.

Wählen Sie Weiter aus.

7. Wählen Sie auf der Seite Zusätzliche Details konfigurieren die Einstellungen aus, die Sie benötigen.

 Note

Wenn Sie zusammen mit AS2 weitere Protokolle konfigurieren, gelten alle zusätzlichen Detaileinstellungen. Für das AS2-Protokoll gelten jedoch nur die Einstellungen in den Abschnitten CloudWatch Protokollierung und Tags.

Auch wenn die Einrichtung einer CloudWatch Protokollierungsrolle optional ist, empfehlen wir dringend, sie so einzurichten, dass Sie den Status Ihrer Nachrichten einsehen und Konfigurationsprobleme beheben können.

8. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Einstellungen, um sicherzustellen, dass sie korrekt sind.

- Wenn Sie eine Ihrer Einstellungen bearbeiten möchten, wählen Sie neben dem Schritt, den Sie ändern möchten, die Option Bearbeiten aus.

 Note

Wenn Sie einen Schritt bearbeiten, empfehlen wir Ihnen, jeden Schritt nach dem Schritt, den Sie bearbeiten möchten, zu überprüfen.

- Wenn Sie keine Änderungen vorgenommen haben, wählen Sie Server erstellen, um Ihren Server zu erstellen. Sie gelangen zur Seite Servers (Server) (siehe unten), auf der der neue Server aufgelistet ist.

Es kann mehrere Minuten dauern, bis sich der Status Ihres neuen Servers auf Online ändert. Ab diesem Zeitpunkt kann der Server Dateioperationen für die Benutzer ausführen.

Verwenden Sie eine Vorlage, um einen Demo-Stack der Transfer Family AS2 zu erstellen

Wir liefern eine eigenständige CloudFormation Vorlage, mit der Sie schnell einen AS2-enabled Transfer Family Family-Server erstellen können. Die Vorlage konfiguriert den Server mit einem öffentlichen Amazon VPC-Endpunkt, Zertifikaten, lokalen Profilen und Partnerprofilen, einer Vereinbarung und einem Connector.

Die grundlegende AS2-Servervorlage erstellt die folgenden Ressourcen:

- Ein AS2-enabled Transfer Family Family-Server mit einem VPC-Endpunkt
- Lokale AS2-Profilen und Partner-AS2-Profilen mit Zertifikaten
- Eine Vereinbarung zwischen den Profilen
- Ein Amazon S3 S3-Bucket für die Dateispeicherung
- Erforderliche IAM-Rollen und -Richtlinien
- CloudWatch Konfiguration der Protokollierung

Bevor Sie diese Vorlage verwenden, sollten Sie Folgendes beachten:

- Wenn Sie anhand dieser Vorlage einen Stack erstellen, werden Ihnen die verwendeten AWS Ressourcen in Rechnung gestellt.

- Die Vorlage erstellt mehrere Zertifikate und platziert sie AWS Secrets Manager , um sie sicher zu speichern. Sie können diese Zertifikate bei Bedarf aus Secrets Manager löschen, da Ihnen die Nutzung dieses Dienstes in Rechnung gestellt wird. Durch das Löschen dieser Zertifikate in Secrets Manager werden sie nicht vom Transfer Family Family-Server gelöscht. Daher wird die Funktionalität des Demo-Stacks nicht beeinträchtigt. Für Zertifikate, die Sie mit einem AS2-Produktionsserver verwenden möchten, möchten Sie jedoch möglicherweise Secrets Manager verwenden, um Ihre gespeicherten Zertifikate zu verwalten und regelmäßig zu rotieren.
- Wir empfehlen, die Vorlage nur als Grundlage und hauptsächlich zu Demonstrationszwecken zu verwenden. Wenn Sie diesen Demo-Stack in der Produktion verwenden möchten, empfehlen wir Ihnen, den YAML-Code der Vorlage zu ändern, um einen robusteren Stack zu erstellen. Erstellen Sie beispielsweise Zertifikate auf Produktionsebene und erstellen Sie eine AWS Lambda Funktion, die Sie in der Produktion verwenden können.

So erstellen Sie einen AS2-enabled Transfer Family Family-Server aus einer CloudFormation Vorlage

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Wählen Sie im linken Navigationsbereich Stack aus.
3. Wählen Sie Create stack (Stack erstellen) und dann With new resources (standard) (Mit neuen Ressourcen (Standard)).
4. Wählen Sie im Abschnitt Voraussetzung — Vorlage vorbereiten die Option Vorhandene Vorlage auswählen aus.
5. Kopieren Sie diesen Link, die [AS2-Demo-Vorlage](#), und fügen Sie ihn in das Amazon S3 S3-URL-Feld ein.
6. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite „Stack-Details angeben“ Ihrem Stack einen Namen und geben Sie dann die folgenden Parameter an:
 - Geben Sie unter AS2 Werte für Lokale AS2-ID und Partner-AS2-ID ein, oder akzeptieren Sie die Standardwerte und. `local partner`
 - Geben Sie unter Netzwerk einen Wert für die CIDR-IP des Sicherheitsgruppeneingangs ein, oder akzeptieren Sie die Standardeinstellung. `0.0.0.0/0`

 Note

Dieser Wert im CIDR-Format gibt an, welche IP-Adressen für eingehenden Datenverkehr zum AS2-Server zulässig sind. Der Standardwert, `0.0.0.0/0`, erlaubt alle IP-Adressen.

- Geben Sie unter Allgemein einen Wert für Präfix ein, oder akzeptieren Sie den Standardwert `transfer-as2`. Dieses Präfix steht vor allen Ressourcennamen, die vom Stack erstellt werden. Wenn Sie beispielsweise das Standardpräfix verwenden, wird Ihr Amazon S3 S3-Bucket benannt `transfer-as2-amzn-s3-demo-bucket`.
8. Wählen Sie Weiter aus. Wählen Sie auf der Seite „Stack-Optionen konfigurieren“ erneut Weiter aus.
 9. Überprüfen Sie die Details für den Stack, den Sie gerade erstellen, und wählen Sie dann Stapel erstellen aus.

 Note

Unten auf der Seite müssen Sie unter Funktionen angeben, dass dadurch CloudFormation möglicherweise Ressourcen AWS Identity and Access Management (IAM) erstellt werden.

Nachdem der Stack erstellt wurde, können Sie mithilfe von AWS Command Line Interface (AWS CLI) eine AS2-Testnachricht vom Partnerserver an Ihren lokalen Transfer Family Family-Server senden. Ein AWS CLI Beispielfehl zum Senden einer Testnachricht wird zusammen mit allen anderen Ressourcen im Stack erstellt.

Um diesen Beispielfehl zu verwenden, wechseln Sie zur Registerkarte Ausgaben Ihres Stacks und kopieren Sie den `TransferExampleAs2Command`. Sie können den Befehl dann mit dem ausführen AWS CLI. Falls Sie das noch nicht installiert haben AWS CLI, finden Sie weitere Informationen unter [Installieren oder Aktualisieren der neuesten Version von AWS CLI](#) im AWS Command Line Interface Benutzerhandbuch.

Der Beispielfehl hat das folgende Format:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

Ihre Version dieses Befehls enthält die tatsächlichen Werte für die *TransferConnectorId* Ressourcen *amzn-s3-demo-bucket* und in Ihrem Stack.

Dieser Beispielbefehl besteht aus zwei separaten Befehlen, die mithilfe der && Zeichenfolge miteinander verkettet sind.

Der erste Befehl erstellt eine neue, leere Textdatei in Ihrem Bucket:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt
```

Dann verwendet der zweite Befehl den Connector, um die Datei vom Partnerprofil an das lokale Profil zu senden. Auf dem Transfer Family Family-Server wurde eine Vereinbarung eingerichtet, die es dem lokalen Profil ermöglicht, Nachrichten vom Partnerprofil anzunehmen.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

Nachdem Sie den Befehl ausgeführt haben, können Sie zu Ihrem Amazon S3 S3-Bucket (*amzn-s3-demo-bucket*) wechseln und den Inhalt anzeigen. Wenn der Befehl erfolgreich ist, sollten Sie die folgenden Objekte in Ihrem Bucket sehen:

- *processed/*— Dieser Ordner enthält eine JSON-Datei, die die übertragene Datei und die MDN-Antwort beschreibt.
- *processing/*— Dieser Ordner enthält vorübergehend Dateien, während sie verarbeitet werden. Nach Abschluss einer Übertragung sollte dieser Ordner jedoch leer sein.
- *server-id/*— Dieser Ordner ist nach Ihrer Transfer Family Family-Server-ID benannt. Er enthält *from-partner* (dieser Ordner wird dynamisch benannt, basierend auf der AS2-ID des Partners), der wiederum *processing/* Ordner *failed/processed/*, und enthält. Der */server-id/from-partner/processed/* Ordner enthält eine Kopie der übertragenen Textdatei und die entsprechenden JSON- und MDN-Dateien.

- `test.txt`— Dieses Objekt ist die (leere) Datei, die übertragen wurde.

Erstellen Sie eine AS2-Vereinbarung

Vereinbarungen sind mit Transfer Family Family-Servern verknüpft. Sie spezifizieren die Details für Geschäftspartner, die das AS2-Protokoll verwenden, um Nachrichten oder Dateien mithilfe von Transfer Family auszutauschen, für eingehende Übertragungen, d. h. das Senden von AS2-Dateien von einer externen, partnereigenen Quelle an einen Transfer Family Family-Server.

In diesem Verfahren wird erklärt, wie AS2-Vereinbarungen mithilfe der Transfer Family Family-Konsole erstellt werden. Wenn Sie AWS CLI stattdessen das verwenden möchten, finden Sie weitere Informationen unter [the section called “Schritt 5: Erstellen Sie eine Vereinbarung zwischen Ihnen und Ihrem Partner”](#).

So erstellen Sie eine Vereinbarung für einen Transfer Family Family-Server

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann einen Server aus, der das AS2-Protokoll verwendet.

Wenn Sie mindestens einen Transfer Family Family-Server haben, der das AS2-Protokoll verwendet, können Sie alternativ im Menü AS2-Handelspartner die Option Vereinbarungen zum Empfangen von Nachrichten auswählen. Wählen Sie dann im Bildschirm „Vereinbarung erstellen“ den AS2-Server aus, dem Sie diese Vereinbarung zuordnen möchten.

3. Scrollen Sie auf der Seite mit den Serverdetails nach unten zum Abschnitt Vereinbarungen.
4. Wählen Sie Vereinbarung hinzufügen aus.
5. Geben Sie die Vereinbarungsparameter wie folgt ein:
 - a. Geben Sie im Abschnitt Vereinbarungskonfiguration einen aussagekräftigen Namen ein. Stellen Sie sicher, dass Sie den Zweck der Vereinbarung anhand des Namens identifizieren können. Legen Sie außerdem den Status für die Vereinbarung fest: entweder Aktiv (standardmäßig ausgewählt) oder Inaktiv.
 - b. Wählen Sie im Abschnitt Kommunikationskonfiguration ein lokales Profil und ein Partnerprofil aus. Wählen Sie außerdem aus, ob das Signieren von Nachrichten erzwungen werden soll oder nicht.

- Standardmäßig ist Nachrichtensignierung erzwingen aktiviert, was bedeutet, dass Transfer Family unsignierte Nachrichten von Ihrem Handelspartner für diese Vereinbarung ablehnt.
 - Deaktivieren Sie diese Einstellung, damit Transfer Family unsignierte Nachrichten von Ihrem Handelspartner für diese Vereinbarung annehmen kann.
- c. Geben Sie im Abschnitt Konfiguration des Posteingangsverzeichnisses die folgenden Informationen ein.
- Stellen Sie fest, ob Sie Separate Verzeichnisse angeben auswählen möchten, um Ihre AS2-Nachrichten, MDN-Dateien und JSON-Statusdateien zu speichern.
 - Wenn Sie diese Option auswählen, geben Sie separate Speicherorte für Payload-Dateien, fehlgeschlagene Dateien, MDN-Dateien, Statusdateien und temporäre Dateien an.
 - Wenn Sie diese Option deaktivieren, werden alle AS2-Dateien an den Speicherort verschoben, den Sie für Ihr Basisverzeichnis angegeben haben.
 - Wählen Sie für S3 Bucket einen Amazon S3 S3-Bucket aus.
 - Als Präfix können Sie ein Präfix (Ordner) eingeben, das zum Speichern von Dateien im Bucket verwendet werden soll.
- Wenn Sie beispielsweise für Ihren Bucket und **amzn-s3-demo-bucket incoming** für Ihr Präfix eingeben, werden Ihre AS2-Dateien in dem **/amzn-s3-demo-bucket/incoming** Ordner gespeichert.
- Wählen Sie für AWS IAM-Rolle eine Rolle aus, die auf den von Ihnen angegebenen Bucket zugreifen kann.
 - Wählen Sie für Preserve filename aus, ob die ursprünglichen Dateinamen für eingehende AS2-Nachrichten-Payloads beibehalten werden sollen.
 - Wenn Sie diese Einstellung wählen, wird der von Ihrem Handelspartner angegebene Dateiname beibehalten, wenn die Datei in Amazon S3 gespeichert wird.
 - Wenn Sie diese Einstellung deaktivieren, wird beim Speichern der Datei durch Transfer Family der Dateiname angepasst, wie unter beschrieben [Dateinamen und Speicherorte](#).
- d. (Optional) Fügen Sie im Abschnitt „Tags“ Stichwörter hinzu.
- e. Nachdem Sie alle Informationen für die Vereinbarung eingegeben haben, wählen Sie Vereinbarung erstellen aus.

Die neue Vereinbarung wird im Abschnitt Vereinbarungen der Serverdetailseite angezeigt.

Konfigurieren Sie AS2-Konnektoren

Der Zweck eines Connectors besteht darin, eine Beziehung zwischen Handelspartnern für ausgehende Übertragungen herzustellen, indem AS2-Dateien von einem Transfer Family Family-Server an ein externes, partnereigenes Ziel gesendet werden. Für den Connector geben Sie die lokale Partei, den Remote-Partner und deren Zertifikate an (indem Sie lokale Profile und Partnerprofile erstellen).

Sobald Sie einen Konnektor eingerichtet haben, können Sie Informationen an Ihre Handelspartner übertragen. Jedem AS2-Server werden drei statische IP-Adressen zugewiesen. AS2-Konnektoren verwenden diese IP-Adressen, um asynchrone mDNS über AS2 an Ihre Handelspartner zu senden.

Note

Die von einem Handelspartner empfangene Nachrichtengröße entspricht nicht der Objektgröße in Amazon S3. Diese Diskrepanz ist darauf zurückzuführen, dass die AS2-Nachricht die Datei vor dem Senden in einen Umschlag verpackt. Daher kann sich die Dateigröße erhöhen, auch wenn die Datei komprimiert gesendet wird. Stellen Sie daher sicher, dass die maximale Dateigröße des Handelspartners größer ist als die Größe der Datei, die Sie senden.

1. [AS2-Zertifikate importieren](#)
2. [Erstellen Sie AS2-Profile](#)
3. [Erstellen Sie einen AS2-Server](#)
4. [Erstellen Sie eine AS2-Vereinbarung](#)
5. Erstellen Sie einen AS2-Connector

Erstellen Sie einen AS2-Konnektor

In diesem Verfahren wird erklärt, wie AS2-Konnektoren mithilfe der AWS Transfer Family Konsole erstellt werden. Wenn Sie AWS CLI stattdessen verwenden möchten, finden Sie weitere Informationen unter [the section called “Schritt 6: Stellen Sie eine Verbindung zwischen Ihnen und Ihrem Partner her”](#).

So erstellen Sie einen AS2-Connector

1. Öffnen Sie die AWS Transfer Family Konsole unter. <https://console.aws.amazon.com/transfer/>
2. Wählen Sie im linken Navigationsbereich im Menü AS2 Trading Partners die Option Connectors zum Senden von Nachrichten aus und wählen Sie dann Create AS2 Connector aus.
3. Geben Sie im Abschnitt Connector-Konfiguration die folgenden Informationen an:
 - URL — Geben Sie die URL für ausgehende Verbindungen ein.
 - IP-Adressierungsmodus — Wählen Sie nur IPv4 (Standard), um ausschließlich IPv4-Adressen zu verwenden oder Dual-stackum sowohl IPv6 als auch IPv4 zu unterstützen. Im Dual-Stack-Modus bevorzugt der Connector IPv6, wenn die DNS-Auflösung IPv6-Ergebnisse zurückgibt, und verwendet IPv4, wenn nur IPv4-DNS-Ergebnisse zurückgegeben werden.
 - Zugriffsrolle — Wählen Sie den Amazon-Ressourcennamen (ARN) der zu AWS Identity and Access Management verwendenden (IAM) -Rolle aus. Stellen Sie sicher, dass diese Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis des Dateispeicherorts bietet, der in der `StartFileTransfer` Anfrage verwendet wird. Stellen Sie außerdem sicher, dass die Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis der Dateien bietet, die Sie mit versenden möchten `StartFileTransfer`.

Note

Wenn Sie die Standardauthentifizierung für Ihren Connector verwenden, benötigt die Zugriffsrolle die `secretsmanager:GetSecretValue` Erlaubnis für den geheimen Schlüssel. Wenn das Geheimnis mithilfe eines vom Kunden verwalteten Schlüssels anstelle von Von AWS verwalteter Schlüssel PIN verschlüsselt wird AWS Secrets Manager, benötigt die Rolle auch die `kms:Decrypt` Erlaubnis für diesen Schlüssel. Wenn Sie Ihr Geheimnis mit dem Präfix benennen `aws/transfer/`, können Sie die erforderliche Berechtigung mit einem Platzhalterzeichen (*) hinzufügen, wie im [Beispiel für eine Berechtigung zum Erstellen von Geheimnissen](#) gezeigt.

- Rolle für die Protokollierung (optional) — Wählen Sie die IAM-Rolle aus, die der Connector verwenden soll, um Ereignisse in Ihre CloudWatch Logs zu übertragen.
4. Wählen Sie im Abschnitt AS2-Konfiguration die lokalen Profile und Partnerprofile, die Verschlüsselungs- und Signierungsalgorithmen aus und legen Sie fest, ob die übertragenen Informationen komprimiert werden sollen. Beachten Sie Folgendes:
 - Der Content-Type Parameter `Preserve S3` ist standardmäßig aktiviert.

Wenn diese Option aktiviert ist, verwendet Transfer Family Amazon S3Content-Type, das Objekten in S3 zugeordnet ist, anstatt den Inhaltstyp anhand der Dateierweiterung zuzuordnen. Deaktivieren Sie diese Einstellung, wenn Sie möchten, dass der Service Ihren AS2-Nachrichten den Inhaltstyp anhand der Dateierweiterung zuordnet, anstatt den Inhaltstyp aus dem S3-Objekt zu verwenden.

- Wählen Sie für den Verschlüsselungsalgorithmus nur, DES_EDE3_CBC wenn Sie einen älteren Client unterstützen müssen, der dies erfordert, da es sich um einen schwachen Verschlüsselungsalgorithmus handelt.
- Der Betreff wird als subject HTTP-Header-Attribut in AS2-Nachrichten verwendet, die mit dem Connector gesendet werden.
- Wenn Sie einen Connector ohne Verschlüsselungsalgorithmus erstellen möchten, müssen Sie dies HTTPS als Protokoll angeben.

5. Geben Sie im Abschnitt Standardauthentifizierung die folgenden Informationen an.

- Um Anmeldeinformationen zusammen mit ausgehenden Nachrichten zu senden, wählen Sie Standardauthentifizierung aktivieren aus. Wenn Sie keine Anmeldeinformationen zusammen mit ausgehenden Nachrichten senden möchten, lassen Sie die Option Standardauthentifizierung aktivieren deaktiviert.
- Wenn Sie die Authentifizierung verwenden, wählen oder erstellen Sie ein Geheimnis.
 - Um ein neues Geheimnis zu erstellen, wählen Sie Neues Geheimnis erstellen und geben Sie dann einen Benutzernamen und ein Passwort ein. Diese Anmeldeinformationen müssen mit dem Benutzer übereinstimmen, der eine Verbindung zum Endpunkt des Partners herstellt.

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret
☐ Choose an existing secret

Username
test-user

Password

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- Um ein vorhandenes Geheimnis zu verwenden, wählen Sie „Bestehendes Geheimnis auswählen“ und wählen Sie dann ein Geheimnis aus dem Dropdownmenü aus. Einzelheiten zur Erstellung eines korrekt formatierten Secrets in Secrets Manager finden Sie unter [Aktivieren Sie die Standardauthentifizierung für AS2-Konnektoren](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret
☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

6. Geben Sie im Abschnitt MDN-Konfiguration die folgenden Informationen an:

- MDN anfordern — Sie haben die Möglichkeit, von Ihrem Handelspartner zu verlangen, dass er Ihnen eine MDN sendet, nachdem er Ihre Nachricht erfolgreich über AS2 erhalten hat.

- Signiertes MDN — Sie haben die Möglichkeit, zu verlangen, dass mDNS signiert wird. Diese Option ist nur verfügbar, wenn Sie MDN anfordern ausgewählt haben.
7. Nachdem Sie alle Ihre Einstellungen bestätigt haben, wählen Sie **Create AS2 Connector** aus, um den Connector zu erstellen.

Die Seite Connectors wird angezeigt, auf der die ID Ihres neuen Connectors zur Liste hinzugefügt wurde. Einzelheiten zu Ihren Konnektoren finden Sie unter [Details zum AS2-Konnektor anzeigen](#).

Algorithmen für AS2-Konnektoren

Wenn Sie einen AS2-Connector erstellen, werden die folgenden Sicherheitsalgorithmen an den Connector angehängt.

Typ	Algorithmus
TLS-Chiffre	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Standardauthentifizierung für AS2-Konnektoren

Wenn Sie einen Transfer Family Family-Server erstellen oder aktualisieren, der das AS2-Protokoll verwendet, können Sie die Standardauthentifizierung für ausgehende Nachrichten hinzufügen. Dazu fügen Sie einem Connector Authentifizierungsinformationen hinzu.

Note

Die Standardauthentifizierung ist nur verfügbar, wenn Sie HTTPS verwenden.

Um die Authentifizierung für Ihren Connector zu verwenden, wählen Sie im Abschnitt Standardauthentifizierung die Option Standardauthentifizierung aktivieren aus. Nachdem Sie die Standardauthentifizierung aktiviert haben, können Sie wählen, ob Sie ein neues Geheimnis erstellen oder ein vorhandenes verwenden möchten. In beiden Fällen werden die Anmeldeinformationen im Secret zusammen mit ausgehenden Nachrichten gesendet, die diesen Connector verwenden. Die Anmeldeinformationen müssen mit dem Benutzer übereinstimmen, der versucht, eine Verbindung zum Remote-Endpunkt des Handelspartners herzustellen.

Der folgende Screenshot zeigt, wie „Standardauthentifizierung aktivieren“ und „Neuen geheimen Schlüssel erstellen“ ausgewählt sind. Nachdem Sie diese Optionen getroffen haben, können Sie einen Benutzernamen und ein Passwort für das Geheimnis eingeben.

Basic authentication [Info](#)
☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

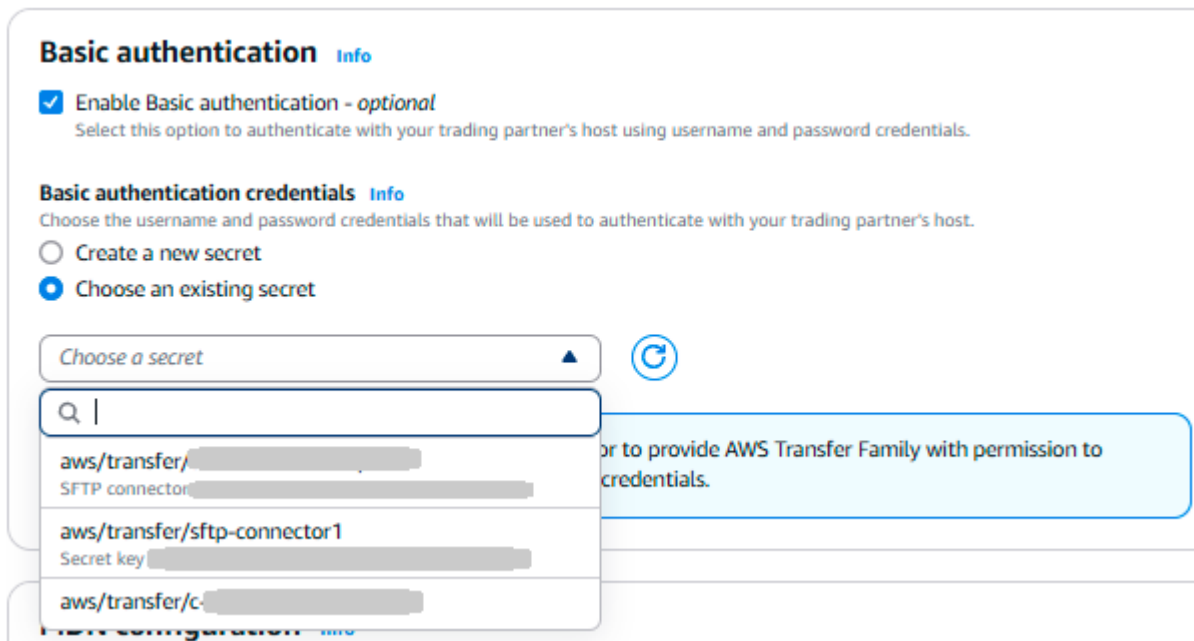
Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.
☒ Create a new secret
☐ Choose an existing secret

Username

Password

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

Der folgende Screenshot zeigt, wie „Standardauthentifizierung aktivieren“ und „Vorhandenes Geheimnis auswählen“ ausgewählt sind. Ihr Geheimnis muss das richtige Format haben, wie unter beschrieben [Aktivieren Sie die Standardauthentifizierung für AS2-Konnektoren](#).



Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c-...

or to provide AWS Transfer Family with permission to credentials.

Aktivieren Sie die Standardauthentifizierung für AS2-Konnektoren

Wenn Sie die Standardauthentifizierung für AS2-Connectoren aktivieren, können Sie entweder ein neues Geheimnis in der Transfer Family Family-Konsole erstellen oder ein Geheimnis verwenden, das Sie in AWS Secrets Manager erstellen. In beiden Fällen wird Ihr Geheimnis im Secrets Manager gespeichert.

Themen

- [Erstellen Sie ein neues Geheimnis in der Konsole](#)
- [Verwenden eines vorhandenen -Secrets](#)
- [Erstellen Sie ein Geheimnis in AWS Secrets Manager](#)

Erstellen Sie ein neues Geheimnis in der Konsole

Wenn Sie einen Connector in der Konsole erstellen, können Sie ein neues Geheimnis erstellen.

Um ein neues Geheimnis zu erstellen, wählen Sie Neues Geheimnis erstellen und geben Sie dann einen Benutzernamen und ein Passwort ein. Diese Anmeldeinformationen müssen mit dem Benutzer übereinstimmen, der eine Verbindung zum Endpunkt des Partners herstellt.

Basic authentication [Info](#)☒ **Enable Basic authentication - optional**

Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)

Choose the username and password credentials that will be used to authenticate with your trading partner's host.

- ☒ Create a new secret
- ☐ Choose an existing secret

Username**Password**

[i](#) Update the [access role associated with your connector](#) [↗](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

Note

Wenn Sie in der Konsole ein neues Geheimnis erstellen, folgt der Name des Geheimnisses dieser Benennungskonvention: **/aws/transfer/connector-id**, wobei die ID des Connectors **connector-id** steht, den Sie erstellen. Beachten Sie dies, wenn Sie versuchen, das Geheimnis in zu finden AWS Secrets Manager.

Verwenden eines vorhandenen -Secrets

Wenn Sie einen Connector in der Konsole erstellen, können Sie ein vorhandenes Geheimnis angeben.

Um ein vorhandenes Geheimnis zu verwenden, wählen Sie **Choose an existing secret** und wählen Sie dann ein Secret aus dem Dropdownmenü aus. Einzelheiten zur Erstellung eines korrekt formatierten Secrets in Secrets Manager finden Sie unter [Erstellen Sie ein Geheimnis in AWS Secrets Manager](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

or to provide AWS Transfer Family with permission to
credentials.

Erstellen Sie ein Geheimnis in AWS Secrets Manager

Das folgende Verfahren beschreibt, wie Sie ein geeignetes Geheimnis für die Verwendung mit Ihrem AS2-Connector erstellen.

Note

Die Standardauthentifizierung ist nur verfügbar, wenn Sie HTTPS verwenden.

Um Benutzeranmeldeinformationen in Secrets Manager für die AS2 Basic-Authentifizierung zu speichern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Secrets Manager Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie im linken Navigationsbereich Secrets aus.
3. Wählen Sie auf der Seite Secrets die Option Neues Geheimnis speichern aus.
4. Wählen Sie auf der Seite Geheimtyp auswählen für Geheimtyp die Option Anderer Geheimtyp aus.
5. Wählen Sie im Bereich Key/value Paare die Key/value Registerkarte aus.
 - Schlüssel — Enter **Username**.

- Wert — Geben Sie den Namen des Benutzers ein, der berechtigt ist, eine Verbindung zum Server des Partners herzustellen.
6. Wenn Sie ein Passwort angeben möchten, wählen Sie Zeile hinzufügen und wählen Sie im Bereich Key/value Paare die Key/valueRegisterkarte aus.

Wählen Sie Zeile hinzufügen und wählen Sie im Bereich Key/valuePaare die Key/valueRegisterkarte aus.
 - Schlüssel — Enter**Password**.
 - Wert — Geben Sie das Passwort für den Benutzer ein.
 7. Wenn Sie einen privaten Schlüssel angeben möchten, wählen Sie Zeile hinzufügen und wählen Sie im Bereich Key/value Paare die Key/valueRegisterkarte aus.
 - Schlüssel — Geben Sie ein**PrivateKey**.
 - Wert — Geben Sie einen privaten Schlüssel für den Benutzer ein. Dieser Wert muss im OpenSSH-Format gespeichert werden und dem öffentlichen Schlüssel entsprechen, der für diesen Benutzer auf dem Remoteserver gespeichert ist.
 8. Wählen Sie Weiter aus.
 9. Geben Sie auf der Seite Geheimen Schlüssel konfigurieren einen Namen und eine Beschreibung für Ihr Geheimnis ein. Wir empfehlen, dass Sie **aws/transfer/** für den Namen das Präfix von verwenden. Sie könnten beispielsweise Ihr Geheimnis benennen**aws/transfer/connector-1**.
 10. Wählen Sie Weiter und akzeptieren Sie dann die Standardeinstellungen auf der Seite Rotation konfigurieren. Klicken Sie anschließend auf Weiter.
 11. Wählen Sie auf der Seite „Überprüfen“ die Option Speichern aus, um das Geheimnis zu erstellen und zu speichern.

Nachdem Sie das Geheimnis erstellt haben, können Sie es beim Erstellen eines Connectors auswählen (siehe [Konfigurieren Sie AS2-Konnektoren](#)). Wählen Sie in dem Schritt, in dem Sie die Standardauthentifizierung aktivieren, das Geheimnis aus der Dropdownliste der verfügbaren Geheimnisse aus.

Details zum AS2-Konnektor anzeigen

In der AWS Transfer Family Konsole finden Sie eine Liste mit Details und Eigenschaften für einen AWS Transfer Family AS2-Connector. Zu den Eigenschaften eines AS2-Connectors gehören seine URL, Rollen, Profile, mDNs, Tags und Überwachungsmetriken.

Dies ist das Verfahren zum Anzeigen von Konnektordetails.

Um die Konnektordetails anzuzeigen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich die Option Connectors aus.
3. Wählen Sie den Bezeichner in der Spalte Connector-ID aus, um die Detailseite für den ausgewählten Connector aufzurufen.

Sie können die Eigenschaften für den AS2-Connector auf der Detailseite des Connectors ändern, indem Sie Bearbeiten wählen.

C-

Delete

Connector configuration

Info

Edit

Name

my-as2-connector

URL

<https://www.example.com>

Access role

[\[Link\]](#)

Logging role

[AWSTransferLoggingAccess \[Link\]](#)

Communication settings

Info

AS2-From header

[\[Link\]](#)

AS2-To header

[\[Link\]](#)

AS2 configuration

Info

Edit

Local profile

[\[Link\]](#)

Partner profile

[\[Link\]](#)

Preserve S3 Content-Type

Enabled

Compression

Enabled

Message Subject

View

Encryption algorithm

AES128_CBC

Signing algorithm

SHA384

MDN configuration

Info

Edit

Request MDN

Enabled

Signed MDN

Default to message signing algorithm: SHA384

Synchronization

Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**
✔ Enabled**Secret**
aws/transfer/c- [REDACTED] [Copy](#)**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

[Copy](#) 23.23.130.9[Copy](#) 44.196.109.11[Copy](#) 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

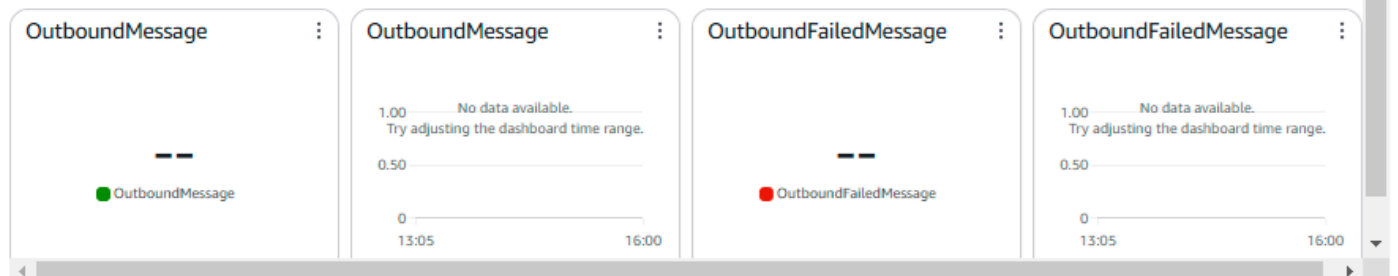
< 1 >

Key	Value
Name	my-as2-connector

AS2 Monitoring

3h 1d 1w

UTC timezone

**Note**

Sie können viele dieser Informationen, wenn auch in einem anderen Format, abrufen, indem Sie den folgenden Befehl ausführen AWS Command Line Interface (AWS CLI) :

```
aws transfer describe-connector --connector-id your-connector-id
```

Weitere Informationen finden Sie [DescribeConnector](#) in der API-Referenz.

Senden und Empfangen von AS2-Nachrichten

In diesem Abschnitt werden die Prozesse zum Senden und Empfangen von AS2-Nachrichten beschrieben. Es enthält auch Einzelheiten zu Dateinamen und Speicherorten, die mit AS2-Nachrichten verknüpft sind.

In der folgenden Tabelle sind die verfügbaren Verschlüsselungsalgorithmen für AS2-Nachrichten aufgeführt und es wird angegeben, wann Sie sie verwenden können.

Verschlüsselungsalgorithmus	HTTP	HTTPS	Hinweise
AES128_CBC	Ja	Ja	
AES192_CBC	Ja	Ja	
AES256_CBC	Ja	Ja	
DES_EDE3_CBC	Ja	Ja	Verwenden Sie diesen Algorithmus nur, wenn Sie einen Legacy-Client unterstützen müssen, der ihn benötigt, da es sich um einen schwachen Verschlüsselungsalgorithmus handelt.
NONE	Nein	Ja	Wenn Sie Nachrichten an einen Transfer Family Family-Server senden, können Sie nur auswählen, NONE ob Sie einen Application Load Balancer (ALB) verwenden.

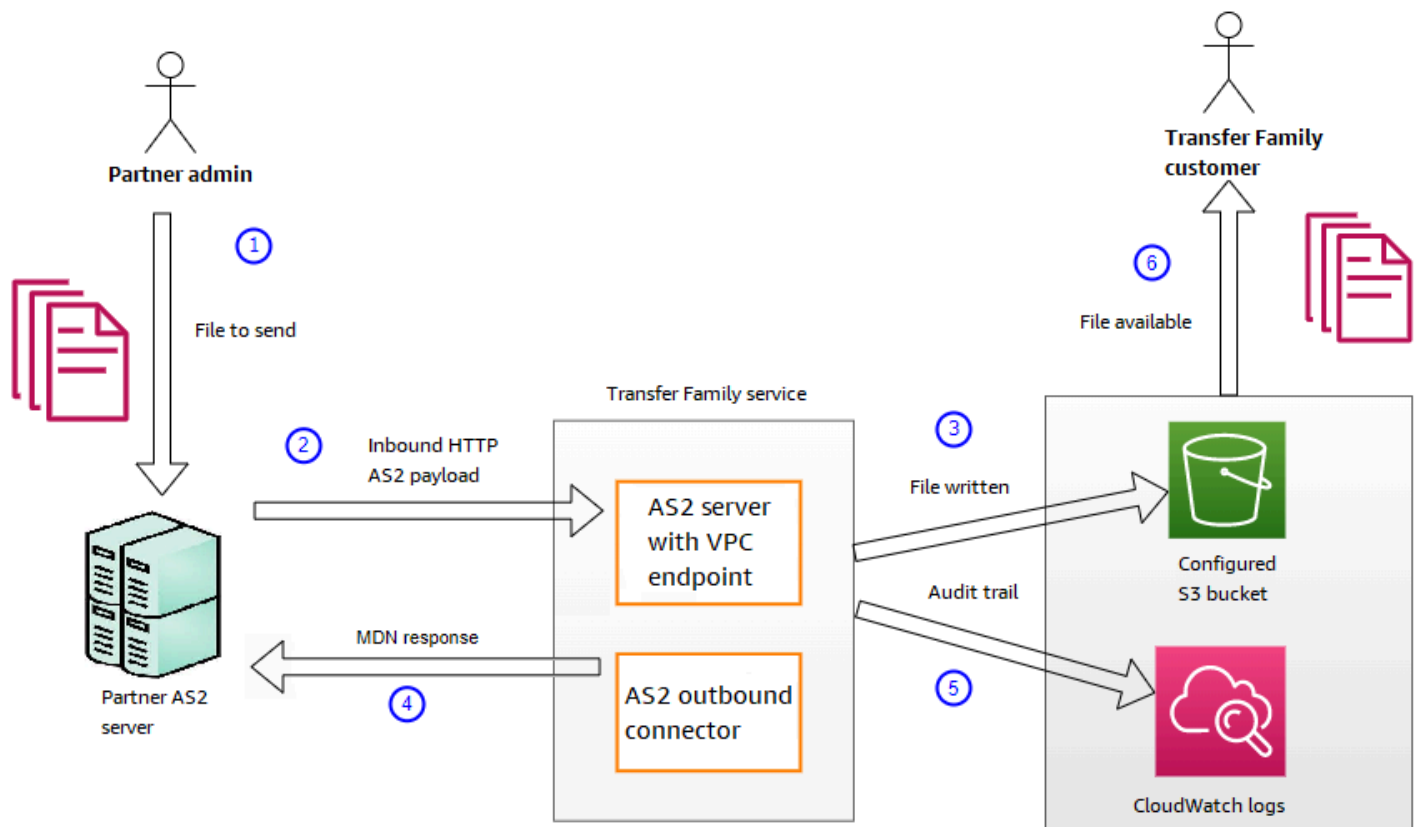
Themen

- [AS2-Nachrichtenprozess empfangen](#)
- [Senden und Empfangen von AS2-Nachrichten über HTTPS](#)
- [Übertragung von Dateien mithilfe eines AS2-Connectors](#)
- [Dateinamen und Speicherorte](#)
- [Statuscodes](#)
- [JSON-Beispieldateien](#)

AS2-Nachrichtenprozess empfangen

Der eingehende Prozess ist als eine Nachricht oder Datei definiert, die auf Ihren AWS Transfer Family Server übertragen wird. Die Reihenfolge für eingehende Nachrichten ist wie folgt:

1. Ein Administrator- oder automatisierter Prozess startet eine AS2-Dateiübertragung auf dem AS2-Remote-Server des Partners.
2. Der Remote-AS2-Server des Partners signiert und verschlüsselt den Dateiinhalt und sendet dann eine HTTP-POST-Anforderung an einen AS2-Eingangsendpunkt, der auf Transfer Family gehostet wird.
3. Mithilfe der konfigurierten Werte für den Server, die Partner, Zertifikate und die Vereinbarung entschlüsselt und verifiziert Transfer Family die AS2-Payload. Der Dateiinhalt wird im konfigurierten Amazon S3 S3-Dateispeicher gespeichert.
4. Die signierte MDN-Antwort wird entweder direkt mit der HTTP-Antwort oder asynchron über eine separate HTTP-POST-Anfrage an den ursprünglichen Server zurückgegeben.
5. Ein Prüfprotokoll CloudWatch mit Einzelheiten zum Austausch wird an Amazon geschrieben.
6. Die entschlüsselte Datei ist in einem Ordner mit dem Namen `inbox/processed` verfügbar.



Senden und Empfangen von AS2-Nachrichten über HTTPS

In diesem Abschnitt wird beschrieben, wie Sie einen Transfer Family Family-Server konfigurieren, der das AS2-Protokoll zum Senden und Empfangen von Nachrichten über HTTPS verwendet.

Themen

- [Senden Sie AS2-Nachrichten über HTTPS](#)
- [Empfangen Sie AS2-Nachrichten über HTTPS](#)

Senden Sie AS2-Nachrichten über HTTPS

Um AS2-Nachrichten über HTTPS zu senden, erstellen Sie einen Connector mit den folgenden Informationen:

- Geben Sie für die URL eine HTTPS-URL an
- Wählen Sie für den Verschlüsselungsalgorithmus einen der verfügbaren Algorithmen aus.

 Note

Um Nachrichten an einen Transfer Family Family-Server zu senden, ohne Verschlüsselung zu verwenden (d. h. Sie wählen NONE den Verschlüsselungsalgorithmus), müssen Sie einen Application Load Balancer (ALB) verwenden.

- Geben Sie die verbleibenden Werte für den Connector ein, wie unter beschrieben. [Konfigurieren Sie AS2-Konnektoren](#)

Empfangen Sie AS2-Nachrichten über HTTPS

AWS Transfer Family AS2-Server bieten derzeit nur HTTP-Transport über Port 5080. Sie können TLS jedoch auf einem Netzwerk oder einem Application Load Balancer vor Ihrem Transfer Family Family-Server-VPC-Endpunkt beenden, indem Sie einen Port und ein Zertifikat Ihrer Wahl verwenden. Mit diesem Ansatz können Sie festlegen, dass eingehende AS2-Nachrichten HTTPS verwenden.

Voraussetzungen

- Die VPC muss sich auf demselben Server AWS-Region wie Ihr Transfer Family Family-Server befinden.
- Die Subnetze Ihrer VPC müssen sich innerhalb der Availability Zones befinden, in denen Sie Ihren Server verwenden möchten.

 Note

Jeder Transfer Family Family-Server kann bis zu drei Availability Zones unterstützen.

- Weisen Sie bis zu drei Elastic IP-Adressen in derselben Region wie Ihr Server zu. Sie können sich auch dafür entscheiden, Ihren eigenen IP-Adressbereich (BYOIP) mitzubringen.

 Note

Die Anzahl der Elastic IP-Adressen muss der Anzahl der Availability Zones entsprechen, die Sie mit Ihren Serverendpunkten verwenden.

Sie können entweder einen Network Load Balance (NLB) oder einen Application Load Balancer (ALB) konfigurieren. In der folgenden Tabelle sind die Vor- und Nachteile der einzelnen Ansätze aufgeführt.

In der folgenden Tabelle sind die Unterschiede in den Funktionen aufgeführt, wenn Sie einen NLB und einen ALB zum Beenden von TLS verwenden.

Feature	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latenz	Geringere Latenz, da er auf Netzwerkebene arbeitet.	Höhere Latenz, da es auf der Anwendungsebene arbeitet.
Unterstützung für statische IPs	Kann elastische IP-Adressen anhängen, die statisch sein können.	Elastic IP-Adressen können nicht angehängt werden: Stellt eine Domain bereit, deren zugrunde liegende IP-Adressen sich ändern können.
Erweitertes Routing	Unterstützt kein erweitertes Routing.	Unterstützt erweitertes Routing. Kann den für AS2 erforderlichen X-Forwarded-Proto Header ohne Verschlüsselung einfügen. Dieser Header wird X-Forwarded-Proto auf der Website developer.mozilla.org beschrieben.
TLS/SSL Kündigung	Unterstützt die TLS/SSL Kündigung	Unterstützt die TLS/SSL Kündigung
Gegenseitiges TLS (mTLS)	Transfer Family unterstützt derzeit nicht die Verwendung eines NLB für mTLS	Support für mTLS

Configure NLB

Dieses Verfahren beschreibt, wie Sie einen mit dem Internet verbundenen Network Load Balancer (NLB) in Ihrer VPC einrichten.

Um einen Network Load Balancer zu erstellen und den VPC-Endpunkt des Servers als Ziel des Load Balancers zu definieren

1. Öffnen Sie die Amazon Elastic Compute Cloud-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich Load Balancers und dann Create Load Balancer aus.
3. Wählen Sie im Bereich Network Load Balancer die Option Erstellen.
4. Geben Sie im Abschnitt Grundkonfiguration die folgenden Informationen ein:
 - Geben Sie unter Name einen aussagekräftigen Namen für den Load Balancer ein.
 - Wählen Sie für Schema die Option. Internet-facing
 - Wählen Sie als IP-Adresstyp IPv4 aus.
5. Geben Sie im Abschnitt Netzwerkzuordnung die folgenden Informationen ein:
 - Wählen Sie für VPC die Virtual Private Cloud (VPC) aus, die Sie erstellt haben.
 - Wählen Sie unter Zuordnungen die Availability Zones aus, die den öffentlichen Subnetzen zugeordnet sind, die in derselben VPC verfügbar sind, die Sie mit Ihren Serverendpunkten verwenden.
 - Wählen Sie für die IPv4-Adresse jedes Subnetzes eine der Elastic IP-Adressen aus, die Sie zugewiesen haben.
6. Geben Sie im Abschnitt Listener und Routing die folgenden Informationen ein:
 - Wählen Sie als Protokoll die Option TLS aus.
 - Geben Sie im Feld Port **5080** ein.
 - Wählen Sie für Standardaktion die Option Zielgruppe erstellen aus. Einzelheiten zum Erstellen einer neuen Zielgruppe finden Sie unter [Erstellen einer Zielgruppe](#).

Nachdem Sie eine Zielgruppe erstellt haben, geben Sie ihren Namen in das Feld Standardaktion ein.

7. Wählen Sie im Bereich Secure Listener Settings Ihr Zertifikat im Bereich SSL/TLS Standardzertifikat aus.

8. Wählen Sie Create Load Balancer aus, um Ihren NLB zu erstellen.
9. (Optional, aber empfohlen) Aktivieren Sie die Zugriffsprotokolle für den Network Load Balancer, um einen vollständigen Audit-Trail zu führen, wie unter [Zugriffsprotokolle für Ihren Network Load Balancer](#) beschrieben.

Wir empfehlen diesen Schritt, da die TLS-Verbindung im NLB beendet wird. Daher ist die Quell-IP-Adresse, die in Ihren CloudWatch AS2-Protokollgruppen von Transfer Family wiedergegeben wird, die private IP-Adresse der NLB und nicht die externe IP-Adresse Ihres Handelspartners.

Configure ALB

Dieses Verfahren beschreibt, wie Sie einen Application Load Balancer (ALB) in Ihrer VPC einrichten.

Um einen Application Load Balancer zu erstellen und den VPC-Endpunkt des Servers als Ziel des Load Balancers zu definieren

1. Öffnen Sie die Amazon Elastic Compute Cloud-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich Load Balancers und dann Create Load Balancer aus.
3. Wählen Sie unter Application Load Balancer Create (Erstellen) aus.
4. Erstellen Sie in der ALB-Konsole einen neuen HTTP-Listener auf Port 443 (HTTPS).
5. (Optional). Wenn Sie die gegenseitige Authentifizierung (mTLS) einrichten möchten, konfigurieren Sie Sicherheitseinstellungen und einen Trust Store.
 - a. Hängen Sie Ihr SSL/TLS Zertifikat an den Listener an.
 - b. Wählen Sie unter Behandlung von Client-Zertifikaten die Option Gegenseitige Authentifizierung (mTLS) aus.
 - c. Wählen Sie Mit Trust Store verifizieren aus.
 - d. Wählen Sie unter Erweiterte mTLS-Einstellungen einen Vertrauensspeicher aus oder erstellen Sie ihn, indem Sie Ihre CA-Zertifikate hochladen.
6. Erstellen Sie eine neue Zielgruppe und fügen Sie die privaten IP-Adressen Ihrer Transfer Family AS2-Serverendpunkte als Ziele auf Port 5080 hinzu. Einzelheiten zur Erstellung einer neuen Zielgruppe finden Sie unter [Erstellen einer Zielgruppe](#)

7. Konfigurieren Sie Integritätsprüfungen für die Zielgruppe, um das HTTP-Protokoll auf Port 5080 zu verwenden.
8. Erstellen Sie eine neue Regel, um HTTPS-Verkehr vom Listener an die Zielgruppe weiterzuleiten.
9. Konfigurieren Sie den Listener so, dass er Ihr SSL/TLS Zertifikat verwendet.

Nachdem Sie den Load Balancer eingerichtet haben, kommunizieren die Clients mit dem Load Balancer über den benutzerdefinierten Port-Listener. Anschließend kommuniziert der Load Balancer über Port 5080 mit dem Server.

Erstellen einer Zielgruppe

1. Nachdem Sie im vorherigen Verfahren „Zielgruppe erstellen“ ausgewählt haben, werden Sie zur Seite „Gruppendetails angeben“ für eine neue Zielgruppe weitergeleitet.
2. Geben Sie im Abschnitt Grundkonfiguration die folgenden Informationen ein.
 - Wählen Sie für Wählen Sie einen Zieltyp die Option IP-Adressen aus.
 - Geben Sie unter Zielgruppenname einen Namen für die Zielgruppe ein.
 - Ihre Auswahl für Protokoll hängt davon ab, ob Sie eine ALB oder eine NLB verwenden.
 - Wählen Sie für einen Network Load Balancer (NLB) TCP
 - Wählen Sie für einen Application Load Balancer (ALB) HTTP
 - Geben Sie im Feld Port **5080** ein.
 - Wählen Sie als IP-Adresstyp IPv4 aus.
 - Wählen Sie für VPC die VPC aus, die Sie für Ihren Transfer Family AS2-Server erstellt haben.
3. Wählen Sie im Abschnitt Health Checks das Health Check-Protokoll aus.
 - Wählen Sie für ein ALB HTTP
 - Wählen Sie für einen NLB TCP
4. Wählen Sie Weiter aus.
5. Geben Sie auf der Seite Ziele registrieren die folgenden Informationen ein:
 - Vergewissern Sie sich, dass für Network die VPC angegeben ist, die Sie für Ihren Transfer Family AS2-Server erstellt haben.
 - Geben Sie für IPv4-Adresse die private IPv4-Adresse der Endpunkte Ihres Transfer Family AS2-Servers ein.

Wenn Sie mehr als einen Endpunkt für Ihren Server haben, wählen Sie IPv4-Adresse hinzufügen, um eine weitere Zeile für die Eingabe einer anderen IPv4-Adresse hinzuzufügen. Wiederholen Sie diesen Vorgang, bis Sie die privaten IP-Adressen für alle Endpunkte Ihres Servers eingegeben haben.

- Stellen Sie sicher, dass Ports auf **5080** eingestellt ist.
 - Wählen Sie unten „Als ausstehend einbeziehen“ aus, um Ihre Einträge zum Abschnitt „Ziele überprüfen“ hinzuzufügen.
6. Überprüfen Sie im Abschnitt Ziele überprüfen Ihre IP-Ziele.
 7. Wählen Sie Zielgruppe erstellen aus, kehren Sie dann zum vorherigen Verfahren zur Erstellung Ihrer NLB zurück und geben Sie die neue Zielgruppe an der angegebenen Stelle ein.

Testen Sie den Zugriff auf den Server von einer Elastic IP-Adresse aus

Stellen Sie über den benutzerdefinierten Port eine Connect zum Server her, indem Sie eine Elastic IP-Adresse oder den DNS-Namen des Network Load Balancer verwenden.

Important

Verwalten Sie den Zugriff auf Ihren Server von Client-IP-Adressen aus, indem Sie die [Network Access Control Lists \(Netzwerk-ACLs\)](#) für die auf dem Load Balancer konfigurierten Subnetze verwenden. Netzwerk-ACL-Berechtigungen werden auf Subnetzebene festgelegt, sodass die Regeln für alle Ressourcen gelten, die das Subnetz verwenden. Sie können den Zugriff von Client-IP-Adressen aus nicht mithilfe von Sicherheitsgruppen steuern, da der Zieltyp des Load Balancers auf IP-Adressen statt auf Instances festgelegt ist. Daher speichert der Load Balancer keine Quell-IP-Adressen. Wenn die [Integritätsprüfungen des Network Load Balancers](#) fehlschlagen, bedeutet dies, dass der Load Balancer keine Verbindung zum Serverendpunkt herstellen kann. Überprüfen Sie Folgendes, um dieses Problem zu beheben:

- Vergewissern Sie sich, dass die dem [Serverendpunkt zugeordnete Sicherheitsgruppe](#) eingehende Verbindungen aus den Subnetzen zulässt, die auf dem Load Balancer konfiguriert sind. Der Load Balancer muss in der Lage sein, über Port 5080 eine Verbindung zum Serverendpunkt herzustellen.
- Vergewissern Sie sich, dass der Serverstatus Online ist.

Übertragung von Dateien mithilfe eines AS2-Connectors

AS2-Konnektoren stellen eine Beziehung zwischen Handelspartnern für die Übertragung von AS2-Nachrichten von einem Transfer Family Family-Server an ein externes, partnereigenes Ziel her.

Sie können Transfer Family verwenden, um AS2-Nachrichten zu senden, indem Sie auf die Connector-ID und die Pfade zu den Dateien verweisen, wie im folgenden Befehl `start-file-transfer` AWS Command Line Interface (AWS CLI) dargestellt:

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-
bucket/myfile2.txt"
```

Führen Sie den folgenden Befehl aus, um die Details für Ihre Konnektoren abzurufen:

```
aws transfer list-connectors
```

Der `list-connectors` Befehl gibt die Connector-IDs, URLs und Amazon-Ressourcennamen (ARNs) für Ihre Konnektoren zurück.

Um die Eigenschaften eines bestimmten Connectors zurückzugeben, führen Sie den folgenden Befehl mit der ID aus, die Sie verwenden möchten:

```
aws transfer describe-connector --connector-id your-connector-id
```

Der `describe-connector` Befehl gibt alle Eigenschaften für den Connector zurück, einschließlich seiner URL, Rollen, Profile, MDNs (Message Disposition Notices), Tags und Überwachungsmetriken.

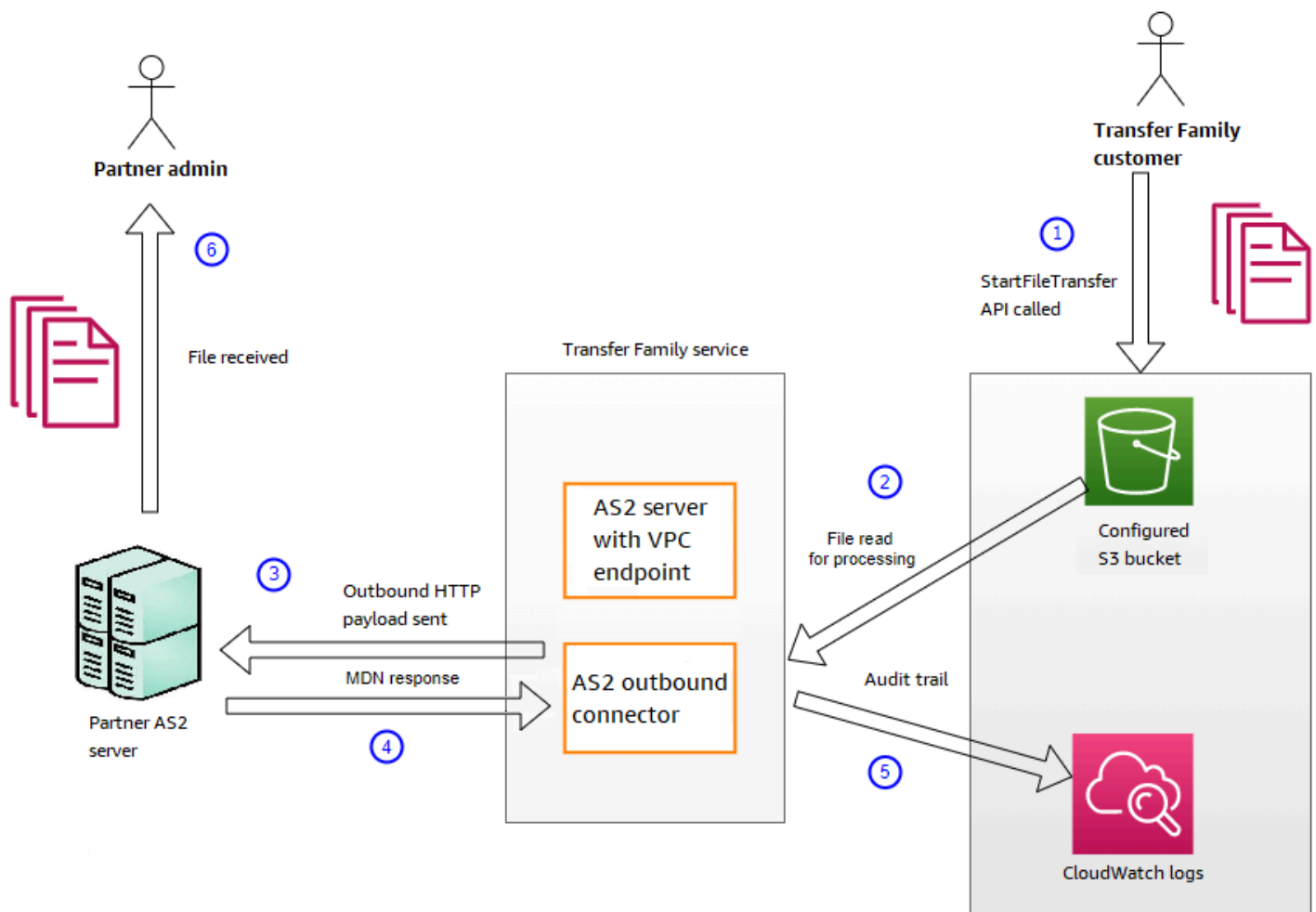
Sie können überprüfen, ob der Partner die Dateien erfolgreich erhalten hat, indem Sie sich die JSON- und MDN-Dateien ansehen. Diese Dateien werden gemäß den unter beschriebenen Konventionen benannt. [Dateinamen und Speicherorte](#) Wenn Sie bei der Erstellung des Connectors eine Protokollierungsrolle konfiguriert haben, können Sie Ihre CloudWatch Protokolle auch auf den Status von AS2-Nachrichten überprüfen.

Einzelheiten zum AS2-Connector finden Sie unter. [Details zum AS2-Konnektor anzeigen](#) Weitere Informationen zum Erstellen von AS2-Konnektoren finden Sie unter. [Konfigurieren Sie AS2-Konnektoren](#)

Um eine ausgehende AS2-Nachricht zu senden

Der ausgehende Prozess ist definiert als eine Nachricht oder Datei, die von AWS einem externen Client oder Dienst gesendet wird. Die Reihenfolge für ausgehende Nachrichten ist wie folgt:

1. Ein Administrator ruft den Befehl `start-file-transfer` AWS Command Line Interface (AWS CLI) oder die `StartFileTransfer` API-Operation auf. Diese Operation verweist auf eine `connector` Konfiguration.
2. Transfer Family erkennt eine neue Dateianfrage und lokalisiert die Datei. Die Datei ist komprimiert, signiert und verschlüsselt.
3. Ein Transfer-HTTP-Client führt eine HTTP-POST-Anfrage durch, um die Nutzdaten an den AS2-Server des Partners zu übertragen.
4. Der Prozess gibt die signierte MDN-Antwort zurück, entweder direkt mit der HTTP-Antwort (synchron oder asynchron MDN).
5. Während sich die Datei zwischen verschiedenen Übertragungsphasen bewegt, übermittelt der Prozess dem Kunden die Informationen zum Empfang und zur Verarbeitung der MDN-Antwort.
6. Der Remote-AS2-Server stellt die entschlüsselte und verifizierte Datei dem Partneradministrator zur Verfügung.



Die AS2-Verarbeitung unterstützt viele der RFC 4130-Protokolle, wobei der Schwerpunkt auf allgemeinen Anwendungsfällen und der Integration mit vorhandenen Serverimplementierungen liegt. AS2-enabled Einzelheiten zu den unterstützten Konfigurationen finden Sie unter [AS2-Konfigurationen](#)

Dateinamen und Speicherorte

In diesem Abschnitt werden die Konventionen zur Benennung von Dateien für AS2-Übertragungen beschrieben.

Beachten Sie bei eingehenden Dateiübertragungen Folgendes:

- Sie geben das Basisverzeichnis in einer Vereinbarung an. Das Basisverzeichnis ist der Amazon S3 S3-Bucket-Name in Kombination mit einem Präfix, falls vorhanden. Beispiel, **/amzn-s3-demo-bucket/AS2-folder**.

- Wenn eine eingehende Datei erfolgreich verarbeitet wurde, wird die Datei (und die entsprechende JSON-Datei) in dem /processed Ordner gespeichert. Beispiel, /**amzn-s3-demo-bucket**/AS2-folder/processed.

Die JSON-Datei enthält die folgenden Felder:

- agreement-id
 - as2-from
 - as2-to
 - as2-message-id
 - transfer-id
 - client-ip
 - connector-id
 - failure-message
 - file-path
 - message-subject
 - mdn-message-id
 - mdn-subject
 - requester-file-name
 - requester-content-type
 - server-id
 - status-code
 - failure-code
 - transfer-size
- Wenn eine eingehende Datei nicht erfolgreich verarbeitet werden kann, wird die Datei (und die entsprechende JSON-Datei) in dem /failed Ordner gespeichert. Beispiel, /amzn-s3-demo-bucket/AS2-folder/failed.
 - Die übertragene Datei wird im processed Ordner als gespeichert *original_filename.messageId.original_extension*. Das heißt, die Nachrichten-ID für die Übertragung wird vor der ursprünglichen Erweiterung an den Namen der Datei angehängt.
 - Eine JSON-Datei wird erstellt und gespeichert

als *original_filename.messageId.original_extension*.json. Zusätzlich zur

hinzugefügten Nachrichten-ID wird die Zeichenfolge `.json` an den Namen der übertragenen Datei angehängt.

- Eine MDN-Datei (Message Disposition Notice) wird erstellt und gespeichert als `original_filename.messageId.original_extension.mdn`. Zusätzlich zur hinzugefügten Nachrichten-ID wird die Zeichenfolge `.mdn` an den Namen der übertragenen Datei angehängt.
- Wenn es eine eingehende Datei mit dem Namen `exampleFileInS3Payload.dat`, werden die folgenden Dateien erstellt:
 - Datei —
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - JSON —
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - MDN —
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`

Bei ausgehenden Übertragungen ist die Benennung ähnlich, mit dem Unterschied, dass es keine Datei für eingehende Nachrichten gibt und außerdem die Übertragungs-ID für die übertragene Nachricht zum Dateinamen hinzugefügt wird. Die Übertragungs-ID wird durch den `StartFileTransfer` API-Vorgang zurückgegeben (oder wenn ein anderer Prozess oder ein anderes Skript diesen Vorgang aufruft).

- Das `transfer-id` ist eine Kennung, die mit einer Dateiübertragung verknüpft ist. Alle Anfragen, die Teil eines `StartFileTransfer` Anrufs sind, teilen sich ein `transfer-id`.
- Das Basisverzeichnis entspricht dem Pfad, den Sie für die Quelldatei verwenden. Das heißt, das Basisverzeichnis ist der Pfad, den Sie in der `StartFileTransfer` API-Operation oder im `start-file-transfer` AWS CLI API-Befehl angeben. Beispiel:

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/
file-to-send.txt
```

Wenn Sie diesen Befehl ausführen, werden MDN- und JSON-Dateien in `/amzn-s3-demo-bucket/AS2-folder/processed` (für erfolgreiche Übertragungen) oder `/amzn-s3-demo-bucket/AS2-folder/failed` (für erfolglose Übertragungen) gespeichert.

- Eine JSON-Datei wird erstellt und gespeichert als `original_filename.transferId.messageId.original_extension.json`.

- Eine MDN-Datei wird erstellt und gespeichert
als `original_filename.transferId.messageId.original_extension.mdn`.
- Wenn es eine ausgehende Datei mit dem Namen `gibtExampleFileOutTestOutboundSyncMdn.dat`, werden die folgenden Dateien erstellt:
 - JSON — `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.json`
 - MDN — `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.mdn`

Sie können auch die CloudWatch Protokolle überprüfen, um die Details Ihrer Übertragungen einzusehen, einschließlich fehlgeschlagener Übertragungen.

Statuscodes

In der folgenden Tabelle sind alle Statuscodes aufgeführt, die in den CloudWatch Protokollen protokolliert werden können, wenn Sie oder Ihr Partner eine AS2-Nachricht senden. Verschiedene Schritte zur Nachrichtenverarbeitung gelten für verschiedene Nachrichtentypen und dienen nur der Überwachung. Die Status COMPLETED und FAILED stellen den letzten Verarbeitungsschritt dar und sind in JSON-Dateien sichtbar.

Code	Description	Verarbeitung abgeschlossen?
VERARBEITUNG	Die Nachricht wird gerade in ihr endgültiges Format konvertiert. Beispielsweise haben sowohl die Dekomprimierungs- als auch die Entschlüsselungsschritte diesen Status.	Nein
MDN_TRANSMIT	Die Nachrichtenverarbeitung sendet eine MDN-Antwort.	Nein
MDN_RECEIVE	Die Nachrichtenverarbeitung empfängt eine MDN-Antwort.	Nein

Code	Description	Verarbeitung abgeschlossen?
COMPLETED	Die Nachrichtenverarbeitung wurde erfolgreich abgeschlossen. Dieser Status gilt auch, wenn ein MDN für eine eingehende Nachricht oder für die MDN-Überprüfung ausgehender Nachrichten gesendet wird.	Ja
FEHLGESCHLAGEN	Die Nachrichtenverarbeitung ist fehlgeschlagen. Eine Liste der Fehlercodes finden Sie unter AS2-Fehlercodes .	Ja

JSON-Beispieldateien

In diesem Abschnitt werden JSON-Beispieldateien für eingehende und ausgehende Übertragungen aufgeführt, einschließlich Beispieldateien für erfolgreiche Übertragungen und fehlgeschlagene Übertragungen.

Beispiel für eine ausgehende Datei, die erfolgreich übertragen wurde:

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-
d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been
accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
}
```

```

"file-path": "/amzn-s3-demo-bucket/as2testcell10000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
"as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@9c705f0baaaabaa",
"timestamp": "2022-07-11T06:30:10.791274Z"
}

```

Beispiel für eine ausgehende Datei, die nicht erfolgreich übertragen wurde:

```

{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}

```

Beispiel für eine eingehende Datei, die erfolgreich übertragen wurde:

```

{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat",
  "as2-from": "MyCompany_OID",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 1050,
  "mdn-subject": "Message Disposition Notification",
  "as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID",
  "as2-to": "PartnerA_OID",
  "agreement-id": "a-f5c5cbea5f7741988",
}

```

```

"file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
"server-id": "s-5f7422b04c2447ef9",
"timestamp": "2022-07-11T23:36:36.105030Z"
}

```

Beispiel für eine eingehende Datei, die nicht erfolgreich übertragen wurde:

```

{
  "failure-code": "INVALID_REQUEST",
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-
integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-
TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}

```

Passen Sie HTTP-Header für AS2-Nachrichten an

Wenn Sie AS2-Nachrichten an Handelspartner senden, müssen Sie möglicherweise die HTTP-Header anpassen, um bestimmte Anforderungen zu erfüllen oder die Kompatibilität mit der AS2-Serverkonfiguration Ihres Partners zu verbessern. Diese CloudFormation Vorlage erstellt eine Infrastruktur, um benutzerdefinierte HTTP-Header für AS2-Nachrichten zu aktivieren, die über gesendet werden. AWS Transfer Family Es richtet ein Amazon API Gateway und eine Lambda-Funktion ein, die als Proxy fungiert und die dynamische Änderung von Headern ermöglicht, die von den AS2-Servern der Handelspartner benötigt werden.

Verwenden Sie diese Vorlage, um Folgendes zu tun:

- Fügen Sie benutzerdefinierte HTTP-Header zu ausgehenden AS2-Nachrichten hinzu
- Überschreiben Sie die Standard-Header-Werte mit benutzerdefinierten Werten

 Important

Seien Sie vorsichtig, wenn Sie Standard-Header-Werte überschreiben, da dies zu Sendefehlern führen kann: einige AS2-Header sind erforderlich.

- Stellen Sie die Kompatibilität mit Handelspartnern sicher, die spezifische Header-Anforderungen haben

Vorlagen – Übersicht

Die Vorlage erstellt die folgenden Hauptkomponenten:

- Eine Lambda-Funktion, die AS2-Nachrichten verarbeitet und weiterleitet
- Ein Amazon API Gateway zur Bereitstellung der Lambda-Funktion
- IAM-Rollen und -Berechtigungen für die Lambda-Funktion
- Bedingte Ressourcen für die HTTPS-Unterstützung

Die Vorlagendatei ist hier verfügbar: [Vorlage für dynamische HTTP-Header](#).

So funktioniert's

1. Das Amazon API Gateway empfängt eingehende AS2-Nachrichten von AWS Transfer Family.
2. Die Anfrage wird an die Lambda-Funktion weitergeleitet.
3. Die Lambda-Funktion verarbeitet die Anfrage und fügt nach Bedarf Header hinzu oder ändert sie.
4. Die geänderte Anfrage wird dann an den AS2-Server des Partners weitergeleitet.
5. Die Antwort vom Server des Partners wird über Lambda und Amazon API Gateway an AWS Transfer Family zurückgesendet.

Wichtigste Funktionen

- **Dynamische Header-Änderung:** Ermöglicht die Anpassung des Betreff-Headers und das Hinzufügen weiterer erforderlicher Header.
- **Protokollunterstützung:** Funktioniert sowohl mit HTTP- als auch mit HTTPS-Protokollen.
- **Flexible Konfiguration:** Ermöglicht die Angabe von Partnerhost, Port und Pfad.

Implementierungsinformationen

Die Vorlage implementiert die folgenden Schlüsselkomponenten:

Lambda-Funktion

Der Kern der Lösung ist eine Node.js Lambda-Funktion, die:

- Empfängt Anfragen vom Amazon API Gateway
- Ändert Header auf der Grundlage der Konfiguration und der eingehenden Anforderungsdaten
- Leitet die geänderte Anfrage an den AS2-Server des Partners weiter
- Verarbeitet sowohl HTTP- als auch HTTPS-Protokolle
- Beinhaltet Fehlerbehandlung und Protokollierung

Amazon API Gateway

Eine HTTP-API ist eingerichtet für:

- Empfangen Sie eingehende AS2-Nachrichten
- Anfragen an die Lambda-Funktion weiterleiten
- Geben Sie die Antworten zurück an AWS Transfer Family

Vorlagenparameter

Geben Sie die Informationen für die Vorlagenparameter wie folgt ein. Beachten Sie, dass es sich bei all diesen Parametern um Zeichenketten handelt.

- **Environment:** Dieser Parameter wird verwendet, um die Ressourcen zu benennen, die die Vorlage erstellt, und zwar unabhängig davon, ob sie für eine Entwicklungs- oder Produktionsumgebung bestimmt sind. Gültige Werte sind dev und prod.
- **PartnerHost:** Die IP-Adresse oder der Hostname des AS2-Partnerservers.
- **PartnerPort:** Die Portnummer für den AS2-Partnerserver. Wenn nicht angegeben, wird standardmäßig 80 für HTTP und 443 für HTTPS verwendet.
- **PartnerPath:** der Pfad zum AS2-Endpunkt auf dem Partnerserver
- **ProtocolType:** das für die AS2-Kommunikation zu verwendende Protokoll: Gültige Werte sind HTTP und HTTPS.

Bedingte Ressourcen

Für die HTTPS-Unterstützung erstellt die Vorlage unter bestimmten Bedingungen:

- Eine Lambda-Schicht für CA-Zertifikate
- HTTPS-specific Konfiguration in der Lambda-Funktion

Bereitstellung und Verwendung

Um AS2-HTTP-Header mithilfe einer Vorlage anzupassen CloudFormation

1. Öffnen Sie die CloudFormation Konsole unter. <https://console.aws.amazon.com/cloudformation>
2. Wählen Sie im linken Navigationsbereich Stack aus.
3. Wählen Sie Create stack (Stack erstellen) und dann With new resources (standard) (Mit neuen Ressourcen (Standard)).
4. Wählen Sie im Abschnitt Voraussetzung — Vorlage vorbereiten die Option Vorhandene Vorlage auswählen aus.
5. Kopieren Sie diesen Link, die [Vorlage für dynamische HTTP-Header](#), und fügen Sie ihn in das Amazon S3 S3-URL-Feld ein.
6. Wählen Sie Weiter aus.
7. Füllen Sie die Parameterdetails mit Ihren Informationen aus. Diese sind detailliert in [Vorlagenparameter](#).
8. Wählen Sie Weiter aus. Wählen Sie auf der Seite „Stack-Optionen konfigurieren“ erneut Weiter aus.
9. Überprüfen Sie die Details für den Stack, den Sie gerade erstellen, und wählen Sie dann Stapel erstellen aus.

Note

Unten auf der Seite müssen Sie unter Funktionen angeben, dass dadurch CloudFormation möglicherweise Ressourcen AWS Identity and Access Management (IAM) erstellt werden.

Nach der Bereitstellung dieses CloudFormation Stacks:

1. Notieren Sie sich die Amazon API Gateway Gateway-Endpunkt-URL, die in den Stack-Ausgaben angegeben ist.
2. Aktualisieren Sie Ihren vorhandenen AWS Transfer Family Connector, um diesen neuen Amazon API Gateway Gateway-Endpunkt zu verwenden.
3. Die Lösung verarbeitet jetzt AS2-Nachrichten und fügt Header wie konfiguriert hinzu oder ändert sie.

 Warning

Ändern Sie nur den Betreff-Header oder fügen Sie Header hinzu, die Ihr Partner ausdrücklich erwartet. Das Ändern anderer Header kann zu Übertragungsfehlern führen.

Überwachung der AS2-Nutzung

Sie können die AS2-Aktivität mit Amazon CloudWatch und AWS CloudTrail überwachen. Weitere Servermetriken für Transfer Family finden Sie unter [CloudWatch Amazon-Protokollierung für AWS Transfer Family Server](#)

AS2-Metriken

Metrik	Description
InboundMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolgreich von einem Handelspartner empfangen wurden. Einheiten: Anzahl Dauer: 5 Minuten
InboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die von einem Handelspartner erfolglos empfangen wurden. Das heißt, ein Handelspartner hat eine Nachricht gesendet, aber der Transfer Family Family-Server konnte sie nicht erfolgreich verarbeiten.

Metrik	Description
	Einheiten: Anzahl Dauer: 5 Minuten
OutboundMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolgreich vom Transfer Family Family-Server an einen Handelspartner gesendet wurden. Einheiten: Anzahl Zeitraum: 5 Minuten
OutboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolglos an einen Handelspartner gesendet wurden. Das heißt, sie wurden vom Transfer Family Family-Server gesendet, aber vom Handelspartner nicht erfolgreich empfangen. Einheiten: Anzahl Dauer: 5 Minuten
DaysUntilExpiry	Die Anzahl der Tage, bis ein Zertifikat abläuft, wird durch den InactiveDate Wert bestimmt, der beim Import auf dem Zertifikat angegeben ist. Einheiten: Anzahl Abmessungen: CertificateId , Description (falls angegeben) Zeitraum: 1 Tag Weitere Informationen finden Sie unter Rotation der AS2-Zertifikate.

AS2-Statuscodes

In der folgenden Tabelle sind alle Statuscodes aufgeführt, die in CloudWatch Protokollen protokolliert werden können, wenn Sie oder Ihr Partner eine AS2-Nachricht senden. Verschiedene Schritte zur Nachrichtenverarbeitung gelten für verschiedene Nachrichtentypen und dienen nur der Überwachung. Die Status COMPLETED und FAILED stellen den letzten Verarbeitungsschritt dar und sind in JSON-Dateien sichtbar.

Code	Description	Die Verarbeitung ist abgeschlossen?
VERARBEITUNG	Die Nachricht wird gerade in ihr endgültiges Format konvertiert. Beispielsweise haben sowohl die Dekomprimierungs- als auch die Entschlüsselungsschritte diesen Status.	Nein
MDN_TRANSMIT	Die Nachrichtenverarbeitung sendet eine MDN-Antwort.	Nein
MDN_RECEIVE	Die Nachrichtenverarbeitung empfängt eine MDN-Antwort.	Nein
COMPLETED	Die Nachrichtenverarbeitung wurde erfolgreich abgeschlossen. Dieser Status gilt auch, wenn ein MDN für eine eingehende Nachricht oder für die MDN-Überprüfung ausgehender Nachrichten gesendet wird.	Ja
FEHLGESCHLAGEN	Die Nachrichtenverarbeitung ist fehlgeschlagen. Eine Liste der Fehlercodes finden Sie unter AS2-Fehlercodes .	Ja

AS2-Fehlercodes

In der folgenden Tabelle werden Fehlercodes aufgeführt und beschrieben, die Sie möglicherweise bei AS2-Dateiübertragungen erhalten.

AS2-Fehlercodes

Code	Fehler	Beschreibung und Lösung
ACCESS_DENIED	- Zugriff verweigert. Prüfen Sie, ob Ihre Zugriffsrolle über die erforderlichen Berechtigungen verfügt. - Ungültiger Dateipfad <i>send-file-path</i> - Anmeldeinformationen konnten nicht abgerufen werden mit ErrorCode: <i>error-code</i>	Tritt auf, wenn eine <code>StartFileTransfer</code> Anfrage bearbeitet wird, bei der eine der <code>SendFilePaths</code> Anfragen ungültig oder falsch formatiert ist. Das heißt, dem Pfad fehlt der Amazon S3 S3-Bucket-Name oder der Pfad enthält ungültige Zeichen. Tritt auch auf, wenn Transfer Family die Zugriffs- oder Protokollierungsrolle nicht übernimmt. Stellen Sie sicher, dass der Pfad einen gültigen Amazon S3 S3-Bucket-Namen und einen gültigen Schlüsselnamen enthält.
AGREEMENT_NOT_FOUND	Es wurde keine Vereinbarung gefunden.	Entweder wurde die Vereinbarung nicht gefunden, oder die Vereinbarung ist mit einem inaktiven Profil verknüpft. Aktualisieren Sie die Vereinbarung auf dem Transfer Family Family-Server, sodass sie aktive Profile enthält.

Code	Fehler	Beschreibung und Lösung
CONNECTOR_NOT_FOUND	Der Connector oder die zugehörige Konfiguration wurde nicht gefunden.	Entweder wurde der Connector nicht gefunden, oder der Connector ist einem inaktiven Profil zugeordnet. Aktualisieren Sie den Connector so, dass er aktive Profile enthält.

Code	Fehler	Beschreibung und Lösung
CREDENTIALS_RETRIEVAL_FAILED	1. Secret wurde im Secrets Manager nicht gefunden. 2. Auf Secrets Manager kann nicht zugegriffen werden. 3. Das Geheimnis konnte in Secrets Manager nicht entschlüsselt werden. 4. Der geheime Wert kann aufgrund der Drosselung nicht abgerufen werden.	Für die AS2 Basic-Authentifizierung muss der geheime Schlüssel korrekt formatiert sein. Die folgenden Lösungen entsprechen den in der vorherigen Spalte aufgeführten Fehlern. 1. Stellen Sie sicher, dass die geheime ID korrekt ist. 2. Stellen Sie sicher, dass die Zugriffsrolle über die entsprechenden Berechtigungen zum Lesen des Geheimnisses verfügt. Die Zugriffsrolle muss Lese- und Schreibzugriff auf das übergeordnete Verzeichnis des in der StartFile Transfer Anfrage verwendeten Dateispeicherorts gewähren. Stellen Sie außerdem sicher, dass die Rolle Lese- und Schreibzugriff auf das übergeordnete Verzeichnis der Dateien bietet, die Sie mit versenden möchtenStartFile Transfer . 3. Wenn ein vom Kunden verwalteter Schlüssel für den geheimen Schlüssel verwendet wird, stellen Sie

Code	Fehler	Beschreibung und Lösung
		sicher, dass die Zugriffsrolle über Berechtigungen für den Schlüssel AWS Key Management Service (AWS KMS) verfügt. 4. Die geltenden Kontingente finden Sie unter Kontingente für den Umgang mit Geheimnissen.
DECOMPRESSION_FAILED	Nachricht konnte nicht dekomprimiert werden.	Entweder ist die gesendete Datei beschädigt, oder der Komprimierungsalgorithmus ist ungültig. Senden Sie die Nachricht erneut und stellen Sie sicher, dass die ZLIB-Komprimierung verwendet wird, oder senden Sie die Nachricht erneut, ohne dass die Komprimierung aktiviert ist.
DECRYPT_FAILED	Nachricht konnte nicht entschlüsselt werden. <i>message-ID</i> Stellen Sie sicher, dass der Partner über den richtigen öffentlichen Verschlüsselungsschlüssel verfügt.	Die Entschlüsselung ist fehlgeschlagen. Vergewissern Sie sich, dass der Partner eine Payload mithilfe eines gültigen Zertifikats gesendet hat und dass die Verschlüsselung mit einem gültigen Verschlüsselungsalgorithmus durchgeführt wurde.

Code	Fehler	Beschreibung und Lösung
DECRYPT_FAILED_INVALID_SMIME_FORMAT	Das umhüllte MIMEPart konnte nicht analysiert werden.	Die MIME-Nutzlast ist entweder beschädigt oder hat ein nicht unterstütztes S/MIME-Format. Der Absender sollte sicherstellen, dass das von ihm verwendete Format unterstützt wird, und die Payload dann erneut senden.
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	Es wurde kein passender Entschlüsselungsschlüssel gefunden.	Dem Partnerprofil wurde kein Zertifikat zugewiesen, das der Nachricht entsprach, oder die Zertifikate, die der Nachricht entsprachen, sind jetzt abgelaufen oder nicht mehr gültig. Sie müssen das Partnerprofil aktualisieren und sicherstellen, dass es ein gültiges Zertifikat enthält.
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	Die SMIME-Nutzlastentschlüsselung wurde mithilfe eines nicht unterstützten Algorithmus mit der ID angefordert: <i>encryption-ID</i>	Der entfernte Absender hat eine AS2-Nutzlast mit einem nicht unterstützten Verschlüsselungsalgorithmus gesendet. Der Absender muss einen Verschlüsselungsalgorithmus wählen, der von unterstützt wird. AWS Transfer Family

Code	Fehler	Beschreibung und Lösung
DUPLICATE_MESSAGE	Doppelter oder doppelt verarbeiteter Schritt.	Die Payload hat einen doppelten Verarbeitungsschritt. Beispielsweise gibt es zwei Verschlüsselungsschritte. Senden Sie die Nachricht erneut mit einem einzigen Schritt zum Signieren, Komprimieren und Verschlüsseln.
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	Im Profil wurden keine gültigen öffentlichen Verschlüsselungszertifikate gefunden: <i>local-profile-ID</i>	Transfer Family versucht, eine ausgehende Nachricht zu verschlüsseln, es wurden jedoch keine Verschlüsselungszertifikate für das lokale Profil gefunden. Auflösungsoptionen: • Stellen Sie sicher, dass dem lokalen Profil ein Zertifikat und ein privater Schlüssel für die Verschlüsselung beigelegt sind. • Stellen Sie sicher, dass das Verschlüsselungszertifikat derzeit aktiv ist.

Code	Fehler	Beschreibung und Lösung
ENCRYPTION_FAILED	Die Datei <i>file-name</i> konnte nicht verschlüsselt werden.	Die zu sendende Datei ist nicht für die Verschlüsselung verfügbar. Stellen Sie sicher, dass sich die Datei an ihrem erwarteten AS2-Speicherort befindet und dass Sie AWS Transfer Family über Leserechte für die Datei verfügen.
FILE_SIZE_TOO_LARGE	Die Dateigröße ist zu groß.	Dies tritt auf, wenn eine Datei gesendet oder empfangen wird, die die Dateigrößenbeschränkung überschreitet.
HTTP_ERROR_RESPONSE_FROM_PARTNER	<i>partner-URL</i> hat den Status 400 für eine Nachricht mit ID= <i>message-ID</i> zurückgegeben.	Bei der Kommunikation mit dem AS2-Server des Partners wurde ein unerwarteter HTTP-Antwortcode zurückgegeben. Der Partner kann möglicherweise weitere Diagnosen anhand seiner AS2-Serverprotokolle bereitstellen.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	Verschlüsselung ist erforderlich.	Der Partner hat eine unverschlüsselte Nachricht an Transfer Family gesendet, die nicht unterstützt wird. Der Absender muss eine verschlüsselte Nutzlast verwenden.

Code	Fehler	Beschreibung und Lösung
INVALID_ENDPOINT_PROTOCOL	Nur HTTP und HTTPS werden unterstützt.	Sie müssen HTTP oder HTTPS als Protokoll in Ihrer AS2-Connectorkonfiguration angeben.

Code	Fehler	Beschreibung und Lösung
INVALID_REQUEST	1. Es besteht ein Problem mit einem Nachrichtenheader. 2. Geheimes JSON konnte nicht analysiert werden. Geheimes JSON entsprach nicht dem erwarteten Format. 3. Secret muss eine JSON-Zeichenfolge sein. 4. Der Benutzername darf keinen Doppelpunkt enthalten. Der Benutzername darf keine Steuerzeichen enthalten. Der Benutzername darf nur ASCII-Zeichen enthalten. Das Passwort darf keine Steuerzeichen enthalten. Das Passwort darf nur ASCII-Zeichen enthalten.	Dieser Fehler hat mehrere Ursachen. Die folgenden Lösungen entsprechen den in der vorherigen Spalte aufgeführten Fehlern. 1. Überprüfen Sie die as2-to Felder as2-from und. Stellen Sie sicher, dass die ursprüngliche Nachrichten-ID für das MDN-Format korrekt ist. Stellen Sie außerdem sicher, dass im Nachrichten-ID-Format keine AS2-Header fehlen. 2. Stellen Sie sicher, dass der geheime Wert dem dokumentierten Format entspricht, wie unter beschrieben. Aktivieren Sie die Standardauthentifizierung für AS2-Konnektoren 3. Stellen Sie sicher, dass das Geheimnis als Zeichenfolge und nicht als Binärdatei bereitgestellt wird. 4. Nehmen Sie die erforderlichen Korrekturen am Benutzernamen oder Passwort vor.

Code	Fehler	Beschreibung und Lösung
INVALID_URL_FORMAT	Ungültiges URL-Format: <i>URL</i>	Dies tritt auf, wenn Sie eine ausgehende Nachricht mithilfe eines Connectors senden, der mit einer falsch formatierten URL konfiguriert ist. Stellen Sie sicher, dass der Connector mit einer gültigen HTTP- oder HTTPS-URL konfiguriert ist.
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	Nicht zutreffend	Der Empfänger kann den Absender nicht authentifizieren. Der Geschäftspartner gibt ein MDN mit dem Dispositionsmodifikator Error: authentication-failed an Transfer Family zurück.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	Nicht zutreffend	Dies tritt auf, wenn der Empfänger den Nachrichteninhalte nicht dekomprimieren kann. Der Geschäftspartner gibt ein MDN mit dem Dispositionsmodifikator Error: decompression-failed an Transfer Family zurück.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	Nicht zutreffend	Der Empfänger kann den Nachrichteninhalte nicht entschlüsseln. Der Geschäftspartner gibt ein MDN mit dem Dispositionsmodifikator Error: authentication-failed an Transfer Family zurück.

Code	Fehler	Beschreibung und Lösung
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	Nicht zutreffend	Der Empfänger erwartet, dass die Nachricht signiert oder verschlüsselt ist, ist es aber nicht. Der Geschäftspartner sendet ein MDN mit dem Dispositionsmodifikator Error: insufficient-message-security an Transfer Family zurück. Aktivieren Sie die and/or Signierungsverschlüsselung auf dem Connector, um den Erwartungen des Handelspartners zu entsprechen.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Nicht zutreffend	Der Empfänger kann die Integrität des Inhalts nicht überprüfen. Der Geschäftspartner gibt ein MDN mit dem Dispositionsmodifikator Error: integrity-check-failed an Transfer Family zurück.
PATH_NOT_FOUND	Das Verzeichnis konnte nicht erstellt werden. <i>file-path</i> Der übergeordnete Pfad konnte nicht gefunden werden.	Transfer Family versucht, ein Verzeichnis im Amazon S3 S3-Bucket des Kunden zu erstellen, aber der Bucket wurde nicht gefunden. Stellen Sie sicher, dass jeder im StartFileTransfer Befehl erwähnte Pfad den Namen eines vorhandenen Buckets enthält.

Code	Fehler	Beschreibung und Lösung
SEND_FILE_NOT_FOUND	Der Dateipfad wurde <i>file-path</i> nicht gefunden.	Transfer Family kann die Datei beim Senden der Datei nicht finden. Überprüfen Sie, ob das konfigurierte Home-Verzeichnis und der Pfad gültig sind und ob Transfer Family über Leseberechtigungen für die Datei verfügt.
SERVER_NOT_FOUND	Der mit der Nachricht verknüpfte Server konnte nicht gefunden werden.	Transfer Family konnte den Server beim Empfang einer Nachricht nicht finden. Dies kann passieren, wenn der Server während der Verarbeitung einer eingehenden Nachricht gelöscht wird.
SERVER_NOT_ONLINE	<i>server-ID</i> Der Server ist nicht online.	Der Transfer Family Family-Server ist offline. Starten Sie den Server, damit er Nachrichten empfangen und verarbeiten kann.

Code	Fehler	Beschreibung und Lösung
SIGNING_FAILED	Die Datei konnte nicht signiert werden.	Die zu sendende Datei ist nicht zum Signieren verfügbar , oder das Signieren konnte nicht durchgeführt werden. Vergewissern Sie sich, dass sich die Datei am erwarteten AS2-Speicherort befindet und dass Sie AWS Transfer Family über die Leseberechtigung für die Datei verfügen.
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	Für das Profil wurde kein Zertifikat gefunden: <i>local-profile-ID</i> .	Es wird versucht, eine ausgehende Nachricht zu signieren, aber es wurden keine Signaturzertifikate für das lokale Profil gefunden. Lösungsoptionen: • Stellen Sie sicher, dass dem lokalen Profil ein Zertifikat und ein privater Schlüssel zum Signieren beigelegt sind. • Stellen Sie sicher, dass das Signaturzertifikat derzeit aktiv ist.

Code	Fehler	Beschreibung und Lösung
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	Der Hostname konnte nicht in IP-Adressen aufgelöst werden.	Transfer Family kann auf dem öffentlichen DNS-Server, der im AS2-Connector konfiguriert ist, keine DNS-zu-IP-Adressauflösung durchführen. Aktualisieren Sie den Connector so, dass er auf eine gültige Partner-URL verweist.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	Das Zeitlimit für die Verbindung zum Endpunkt wurde überschritten.	Transfer Family kann keine Socketverbindung zum AS2-Server des konfigurierten Partners herstellen. Stellen Sie sicher, dass der AS2-Server des Partners unter der konfigurierten IP-Adresse verfügbar ist.
UNABLE_TO_RESOLVE_HOSTNAME	Der <i>hostname</i> Hostname konnte nicht aufgelöst werden.	Der Transfer Family Family-Server konnte den Hostnamen des Partners mithilfe eines öffentlichen DNS-Servers nicht auflösen. Vergewissern Sie sich, dass der konfigurierte Host registriert ist und ob der DNS-Eintrag bereits veröffentlicht wurde.

Code	Fehler	Beschreibung und Lösung
VERIFICATION_FAILED	Die Signaturüberprüfung für die AS2-Nachricht ist fehlgeschlagen <i>message-ID</i> oder ein MIC-Code stimmte nicht überein.	Stellen Sie sicher, dass das Signaturzertifikat des Absenders mit den Signaturzertifikaten für das Remote-Profil übereinstimmt. Überprüfen Sie auch, ob die MIC-Algorithmen kompatibel sind mit AWS Transfer Family.
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- Im Profil konnte kein öffentliches Zertifikat gefunden werden, das mit der Nachrichtensignatur übereinstimmt: <i>partner-profile-ID</i>. - Zertifikate für ein nicht vorhandenes Profil können nicht abgerufen werden: <i>partner-profile-ID</i>. - Im Profil wurde kein gültiges Zertifikat gefunden: <i>partner-profile-ID</i>.	AWS Transfer Family versucht, die Signatur für eine empfangene Nachricht zu überprüfen, aber es wurde kein passendes Signaturzertifikat für das Partnerprofil gefunden. Lösungsoptionen: - Stellen Sie sicher, dass dem Partnerprofil ein Signaturzertifikat beigelegt ist. - Stellen Sie sicher, dass das Zertifikat derzeit aktiv ist. - Stellen Sie sicher, dass das Zertifikat das richtige Signaturzertifikat für den Partner ist.

Überwachung des Ablaufs von Zertifikaten

AWS Transfer Family überwacht automatisch die Ablaufdaten von AS2-Zertifikaten und veröffentlicht eine CloudWatch Amazon-Metrik, mit der Sie nachverfolgen können, wann Zertifikate bald ablaufen.

Auf diese Weise können Sie Zertifikatserneuerungen proaktiv verwalten und Serviceunterbrechungen vermeiden.

DaysUntilExpiry Metrik

Wenn Sie ein Zertifikat für die Verwendung mit AS2 importieren, erstellt Transfer Family automatisch eine CloudWatch Metrik namens `DaysUntilExpiry`. Diese Metrik verfolgt die Anzahl der Tage, die bis zum Ablauf des Zertifikats verbleiben, basierend auf den Werten, die `InactiveDate` Sie beim Import des Zertifikats angegeben haben.

Angaben zur Metrik:

- Name der Metrik: `DaysUntilExpiry`
- Namespace: `AWS/Transfer`
- Abmessungen: `CertificateId` (immer vorhanden), `Description` (falls beim Import des Zertifikats angegeben)
- Einheiten: Anzahl (Tage)
- Häufigkeit: Wird täglich veröffentlicht

Important

Nach dem Import eines Zertifikats kann es bis zu einem ganzen Tag dauern, bis Transfer Family diese Metrik an Ihr Konto sendet.

Der Metrikwert sinkt jeden Tag um eins, wenn sich das Zertifikat seinem Inaktivitätsdatum nähert. Wenn ein Zertifikat beispielsweise noch 30 Tage bis zum Ablauf hat, zeigt die Metrik 30, am nächsten Tag dann 29 usw.

Bewährte Methoden für die Zertifikatsüberwachung

Folgen Sie diesen bewährten Methoden, wenn Sie die Überwachung des Ablaufs von Zertifikaten einrichten:

- Legen Sie mehrere Schwellenwerte für Warnmeldungen fest: Erstellen Sie Alarme für verschiedene Zeiträume (z. B. 30 Tage, 14 Tage und 7 Tage vor Ablauf), um ausreichend Zeit für die Verlängerung des Zertifikats zu haben.

- Verwenden Sie geeignete Statistiken: Verwenden Sie die Maximum Statistik bei der Erstellung von Alarmen, um sicherzustellen, dass Sie den neuesten Metrikwert erfassen.
- Konfigurieren Sie die richtigen Alarmaktionen: Richten Sie Benachrichtigungen ein, um die entsprechenden Teammitglieder darüber zu informieren, welche Zertifikate verlängern können.
- Testen Sie Ihre Benachrichtigungen: Testen Sie Ihr Benachrichtigungssystem regelmäßig, um sicherzustellen, dass Benachrichtigungen ordnungsgemäß zugestellt werden.
- Dokumentieren Sie Ihren Prozess: Bewahren Sie Unterlagen über Ihren Prozess zur Zertifikatserneuerung auf und legen Sie fest, wer für die verschiedenen Zertifikate verantwortlich ist.

Beispiele für Alarmkonfigurationen

Hier sind einige Beispiele für Alarmkonfigurationen für verschiedene Benachrichtigungsszenarien:

30-tägige Ablaufwarnung

Erstellen Sie einen Alarm, der ausgelöst wird, wenn ein Zertifikat innerhalb von 30 Tagen oder weniger abläuft:

- Metrik: DaysUntilExpiry
- Statistik: Maximum
- Zeitraum: 1 Tag
- Schwellenwert: 30
- Vergleich: Weniger als oder gleich dem Schwellenwert
- Behandlung fehlender Daten: Behandeln Sie fehlende Daten als gut (nicht als Verletzung)

Kritische 7-Tage-Ablaufwarnung

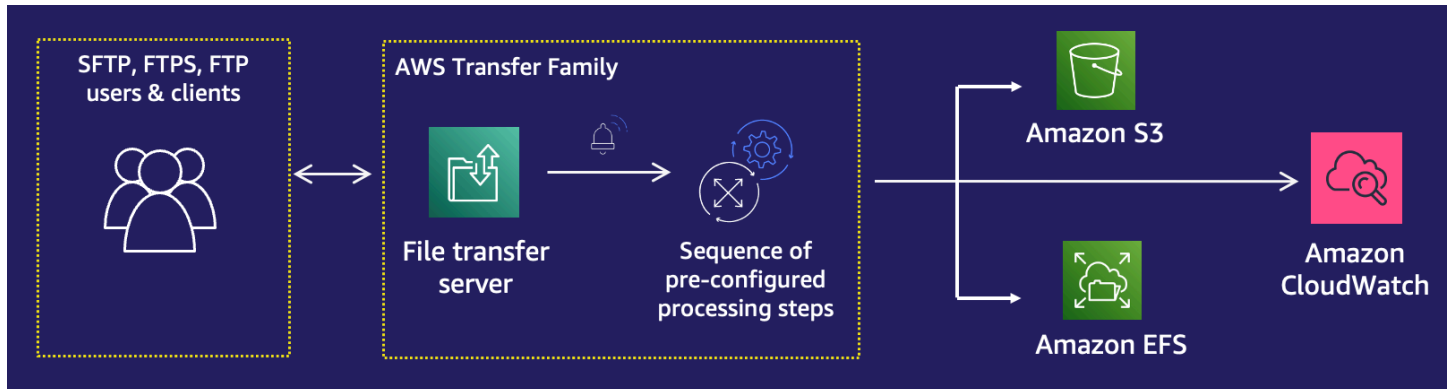
Erstellen Sie einen kritischen Alarm, der ausgelöst wird, wenn ein Zertifikat innerhalb von 7 Tagen oder weniger abläuft:

- Metrik: DaysUntilExpiry
- Statistik: Maximum
- Zeitraum: 1 Tag
- Schwellenwert: 7

- Vergleich: Weniger als oder gleich dem Schwellenwert
- Behandlung fehlender Daten: Behandeln Sie fehlende Daten als gut (nicht als Verletzung)

AWS Transfer Family verwaltete Workflows

AWS Transfer Family unterstützt verwaltete Workflows für die Dateiverarbeitung. Mit verwalteten Workflows können Sie einen Workflow starten, nachdem eine Datei über SFTP, FTPS oder FTP übertragen wurde. Mit dieser Funktion können Sie Ihre Compliance-Anforderungen für den Dateiaustausch zwischen Unternehmen (B2B) sicher und kostengünstig erfüllen, indem Sie alle für die Dateiverarbeitung erforderlichen Schritte koordinieren. Darüber hinaus profitieren Sie von einer umfassenden Prüfung und Transparenz.



Durch die Orchestrierung von Dateiverarbeitungsaufgaben helfen Ihnen verwaltete Workflows dabei, Daten vorzuverarbeiten, bevor sie von Ihren nachgelagerten Anwendungen verwendet werden. Zu diesen Aufgaben zur Dateiverarbeitung können gehören:

- Dateien in benutzerspezifische Ordner verschieben.
- Entschlüsseln von Dateien als Teil eines Workflows.
- Dateien taggen.
- Durchführung einer benutzerdefinierten Verarbeitung durch Erstellen und Anhängen einer AWS Lambda Funktion an einen Workflow.
- Senden von Benachrichtigungen, wenn eine Datei erfolgreich übertragen wurde. (Einen Blogbeitrag, in dem dieser Anwendungsfall detailliert beschrieben wird, finden [Sie unter Anpassen von Benachrichtigungen zur Dateizustellung mithilfe AWS Transfer Family verwalteter Workflows.](#))

Um häufig auftretende Aufgaben zur Dateiverarbeitung nach dem Upload, die sich über mehrere Geschäftsbereiche in Ihrem Unternehmen erstrecken, schnell zu replizieren und zu standardisieren, können Sie Workflows mithilfe von Infrastructure as Code (IaC) bereitstellen. Sie können einen verwalteten Workflow angeben, der für vollständig hochgeladene Dateien initiiert wird. Sie können auch einen anderen verwalteten Workflow angeben, der für Dateien initiiert werden soll, die

aufgrund einer vorzeitigen Sitzungsunterbrechung nur teilweise hochgeladen wurden. Built-in Die Ausnahmebehandlung hilft Ihnen, schnell auf Ergebnisse der Dateiverarbeitung zu reagieren, und bietet Ihnen gleichzeitig die Kontrolle darüber, wie mit Fehlern umgegangen werden soll. Darüber hinaus erstellt jeder Workflow-Schritt detaillierte Protokolle, die Sie überprüfen können, um die Herkunft der Daten nachzuverfolgen.

Führen Sie zunächst die folgenden Aufgaben aus:

1. Richten Sie Ihren Workflow so ein, dass er je nach Ihren Anforderungen Vorverarbeitungsaktionen wie Kopieren, Markieren und andere Schritte enthält. Details dazu finden Sie unter [Erstellen Sie einen Workflow](#).
2. Konfigurieren Sie eine Ausführungsrolle, die Transfer Family zur Ausführung des Workflows verwendet. Details dazu finden Sie unter [IAM-Richtlinien für Workflows](#).
3. Ordnen Sie den Workflow einem Server zu, sodass die in diesem Workflow angegebenen Aktionen beim Eintreffen der Datei in Echtzeit ausgewertet und initiiert werden. Details dazu finden Sie unter [Konfigurieren Sie einen Workflow und führen Sie ihn aus](#).

Ähnliche Informationen

- Informationen zur Überwachung Ihrer Workflow-Ausführungen finden Sie unter [Verwenden von CloudWatch Metriken für Transfer Family Family-Server](#).
- Ausführliche Ausführungsprotokolle und Informationen zur Fehlerbehebung finden Sie unter [Workflow-bezogene Fehler mithilfe von Amazon beheben CloudWatch](#).
- Transfer Family bietet einen Blogbeitrag und einen Workshop, die Sie durch den Aufbau einer Dateiübertragungslösung führen. Diese Lösung nutzt AWS Transfer Family für verwaltete SFTP/FTPS Endgeräte sowie Amazon Cognito und DynamoDB für die Benutzerverwaltung.

Der Blogbeitrag ist unter [Amazon Cognito als Identitätsanbieter mit AWS Transfer Family Amazon S3 verwenden](#) verfügbar. Die Details zum Workshop finden Sie [hier](#).

- Unter [AWS Transfer Family Verwaltete Workflows](#) finden Sie eine kurze Einführung in die Workflows von Transfer Family.
- [Der folgende Workshop bietet praktische Übungen zur Erstellung vollautomatischer und ereignisgesteuerter Workflows, die die Übertragung von Dateien zu oder von externen SFTP-Servern zu Amazon S3 sowie die allgemeine Vor- und Nachverarbeitung dieser Dateien beinhalten: MFT-Workshop. Event-driven](#)

Dieses Video bietet einen Überblick über diesen Workshop.

Themen

- [Erstellen Sie einen Workflow](#)
- [Verwenden Sie vordefinierte Schritte](#)
- [Verwenden Sie benutzerdefinierte Schritte zur Dateiverarbeitung](#)
- [IAM-Richtlinien für Workflows](#)
- [Ausnahmebehandlung für einen Workflow](#)
- [Überwachen Sie die Workflow-Ausführung](#)
- [Erstellen Sie einen Workflow aus einer Vorlage](#)
- [Einen Workflow von einem Transfer Family Family-Server entfernen](#)
- [Einschränkungen und Einschränkungen verwalteter Workflows](#)

Weitere Hilfe zu den ersten Schritten mit verwalteten Workflows finden Sie in den folgenden Ressourcen:

- AWS Transfer Family Demovideo zu [verwalteten Workflows](#)
- Blogbeitrag zum [Aufbau einer Cloud-nativen Dateiübertragungsplattform mithilfe von AWS Transfer Family Workflows](#)

Erstellen Sie einen Workflow

Sie können einen verwalteten Workflow mithilfe von erstellen AWS-Managementkonsole, wie in diesem Thema beschrieben. Um den Prozess der Workflow-Erstellung so einfach wie möglich zu gestalten, sind für die meisten Abschnitte der Konsole kontextuelle Hilfebereiche verfügbar.

Ein Workflow besteht aus zwei Arten von Schritten:

- **Nominale Schritte** — Nominale Schritte sind Schritte zur Dateiverarbeitung, die Sie auf eingehende Dateien anwenden möchten. Wenn Sie mehr als einen nominalen Schritt auswählen, wird jeder Schritt in einer linearen Reihenfolge verarbeitet.
- **Exception-handling Schritte** — Ausnahmebehandlungsroutinen sind Schritte zur Dateiverarbeitung, die AWS Transfer Family ausgeführt werden, falls nominale Schritte fehlschlagen oder zu Validierungsfehlern führen.

Erstellen Sie einen Workflow

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Workflows aus.
3. Wählen Sie auf der Seite Workflows die Option Workflow erstellen aus.
4. Geben Sie auf der Seite Workflow erstellen eine Beschreibung ein. Diese Beschreibung wird auf der Seite Workflows angezeigt.
5. Wählen Sie im Abschnitt Nominale Schritte die Option Schritt hinzufügen aus. Fügen Sie einen oder mehrere Schritte hinzu.
 - a. Wählen Sie einen Schritttyp aus den verfügbaren Optionen aus. Weitere Informationen zu den verschiedenen Schritttypen finden Sie unter [the section called “Verwenden Sie vordefinierte Schritte”](#).
 - b. Wählen Sie Weiter und konfigurieren Sie dann die Parameter für den Schritt.
 - c. Wählen Sie Weiter und überprüfen Sie dann die Details für den Schritt.
 - d. Wählen Sie Schritt erstellen, um den Schritt hinzuzufügen und fortzufahren.
 - e. Fügen Sie nach Bedarf weitere Schritte hinzu. Die maximale Anzahl von Schritten in einem Workflow beträgt 8.
 - f. Nachdem Sie alle erforderlichen nominalen Schritte hinzugefügt haben, scrollen Sie nach unten zum Abschnitt Ausnahmehandler — optional und wählen Sie Schritt hinzufügen aus.
6. Um Ausnahmehandler zu konfigurieren, fügen Sie Schritte auf die gleiche Weise wie zuvor beschrieben hinzu. Wenn eine Datei dazu führt, dass ein Schritt eine Ausnahme auslöst, werden Ihre Ausnahmehandlungsroutinen nacheinander aufgerufen.
7. (Optional) Scrollen Sie nach unten zum Abschnitt „Tags“ und fügen Sie Tags für Ihren Workflow hinzu.
8. Überprüfen Sie die Konfiguration und wählen Sie Workflow erstellen aus.

Note

Damit Sie in Echtzeit über Fehler informiert werden, empfehlen wir Ihnen, Ausnahmehandlungsroutinen und Schritte einzurichten, die ausgeführt werden, wenn Ihr Workflow fehlschlägt.

 Important

Nachdem Sie einen Workflow erstellt haben, können Sie ihn nicht mehr bearbeiten. Überprüfen Sie die Konfiguration daher sorgfältig.

Konfigurieren Sie einen Workflow und führen Sie ihn aus

Bevor Sie einen Workflow ausführen können, müssen Sie ihn einem Transfer Family Family-Server zuordnen.

So konfigurieren Sie Transfer Family so, dass ein Workflow für hochgeladene Dateien ausgeführt wird

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server aus.
 - Um den Workflow zu einem vorhandenen Server hinzuzufügen, wählen Sie den Server aus, den Sie für Ihren Workflow verwenden möchten.
 - Alternativ können Sie einen neuen Server erstellen und den Workflow hinzufügen. Weitere Informationen finden Sie unter [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#).
3. Scrollen Sie auf der Detailseite für den Server nach unten zum Abschnitt Zusätzliche Details und wählen Sie dann Bearbeiten aus.

 Note

Standardmäßig sind Servern keine Workflows zugeordnet. Sie verwenden den Abschnitt Zusätzliche Details, um dem ausgewählten Server einen Workflow zuzuordnen.

4. Wählen Sie auf der Seite Zusätzliche Details bearbeiten im Abschnitt Verwaltete Workflows einen Workflow aus, der für alle Uploads ausgeführt werden soll.

 Note

Wenn Sie noch keinen Workflow haben, wählen Sie Neuen Workflow erstellen aus, um einen zu erstellen.

- a. Wählen Sie die zu verwendende Workflow-ID aus.
- b. Wählen Sie eine Ausführungsrolle aus. Dies ist die Rolle, die Transfer Family bei der Ausführung der Workflow-Schritte einnimmt. Weitere Informationen finden Sie unter [IAM-Richtlinien für Workflows](#). Wählen Sie Save (Speichern) aus.

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#) [external link]

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#) [external link]

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

Note

Wenn Sie nicht mehr möchten, dass ein Workflow dem Server zugeordnet wird, können Sie die Zuordnung entfernen. Details hierzu finden Sie unter [Einen Workflow von einem Transfer Family Family-Server entfernen](#).

Um einen Workflow auszuführen

Um einen Workflow auszuführen, laden Sie eine Datei auf einen Transfer Family Family-Server hoch, den Sie mit einem zugehörigen Workflow konfiguriert haben.

Note

Jedes Mal, wenn Sie einen Workflow von einem Server entfernen und ihn durch einen neuen ersetzen oder die Serverkonfiguration aktualisieren (was sich auf die Ausführungsrolle eines Workflows auswirkt), müssen Sie etwa 10 Minuten warten, bevor Sie den neuen Workflow

ausführen. Der Transfer Family Family-Server speichert die Workflow-Details im Cache, und es dauert 10 Minuten, bis der Server seinen Cache aktualisiert hat.

Darüber hinaus müssen Sie sich von allen aktiven SFTP-Sitzungen abmelden und sich nach Ablauf der 10-minütigen Wartezeit wieder anmelden, um die Änderungen zu sehen.

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

Nachdem Ihre Datei hochgeladen wurde, wird die definierte Aktion an Ihrer Datei ausgeführt. Wenn Ihr Workflow beispielsweise einen Kopierschritt enthält, wird die Datei an den Speicherort kopiert, den Sie in diesem Schritt definiert haben. Sie können Amazon CloudWatch Logs verwenden, um die ausgeführten Schritte und ihren Ausführungsstatus nachzuverfolgen.

Workflow-Details anzeigen

Sie können Details zu zuvor erstellten Workflows oder zu Workflow-Ausführungen anzeigen. Um diese Details anzuzeigen, können Sie die Konsole oder die AWS Command Line Interface (AWS CLI) verwenden.

Console

Workflow-Details anzeigen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Workflows aus.
3. Wählen Sie auf der Workflow-Seite einen Workflow aus.

Die Seite mit den Workflow-Details wird geöffnet.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with links to Servers, Connectors, AS2 Trading Partners, Certificates, Profiles, Workflows (selected), Feature Spotlight, What's New, and Documentation. The main content area displays details for a specific workflow. At the top, there's a breadcrumb trail: Transfer Family > Workflows > w-1234567890abcdef0. A 'Delete' button is in the top right corner. The 'Description' section shows the workflow name 'Test my workflow' and its description 'Test workflow A'. Below this is the 'Nominal steps (1)' section, which contains a table with one step: a 'tag_step' of type 'TAG'. The 'Exception handlers (1)' section also contains a table with one handler: 'delete_if_exception' of type 'DELETE'. The 'In-flight executions (0)' section shows a search bar and a table with no data, indicating 'No executions to display'. At the bottom, the 'Tags (1)' section includes a 'Manage tags' button and a note about using tags to organize workflows.

CLI

Verwenden Sie den `describe-workflow` CLI-Befehl, um die Workflow-Details anzuzeigen, wie im folgenden Beispiel gezeigt. Ersetzen Sie die Workflow-ID `w-1234567890abcdef0` durch Ihren eigenen Wert. Weitere Informationen finden Sie unter [describe-workflow](#) in der AWS CLI Befehlsreferenz.

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
  "Workflow": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/w-1234567890abcdef0",
    "WorkflowId": "w-1234567890abcdef0",
    "Name": "Copy file to shared_files",
    "Steps": [
      {
```

```

        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "amzn-s3-demo-bucket",
              "Key": "home/shared_files/"
            }
          }
        }
      ],
      "OnException": {}
    }
  }
}

```

Wenn Ihr Workflow als Teil eines AWS CloudFormation Stacks erstellt wurde, können Sie den Workflow mit der CloudFormation Konsole () <https://console.aws.amazon.com/cloudformation> verwalten.

Transfer Family > Workflows > w-

W-
Delete

i This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name	Workflow description
Stack-managed	Workflow for blogpost

Nominal steps (4) [Info](#)

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

Verwenden Sie vordefinierte Schritte

Wenn Sie einen Workflow erstellen, können Sie wählen, ob Sie einen der folgenden vordefinierten Schritte hinzufügen möchten, die in diesem Thema beschrieben werden. Sie können auch Ihre eigenen benutzerdefinierten Dateiverarbeitungsschritte hinzufügen. Weitere Informationen finden Sie unter [the section called “Verwenden Sie benutzerdefinierte Schritte zur Dateiverarbeitung”](#).

Themen

- [Datei kopieren](#)
- [Datei entschlüsseln](#)
- [Datei kennzeichnen](#)
- [Datei löschen](#)
- [Benannte Variablen für Workflows](#)
- [Beispiel für einen Workflow zum Markieren und Löschen](#)

Datei kopieren

Ein Schritt „Datei kopieren“ erstellt eine Kopie der hochgeladenen Datei an einem neuen Amazon S3 S3-Speicherort. Derzeit können Sie den Schritt „Datei kopieren“ nur mit Amazon S3 verwenden.

Der folgende Schritt zum Kopieren von Dateien kopiert Dateien in den test Ordner in *amzn-s3-demo-destination-bucket*.

Wenn der Schritt „Datei kopieren“ nicht der erste Schritt Ihres Workflows ist, können Sie den Speicherort der Datei angeben. Durch Angabe des Dateispeicherorts können Sie entweder die Datei, die im vorherigen Schritt verwendet wurde, oder die Originaldatei, die hochgeladen wurde, kopieren. Sie können diese Funktion verwenden, um mehrere Kopien der Originaldatei zu erstellen und gleichzeitig die Quelldatei für die Dateiarchivierung und Aufbewahrung von Aufzeichnungen intakt zu lassen. Ein Beispiel finden Sie unter [Beispiel für einen Workflow zum Markieren und Löschen](#).

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

Geben Sie den Bucket und die wichtigsten Details an

Sie müssen den Bucket-Namen und einen Schlüssel für das Ziel des Schritts „Datei kopieren“ angeben. Der Schlüssel kann entweder ein Pfadname oder ein Dateiname sein. Ob der Schlüssel als Pfad- oder Dateiname behandelt wird, hängt davon ab, ob Sie den Schlüssel mit einem Schrägstrich (/) beenden.

Wenn das letzte Zeichen ist/, wird Ihre Datei in den Ordner kopiert, und ihr Name ändert sich nicht. Wenn das letzte Zeichen alphanumerisch ist, wird Ihre hochgeladene Datei in den Schlüsselwert

umbenannt. Wenn in diesem Fall bereits eine Datei mit diesem Namen existiert, hängt das Verhalten von der Einstellung für das Feld Bestehende überschreiben ab.

- Wenn Bestehende überschreiben ausgewählt ist, wird die vorhandene Datei durch die Datei ersetzt, die gerade verarbeitet wird.
- Wenn „Bestehende überschreiben“ nicht ausgewählt ist, passiert nichts und die Workflow-Verarbeitung wird gestoppt.

 Tip

Wenn gleichzeitige Schreibvorgänge auf demselben Dateipfad ausgeführt werden, kann dies zu unerwartetem Verhalten beim Überschreiben von Dateien führen.

Wenn Ihr Schlüsselwert beispielsweise lautet `test/`, werden Ihre hochgeladenen Dateien in den `test` Ordner kopiert. Wenn Ihr Schlüsselwert ist (und Bestehende überschreiben ausgewählt ist) `test/today`, wird jede Datei, die Sie hochladen, in eine Datei mit dem Namen `today` im `test` Ordner kopiert, und jede nachfolgende Datei überschreibt die vorherige.

 Note

Amazon S3 unterstützt Buckets und Objekt. Es gibt keine Hierarchie in Amazon S3. Sie können jedoch Präfixe und Trennzeichen in Objektschlüsselnamen verwenden, um eine Hierarchie zu implizieren und Ihre Daten ähnlich wie in Ordnern zu organisieren.

Verwenden Sie eine benannte Variable in einem Schritt zum Kopieren von Dateien

In einem Schritt zum Kopieren von Dateien können Sie eine Variable verwenden, um Ihre Dateien dynamisch in benutzerspezifische Ordner zu kopieren. Derzeit können Sie `${transfer:UserName}` oder `${transfer:UploadDate}` als Variable verwenden, um Dateien an einen Zielort für den Benutzer zu kopieren, der gerade Dateien hochlädt, oder auf der Grundlage des aktuellen Datums.

Wenn der Benutzer im folgenden Beispiel eine Datei `richard-roe` hochlädt, wird sie in den `amzn-s3-demo-destination-bucket/richard-roe/processed/` Ordner kopiert. Wenn der Benutzer eine Datei `mary-major` hochlädt, wird sie in den `amzn-s3-demo-destination-bucket/mary-major/processed/` Ordner kopiert.

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

In ähnlicher Weise können Sie die Variable `${transfer:UploadDate}` als Variable verwenden, um Dateien an einen Zielort zu kopieren, der nach dem aktuellen Datum benannt ist. Wenn Sie im folgenden Beispiel das Ziel `${transfer:UploadDate}/processed` auf den 1. Februar 2022 festlegen, werden die hochgeladenen Dateien in den `amzn-s3-demo-destination-bucket/2022-02-01/processed/` Ordner kopiert.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

Sie können diese beiden Variablen auch zusammen verwenden und so ihre Funktionalität kombinieren. Sie könnten beispielsweise das Zielschlüsselpräfix auf festlegen **folder/** `${transfer:UserName}/${transfer:UploadDate}/`, wodurch beispielsweise `folder/marymajor/2023-01-05/` verschachtelte Ordner erstellt würden.

IAM-Berechtigungen für den Kopierschritt

Damit ein Kopierschritt erfolgreich ausgeführt werden kann, stellen Sie sicher, dass die Ausführungsrolle für Ihren Workflow die folgenden Berechtigungen enthält.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
```

```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

Die `s3:ListBucket` Berechtigung ist nur erforderlich, wenn Sie Bestehende überschreiben nicht auswählen. Mit dieser Berechtigung wird in Ihrem Bucket überprüft, ob bereits eine Datei mit demselben Namen existiert. Wenn Sie Existierende überschreiben ausgewählt haben, muss der Workflow nicht nach der Datei suchen, sondern kann sie einfach schreiben. Wenn Ihre Amazon S3 S3-Dateien Tags haben, müssen Sie Ihrer IAM-Richtlinie eine oder zwei Berechtigungen hinzufügen.

- `s3:GetObjectTagging` Für eine Amazon S3 S3-Datei hinzufügen, die nicht versioniert ist.
- `s3:GetObjectVersionTagging` Für eine Amazon S3 S3-Datei hinzufügen, die versioniert ist.

Datei entschlüsseln

Der AWS Speicher-Blog enthält einen Beitrag, in dem beschrieben wird, wie Dateien mithilfe von Transfer Family Managed Workflows, Verschlüsseln und [Entschlüsseln von Dateien mit PGP und einfach entschlüsselt werden können, ohne Code zu](#) schreiben, beschrieben werden. AWS Transfer Family

Unterstützte symmetrische Verschlüsselungsalgorithmen

Für die PGP-Entschlüsselung unterstützt Transfer Family symmetrische Verschlüsselungsalgorithmen, mit denen die eigentlichen Dateidaten in PGP-Dateien verschlüsselt werden.

- Ausführliche Informationen zu den unterstützten symmetrischen Verschlüsselungsalgorithmen finden Sie unter. [Symmetrische PGP-Verschlüsselungsalgorithmen](#)
- Hinweise zu PGP-Schlüsselpaar-Algorithmen, die mit diesen symmetrischen Algorithmen verwendet werden, finden Sie unter. [PGP-Schlüsselpaar-Algorithmen](#)

Verwenden Sie die PGP-Entschlüsselung in Ihrem Workflow

Transfer Family bietet integrierte Unterstützung für die Pretty Good Privacy (PGP) -Entschlüsselung. Sie können die PGP-Entschlüsselung für Dateien verwenden, die über SFTP, FTPS oder FTP auf Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) hochgeladen werden.

Um die PGP-Entschlüsselung verwenden zu können, müssen Sie die privaten PGP-Schlüssel erstellen und speichern, die für die Entschlüsselung Ihrer Dateien verwendet werden. Ihre Benutzer können dann Dateien mit den entsprechenden PGP-Verschlüsselungsschlüsseln verschlüsseln, bevor sie die Dateien auf Ihren Transfer Family Family-Server hochladen. Nachdem Sie die verschlüsselten Dateien erhalten haben, können Sie diese Dateien in Ihrem Workflow entschlüsseln. Ein detailliertes Tutorial finden Sie unter [Einen verwalteten Workflow für die Entschlüsselung einer Datei einrichten](#).

Informationen zu unterstützten PGP-Algorithmen und Empfehlungen finden Sie unter. [PGP-Verschlüsselungs- und Entschlüsselungsalgorithmen](#)

So verwenden Sie die PGP-Entschlüsselung in Ihrem Workflow

1. Identifizieren Sie einen Transfer Family Family-Server, auf dem Ihr Workflow gehostet werden soll, oder erstellen Sie einen neuen. Sie benötigen die Server-ID, bevor Sie Ihre PGP-Schlüssel AWS Secrets Manager mit dem richtigen geheimen Namen speichern können.
2. Speichern Sie Ihren PGP-Schlüssel AWS Secrets Manager unter dem erforderlichen geheimen Namen. Details hierzu finden Sie unter [PGP-Schlüssel verwalten](#). Workflows können anhand des geheimen Namens in Secrets Manager automatisch den richtigen PGP-Schlüssel finden, der für die Entschlüsselung verwendet werden soll.

Note

Wenn Sie Geheimnisse im Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu den Preisen erhalten Sie unter [AWS Secrets Manager Preise](#).

3. Verschlüsseln Sie eine Datei mit Ihrem PGP-Schlüsselpaar. (Eine Liste der unterstützten Clients finden Sie unter [Unterstützte PGP-Clients](#).) Wenn Sie die Befehlszeile verwenden, führen Sie den folgenden Befehl aus. Um diesen Befehl zu verwenden, ersetzen Sie ihn durch die E-Mail-Adresse, *username@example.com* mit der Sie das PGP-Schlüsselpaar erstellt haben. *testfile.txt* Ersetzen Sie es durch den Namen der Datei, die Sie verschlüsseln möchten.

```
gpg -e -r username@example.com testfile.txt
```

Important

Achten Sie beim Verschlüsseln von Dateien zur Verwendung mit AWS Transfer Family Workflows immer darauf, dass Sie mithilfe des Parameters einen nicht anonymen Empfänger angeben. `-r` Anonyme Verschlüsselung (ohne Angabe eines Empfängers) kann zu Entschlüsselungsfehlern im Workflow führen, da das System nicht erkennen kann, welcher Schlüssel für die Entschlüsselung verwendet werden soll. Informationen zum Debuggen dieses Problems finden Sie unter [Beheben Sie Probleme mit der Verschlüsselung anonymer Empfänger](#)

4. Laden Sie die verschlüsselte Datei auf Ihren Transfer Family Family-Server hoch.
5. Konfigurieren Sie einen Entschlüsselungsschritt in Ihrem Workflow. Weitere Informationen finden Sie unter [Fügen Sie einen Entschlüsselungsschritt hinzu](#).

Fügen Sie einen Entschlüsselungsschritt hinzu

Ein Entschlüsselungsschritt entschlüsselt eine verschlüsselte Datei, die als Teil Ihres Workflows auf Amazon S3 oder Amazon EFS hochgeladen wurde. Einzelheiten zur Konfiguration der Entschlüsselung finden Sie unter [Verwenden Sie die PGP-Entschlüsselung in Ihrem Workflow](#)

Wenn Sie Ihren Entschlüsselungsschritt für einen Workflow erstellen, müssen Sie das Ziel für die entschlüsselten Dateien angeben. Sie müssen auch auswählen, ob vorhandene Dateien überschrieben werden sollen, wenn am Zielspeicherort bereits eine Datei vorhanden ist. Mit Amazon CloudWatch Logs können Sie die Ergebnisse des Entschlüsselungsworkflows überwachen und Prüfprotokolle für jede Datei in Echtzeit abrufen.

Nachdem Sie den Dateityp Entschlüsseln für Ihren Schritt ausgewählt haben, wird die Seite „Parameter konfigurieren“ angezeigt. Geben Sie die Werte für den Abschnitt PGP-Entschlüsselungsparameter konfigurieren ein.

Die verfügbaren Optionen lauten wie folgt:

- **Schrittname** — Geben Sie einen aussagekräftigen Namen für den Schritt ein.
- **Dateispeicherort** — Durch Angabe des Dateispeicherorts können Sie entweder die Datei, die im vorherigen Schritt verwendet wurde, oder die Originaldatei, die hochgeladen wurde, entschlüsseln.

 Note

Dieser Parameter ist nicht verfügbar, wenn dieser Schritt der erste Schritt des Workflows ist.

- **Ziel für entschlüsselte Dateien** — Wählen Sie einen Amazon S3 S3-Bucket oder ein Amazon EFS-Dateisystem als Ziel für die entschlüsselte Datei.
 - Wenn Sie sich für Amazon S3 entscheiden, müssen Sie einen Ziel-Bucket-Namen und ein Zielschlüsselpräfix angeben. Um das Zielschlüsselpräfix nach Benutzername zu parametrisieren, geben Sie **`${transfer:UserName}`** als Zielschlüsselpräfix ein. Um das Zielschlüsselpräfix anhand des Upload-Datums zu parametrisieren, geben **`${Transfer:UploadDate}`** Sie in ähnlicher Weise das Zielschlüsselpräfix ein.
 - Wenn Sie Amazon EFS wählen, müssen Sie ein Zieldateisystem und einen Pfad angeben.

 Note

Die Speicheroption, die Sie hier auswählen, muss mit dem Speichersystem übereinstimmen, das vom Transfer Family Family-Server verwendet wird, mit dem dieser Workflow verknüpft ist. Andernfalls erhalten Sie eine Fehlermeldung, wenn Sie versuchen, diesen Workflow auszuführen.

- **Bestehende überschreiben** — Wenn Sie eine Datei hochladen und am Ziel bereits eine Datei mit demselben Dateinamen vorhanden ist, hängt das Verhalten von der Einstellung für diesen Parameter ab:
 - Wenn „Bestehende überschreiben“ ausgewählt ist, wird die bestehende Datei durch die Datei ersetzt, die gerade verarbeitet wird.
 - Wenn „Bestehende überschreiben“ nicht ausgewählt ist, passiert nichts und die Workflow-Verarbeitung wird gestoppt.

 Tip

Wenn gleichzeitige Schreibvorgänge auf demselben Dateipfad ausgeführt werden, kann dies zu unerwartetem Verhalten beim Überschreiben von Dateien führen.

Der folgende Screenshot zeigt ein Beispiel für die Optionen, die Sie für den Schritt „Datei entschlüsseln“ wählen könnten.

Step 1

[Choose step type](#)

Step 2

Configure parameters

Step 3

Review and create

Configure parameters

Configure PGP decryption parameters

Store your PGP private key(s) and passphrase(s) in AWS Secrets Manager. [Learn more](#)

 Refer to the [AWS Transfer Family pricing page](#) for pricing details. 

Step name

File location

Select the file location to use as an input for this step

- ☒ **Apply on the file created from the previous step**
Input file is selected from the previous step's output
- ☐ **Apply on the original file**
Originally uploaded file

Destination for decrypted files

Choose an S3 bucket or an EFS file system for storing decrypted files.

☒ **Amazon S3**
Store your decrypted files as Amazon S3 objects

☐ **Amazon EFS**
Store your decrypted files in an EFS file system

Destination bucket name

Destination key prefix

If you are decrypting files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize the destination prefix by username or upload date respectively.

- ☐ **Overwrite existing**
Overwrite if a file with the same file name already exists at the destination.

Schritt „IAM-Berechtigungen für die Entschlüsselung“

Damit ein Entschlüsselungsschritt erfolgreich ausgeführt werden kann, stellen Sie sicher, dass die Ausführungsrolle für Ihren Workflow die folgenden Berechtigungen enthält.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
  ],
  "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

Die `s3:ListBucket` Berechtigung ist nur erforderlich, wenn Sie Bestehende überschreiben nicht auswählen. Mit dieser Berechtigung wird in Ihrem Bucket überprüft, ob bereits eine Datei mit demselben Namen existiert. Wenn Sie Existierende überschreiben ausgewählt haben, muss der Workflow nicht nach der Datei suchen, sondern kann sie einfach schreiben. Wenn Ihre Amazon S3 S3-Dateien Tags haben, müssen Sie Ihrer IAM-Richtlinie eine oder zwei Berechtigungen hinzufügen.

- `s3:GetObjectTagging` Für eine Amazon S3 S3-Datei hinzufügen, die nicht versioniert ist.
- `s3:GetObjectVersionTagging` Für eine Amazon S3 S3-Datei hinzufügen, die versioniert ist.

Datei kennzeichnen

Verwenden Sie einen Tag-Schritt, um eingehende Dateien für die weitere Verarbeitung zu kennzeichnen. Geben Sie den Wert des Tags ein, das Sie den eingehenden Dateien zuweisen möchten. Derzeit wird der Tag-Vorgang nur unterstützt, wenn Sie Amazon S3 für Ihren Transfer Family Family-Serverspeicher verwenden.

Der folgende Beispiel-Tag-Schritt weist `scan_outcome` und `clean` als Tag-Schlüssel bzw. -Wert zu.

The screenshot shows the 'Configure tag parameters' step in the AWS Transfer Family console. It includes a 'Step name' field with the value 'tag scan'. Under 'File location', the option 'Tag the file created from previous step' is selected. The 'Tags' section shows a table with one entry: 'scan_outcome' as the Key and 'clean' as the Value. There are buttons for 'Remove tag' and 'Add tag'.

Key	Value
scan_outcome	clean

Damit ein Tag-Schritt erfolgreich ausgeführt werden kann, stellen Sie sicher, dass die Ausführungsrolle für Ihren Workflow die folgenden Berechtigungen enthält.

```
{
```

```
"Sid": "Tag",
"Effect": "Allow",
"Action": [
    "s3:PutObjectTagging",
    "s3:PutObjectVersionTagging"
],
"Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
]
}
```

Note

Wenn Ihr Workflow einen Tag-Schritt enthält, der entweder vor einem Kopier- oder Entschlüsselungsschritt ausgeführt wird, müssen Sie Ihrer IAM-Richtlinie eine oder zwei Berechtigungen hinzufügen.

- `s3:GetObjectTagging` Für eine Amazon S3 S3-Datei hinzufügen, die nicht versioniert ist.
- `s3:GetObjectVersionTagging` Für eine Amazon S3 S3-Datei hinzufügen, die versioniert ist.

Datei löschen

Um eine verarbeitete Datei aus einem vorherigen Workflow-Schritt oder die ursprünglich hochgeladene Datei zu löschen, verwenden Sie einen Schritt „Datei löschen“.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

Damit ein Löschschritt erfolgreich ausgeführt werden kann, stellen Sie sicher, dass die Ausführungsrolle für Ihren Workflow die folgenden Berechtigungen enthält.

```
{
    "Sid": "Delete",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
* "
}
```

Benannte Variablen für Workflows

Für Schritte zum Kopieren und Entschlüsseln können Sie eine Variable verwenden, um Aktionen dynamisch auszuführen. AWS Transfer Family unterstützt derzeit die folgenden benannten Variablen.

- Wird verwendet `${transfer:UserName}`, um Dateien an ein Ziel zu kopieren oder zu entschlüsseln, das auf dem Benutzer basiert, der die Dateien hochlädt.
- Wird verwendet `${transfer:UploadDate}`, um Dateien auf der Grundlage des aktuellen Datums an einen Zielort zu kopieren oder zu entschlüsseln.

Beispiel für einen Workflow zum Markieren und Löschen

Das folgende Beispiel zeigt einen Workflow, der eingehende Dateien kennzeichnet, die von einer nachgelagerten Anwendung, z. B. einer Datenanalyseplattform, verarbeitet werden müssen. Nach dem Markieren der eingehenden Datei löscht der Workflow dann die ursprünglich hochgeladene Datei, um Speicherkosten zu sparen.

Console

Beispiel für einen Arbeitsablauf zum Markieren und Verschieben

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Workflows aus.

3. Wählen Sie auf der Seite Workflows die Option Workflow erstellen aus.
4. Geben Sie auf der Seite Workflow erstellen eine Beschreibung ein. Diese Beschreibung wird auf der Seite Workflows angezeigt.
5. Fügen Sie den ersten Schritt hinzu (Kopie).
 - a. Wählen Sie im Abschnitt Nominale Schritte die Option Schritt hinzufügen aus.
 - b. Wählen Sie „Datei kopieren“ und anschließend „Weiter“.
 - c. Geben Sie einen Schrittnamen ein und wählen Sie dann einen Ziel-Bucket und ein key prefix aus.

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure copy parameters

Step name
copy-step-first-step

Destination bucket name
example-bucket ▼

Destination key prefix
If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.
test/

☐ Overwrite existing

- d. Wählen Sie Weiter und überprüfen Sie dann die Details für den Schritt.
 - e. Wählen Sie Schritt erstellen, um den Schritt hinzuzufügen und fortzufahren.
6. Fügen Sie den zweiten Schritt (Tag) hinzu.
 - a. Wählen Sie im Abschnitt Nominale Schritte die Option Schritt hinzufügen aus.
 - b. Wählen Sie „Datei taggen“ und anschließend „Weiter“.
 - c. Geben Sie einen Schrittnamen ein.
 - d. Wählen Sie für Dateispeicherort die Option Datei kennzeichnen, die im vorherigen Schritt erstellt wurde.
 - e. Geben Sie einen Schlüssel und einen Wert ein.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. Wählen Sie Weiter und überprüfen Sie dann die Details für den Schritt.
 - g. Wählen Sie Schritt erstellen, um den Schritt hinzuzufügen und fortzufahren.
7. Fügen Sie den dritten Schritt hinzu (Löschen).
- a. Wählen Sie im Abschnitt Nominale Schritte die Option Schritt hinzufügen aus.
 - b. Wählen Sie „Datei löschen“ und anschließend „Weiter“.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- c. Geben Sie einen Schrittnamen ein.

- d. Wählen Sie unter Dateispeicherort die Option Ursprüngliche Quelldatei löschen aus.
 - e. Wählen Sie Weiter und überprüfen Sie dann die Details für den Schritt.
 - f. Wählen Sie Schritt erstellen, um den Schritt hinzuzufügen und fortzufahren.
8. Überprüfen Sie die Workflow-Konfiguration und wählen Sie dann Workflow erstellen aus.

CLI

Beispiel für einen Workflow zum Markieren und Verschieben

1. Speichern Sie den folgenden Code in einer Datei, `tagAndMoveWorkflow.json` z. B. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```

```
        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
```

Im ersten Schritt wird die hochgeladene Datei an einen neuen Amazon S3 S3-Speicherort kopiert. Im zweiten Schritt wird der Datei (), die an den neuen Speicherort kopiert wurde, ein Tag (Schlüssel-Wert-Paar `previous.file`) hinzugefügt. Und schließlich löscht der dritte Schritt die Originaldatei (). `original.file`

2. Erstellen Sie einen Workflow aus der gespeicherten Datei. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID
```

Beispiel:

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1
```

 Note

Weitere Informationen zur Verwendung von Dateien zum Laden von Parametern finden Sie unter [So laden Sie Parameter aus einer Datei](#).

3. Aktualisieren Sie einen vorhandenen Server.

 Note

In diesem Schritt wird davon ausgegangen, dass Sie bereits über einen Transfer Family Family-Server verfügen und diesem einen Workflow zuordnen möchten. Falls nicht, siehe [Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts](#). Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
aws transfer update-server --server-id server-ID --region region-ID
```

```
--workflow-details '{"OnUpload": [{ "WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN" } ]}'
```

Beispiel:

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2  
--workflow-details '{"OnUpload": [{ "WorkflowId": "w-  
abcdef01234567890", "ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-  
execution-role" } ]}'
```

Verwenden Sie benutzerdefinierte Schritte zur Dateiverarbeitung

Mithilfe eines benutzerdefinierten Dateiverarbeitungsschritts können Sie Ihre eigene Dateiverarbeitungslogik verwenden. AWS Lambda Beim Eintreffen einer Datei ruft ein Transfer Family Family-Server eine Lambda-Funktion auf, die benutzerdefinierte Dateiverarbeitungslogik enthält, z. B. das Verschlüsseln von Dateien, das Scannen nach Malware oder das Überprüfen auf falsche Dateitypen. Im folgenden Beispiel wird die AWS Lambda Zielfunktion verwendet, um die Ausgabedatei aus dem vorherigen Schritt zu verarbeiten.

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

 Note

Eine Beispielfunktion für Lambda finden Sie unter [Beispiel für eine Lambda-Funktion für einen benutzerdefinierten Workflow-Schritt](#). Beispiele für Ereignisse (einschließlich des Speicherorts für Dateien, die an das Lambda übergeben wurden) finden Sie unter [Beispiele für Ereignisse, an die AWS Lambda beim Hochladen einer Datei gesendet werden](#).

Bei einem benutzerdefinierten Workflow-Schritt müssen Sie die Lambda-Funktion so konfigurieren, dass sie den [SendWorkflowStepState](#) API-Vorgang aufruft. `SendWorkflowStepState` benachrichtigt die Workflow-Ausführung darüber, dass der Schritt entweder mit einem Erfolgs- oder einem Fehlerstatus abgeschlossen wurde. Der Status der `SendWorkflowStepState` API-Operation ruft einen Exception-Handler-Schritt oder einen nominalen Schritt in der linearen Sequenz auf, basierend auf dem Ergebnis der Lambda-Funktion.

Wenn die Lambda-Funktion ausfällt oder das Zeitlimit überschritten wird, schlägt der Schritt fehl, und das sehen Sie `StepErrored` in Ihren CloudWatch Protokollen. Wenn die Lambda-Funktion Teil des nominalen Schritts ist und die Funktion `SendWorkflowStepState` mit `Status="FAILURE"` oder Timeout reagiert, wird der Ablauf mit den Exception-Handler-Schritten fortgesetzt. In diesem Fall setzt der Workflow die Ausführung der verbleibenden (falls vorhanden) nominalen Schritte nicht fort. Weitere Details finden Sie unter [Ausnahmebehandlung für einen Workflow](#).

Wenn Sie den `SendWorkflowStepState` API-Vorgang aufrufen, müssen Sie die folgenden Parameter senden:

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Sie können das `ExecutionIdToken`, und `WorkflowId` aus dem Eingabeereignis extrahieren, das bei der Ausführung der Lambda-Funktion übergeben wird (Beispiele werden in den folgenden Abschnitten gezeigt). Der Status Wert kann entweder `SUCCESS` sein. `FAILURE`

Um den `SendWorkflowStepState` API-Vorgang von Ihrer Lambda-Funktion aus aufrufen zu können, müssen Sie eine Version des AWS SDK verwenden, die nach der [Einführung von Managed Workflows](#) veröffentlicht wurde.

Mehrere Lambda-Funktionen nacheinander verwenden

Wenn Sie mehrere benutzerdefinierte Schritte nacheinander verwenden, funktioniert die Option Dateispeicherort anders als wenn Sie nur einen einzigen benutzerdefinierten Schritt verwenden. Transfer Family unterstützt nicht die Rückgabe der Lambda-processed Datei, um sie als Eingabe für den nächsten Schritt zu verwenden. Wenn Sie also mehrere benutzerdefinierte Schritte für die Verwendung dieser `previous.file` Option konfiguriert haben, verwenden sie alle denselben Dateispeicherort (den Speicherort der Eingabedatei für den ersten benutzerdefinierten Schritt).

Note

Die `previous.file` Einstellung funktioniert auch anders, wenn Sie nach einem benutzerdefinierten Schritt einen vordefinierten Schritt (kennzeichnen, kopieren, entschlüsseln oder löschen) haben. Wenn der vordefinierte Schritt so konfiguriert ist, dass er die `previous.file` Einstellung verwendet, verwendet der vordefinierte Schritt dieselbe Eingabedatei wie der benutzerdefinierte Schritt. Die verarbeitete Datei aus dem benutzerdefinierten Schritt wird nicht an den vordefinierten Schritt übergeben.

Zugreifen auf eine Datei nach der benutzerdefinierten Verarbeitung

Wenn Sie Amazon S3 als Speicher verwenden und Ihr Workflow einen benutzerdefinierten Schritt umfasst, der Aktionen an der ursprünglich hochgeladenen Datei ausführt, können nachfolgende Schritte nicht auf diese verarbeitete Datei zugreifen. Das heißt, jeder Schritt nach dem benutzerdefinierten Schritt kann nicht auf die aktualisierte Datei aus der Ausgabe des benutzerdefinierten Schritts verweisen.

Nehmen wir zum Beispiel an, dass Sie die folgenden drei Schritte in Ihrem Workflow haben.

- Schritt 1 — Laden Sie eine Datei mit dem Namen `hochexample-file.txt`.
- Schritt 2 — Rufen Sie eine Lambda-Funktion auf, die sich `example-file.txt` in irgendeiner Weise ändert.
- Schritt 3 — Versuchen Sie, die aktualisierte Version von weiter zu verarbeiten. `example-file.txt`

Wenn Sie das `sourceFileLocation` für Schritt 3 so konfigurieren `${original.file}`, verwendet Schritt 3 den ursprünglichen Speicherort der Datei aus dem Zeitpunkt, zu dem der Server die Datei in

Schritt 1 in den Speicher hochgeladen hat. Wenn Sie `${previous.file}` für Schritt 3 verwenden, wird in Schritt 3 der Speicherort wiederverwendet, den Schritt 2 als Eingabe verwendet hat.

Daher verursacht Schritt 3 einen Fehler. Wenn in Schritt 3 beispielsweise versucht wird, das Update zu `kopierenexample-file.txt`, wird die folgende Fehlermeldung angezeigt:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "NOT_FOUND",
    "errorMessage": "ETag constraint not met (Service: null; Status Code: 412; Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
    "stepType": "COPY",
    "stepName": "CopyFile"
  },
}
```

Dieser Fehler tritt auf, weil der benutzerdefinierte Schritt das Entity-Tag (ETag) für `example-file.txt` so ändert, dass es nicht mit der Originaldatei übereinstimmt.

Note

Dieses Verhalten tritt nicht auf, wenn Sie Amazon EFS verwenden, da Amazon EFS keine Entitäts-Tags zur Identifizierung von Dateien verwendet.

Beispiele für Ereignisse, an die AWS Lambda beim Hochladen einer Datei gesendet werden

Die folgenden Beispiele zeigen die Ereignisse, an die gesendet werden, AWS Lambda wenn ein Datei-Upload abgeschlossen ist. Ein Beispiel verwendet einen Transfer Family Family-Server, auf dem die Domain mit Amazon S3 konfiguriert ist. Das andere Beispiel verwendet einen Transfer Family Family-Server, auf dem die Domain Amazon EFS verwendet.

Custom step that uses an Amazon S3 domain

```
{
  "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
  "serviceMetadata": {
    "executionDetails": {
```

```

        "workflowId": "w-1234567890example",
        "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
    "transferDetails": {
        "sessionId": "36688ff5d2deda8c",
        "userName": "myuser",
        "serverId": "s-example1234567890"
    }
},
"fileLocation": {
    "domain": "S3",
    "bucket": "amzn-s3-demo-bucket",
    "key": "path/to/mykey",
    "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
    "versionId": null
}
}

```

Custom step that uses an Amazon EFS domain

```

{
    "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "EFS",
        "fileSystemId": "fs-1234567",
        "path": "/path/to/myfile"
    }
}

```

Beispiel für eine Lambda-Funktion für einen benutzerdefinierten Workflow-Schritt

Die folgende Lambda-Funktion extrahiert die Informationen zum Ausführungsstatus und ruft dann den [SendWorkflowStepState](#) API-Vorgang auf, um den Status für den Schritt an den Workflow zurückzugeben — SUCCESS entweder oder. FAILURE Bevor Ihre Funktion den SendWorkflowStepState API-Vorgang aufruft, können Sie Lambda so konfigurieren, dass eine Aktion auf der Grundlage Ihrer Workflow-Logik ausgeführt wird.

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
    # SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

IAM-Berechtigungen für einen benutzerdefinierten Schritt

Damit ein Schritt, der ein Lambda aufruft, erfolgreich sein kann, stellen Sie sicher, dass die Ausführungsrolle für Ihren Workflow die folgenden Berechtigungen enthält.

```
{
  "Sid": "Custom",
  "Effect": "Allow",
```



```
"Action": [  
    "lambda:InvokeFunction"  
],  
"Resource": [  
    "arn:aws:lambda:region:account-id:function:function-name"  
]  
}
```

IAM-Richtlinien für Workflows

Wenn Sie einem Server einen Workflow hinzufügen, müssen Sie eine Ausführungsrolle auswählen. Der Server verwendet diese Rolle, wenn er den Workflow ausführt. Wenn die Rolle nicht über die richtigen Berechtigungen verfügt, AWS Transfer Family kann der Workflow nicht ausgeführt werden.

In diesem Abschnitt wird ein möglicher Satz von AWS Identity and Access Management (IAM-) Berechtigungen beschrieben, mit denen Sie einen Workflow ausführen können. Weitere Beispiele werden später in diesem Thema beschrieben.

Note

Wenn Ihre Amazon S3 S3-Dateien Tags haben, müssen Sie Ihrer IAM-Richtlinie eine oder zwei Berechtigungen hinzufügen.

- `s3:GetObjectTagging`Für eine Amazon S3 S3-Datei hinzufügen, die nicht versioniert ist.
- `s3:GetObjectVersionTagging`Für eine Amazon S3 S3-Datei hinzufügen, die versioniert ist.

Um eine Ausführungsrolle für Ihren Workflow zu erstellen

1. Erstellen Sie eine neue IAM-Rolle und fügen Sie der Rolle die AWS verwaltete Richtlinie `AWSTransferFullAccess` hinzu. Weitere Informationen zum Erstellen einer neuen IAM-Rolle finden Sie unter [the section called “Erstellen Sie eine IAM-Rolle und -Richtlinie”](#)
2. Erstellen Sie eine weitere Richtlinie mit den folgenden Berechtigungen und fügen Sie sie Ihrer Rolle hinzu. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ConsoleAccess",
    "Effect": "Allow",
    "Action": "s3:GetBucketLocation",
    "Resource": "*"
  },
  {
    "Sid": "ListObjectsInBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "AllObjectActions",
    "Effect": "Allow",
    "Action": "s3:*Object",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "GetObjectVersion",
    "Effect": "Allow",
    "Action": "s3:GetObjectVersion",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:function-name"
    ]
  },
  {
    "Sid": "Tag",

```

```

        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    }
}

```

3. Speichern Sie diese Rolle und geben Sie sie als Ausführungsrolle an, wenn Sie einem Server einen Workflow hinzufügen.

Note

AWS empfiehlt, bei der Erstellung von IAM-Rollen den Zugriff auf Ihre Ressourcen so weit wie möglich für Ihren Workflow einzuschränken.

Vertrauensbeziehungen im Arbeitsablauf

Rollen für die Workflow-Ausführung erfordern auch eine Vertrauensbeziehung mit `transfer.amazonaws.com`. Informationen zum Einrichten einer Vertrauensbeziehung für AWS Transfer Family finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

Während Sie Ihr Vertrauensverhältnis aufbauen, können Sie auch Maßnahmen ergreifen, um das Problem des verwirrten Stellvertreters zu vermeiden. Eine Beschreibung dieses Problems sowie Beispiele, wie es vermieden werden kann, finden Sie unter [the section called "Cross-service Prävention von verwirrten Stellvertretern"](#).

Beispiel für eine Ausführungsrolle: Entschlüsseln, Kopieren und Markieren

Wenn Sie Workflows haben, die Schritte zum Markieren, Kopieren und Entschlüsseln beinhalten, können Sie die folgende IAM-Richtlinie verwenden. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```

{
    "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Sid": "CopyRead",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectTagging",
      "s3:GetObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
  },
  {
    "Sid": "CopyWrite",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  },
  {
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-source-bucket",
      "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
  },
  {
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
      "s3:PutObjectTagging",
      "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
      "StringEquals": {
        "s3:RequestObjectTag/Archive": "yes"
      }
    }
  }
]

```

```

        "Sid": "ListBucket",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObjectVersion",
            "s3:DeleteObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
        "Sid": "Decrypt",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
    }
]
}

```

Beispiel für eine Ausführungsrolle: Funktion ausführen und löschen

In diesem Beispiel haben Sie einen Workflow, der eine AWS Lambda Funktion aufruft. Wenn der Workflow die hochgeladene Datei löscht und über einen Exception-Handler-Schritt verfügt, der auf eine fehlgeschlagene Workflow-Ausführung im vorherigen Schritt reagiert, verwenden Sie die folgende IAM-Richtlinie. Ersetzen Sie jeden *user input placeholder* durch Ihre Informationen.

```

{
    "Version": "2012-10-17",
    "Statement": [

```

```

    {
      "Sid": "Delete",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3::bucket-name"
    },
    {
      "Sid": "Custom",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:function-name"
      ]
    }
  ]
}

```

Ausnahmebehandlung für einen Workflow

Wenn während der Ausführung eines Workflows Fehler auftreten, werden die von Ihnen angegebenen Schritte zur Ausnahmebehandlung ausgeführt. Sie geben die Schritte zur Fehlerbehandlung für einen Workflow auf die gleiche Weise an, wie Sie die nominalen Schritte für den Workflow angeben. Nehmen wir beispielsweise an, Sie haben die benutzerdefinierte Verarbeitung in nominalen Schritten konfiguriert, um eingehende Dateien zu überprüfen. Wenn die Dateiüberprüfung fehlschlägt, kann in einem Schritt zur Ausnahmebehandlung eine E-Mail an den Administrator gesendet werden.

Der folgende Beispiel-Workflow umfasst zwei Schritte:

- Ein nominaler Schritt, der überprüft, ob die hochgeladene Datei im CSV-Format vorliegt
- Ein Schritt zur Ausnahmebehandlung, bei dem eine E-Mail gesendet wird, falls die hochgeladene Datei nicht im CSV-Format vorliegt und der nominelle Schritt fehlschlägt

Um den Schritt zur Ausnahmebehandlung einzuleiten, muss die AWS Lambda Funktion im nominalen Schritt mit antworten. Status="FAILURE" Weitere Informationen zur Fehlerbehandlung in Workflows finden Sie unter. [the section called “Verwenden Sie benutzerdefinierte Schritte zur Dateiverarbeitung”](#)

w-1234567890abcdef0

Delete

Description

Name

Delete after upload

Workflow description

test-my-workflow

Nominal steps (1) Info

Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details

Exception handlers (1) Info

Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

Überwachen Sie die Workflow-Ausführung

Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, die Sie ausführen, AWS Cloud in Echtzeit. Sie können Amazon verwenden, CloudWatch um Metriken zu sammeln und zu verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Workflows messen können. Sie können Workflow-Metriken und konsolidierte Protokolle mithilfe von Amazon anzeigen CloudWatch.

CloudWatch Protokollierung für einen Workflow

CloudWatch bietet eine konsolidierte Prüfung und Protokollierung des Fortschritts und der Ergebnisse von Workflows.

CloudWatch Amazon-Protokolle für Workflows anzeigen

1. Öffnen Sie die CloudWatch Amazon-Konsole unter <https://console.aws.amazon.com/cloudwatch/>.

2. Wählen Sie im linken Navigationsbereich Logs und anschließend Log-Gruppen aus.
3. Wählen Sie auf der Seite Protokollgruppen in der Navigationsleiste die richtige Region für Ihren AWS Transfer Family Server aus.
4. Wählen Sie die Protokollgruppe aus, die Ihrem Server entspricht.

Wenn Ihre Server-ID beispielsweise lautet `-1234567890abcdef0`, ist Ihre Protokollgruppe `/aws/transfer/s-1234567890abcdef0`.

5. Auf der Seite mit den Protokollgruppendetails für Ihren Server werden die neuesten Protokollstreams angezeigt. Es gibt zwei Protokollstreams für den Benutzer, den Sie untersuchen:

- Einer für jede Secure Shell (SSH) File Transfer Protocol (SFTP) -Sitzung.
- Eine für den Workflow, der für Ihren Server ausgeführt wird. Das Format für den Protokollstream für den Workflow ist `username.workflowID.uniqueStreamSuffix`.

Wenn Ihr Benutzer beispielsweise ist `mary-major`, haben Sie die folgenden Protokollstreams:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

Die in diesem Beispiel aufgeführten 16-stelligen alphanumerischen Identifikatoren sind fiktiv. Die Werte, die Sie bei Amazon sehen, CloudWatch sind unterschiedlich.

Auf der Seite Ereignisse protokollieren für `mary-major-usa-east.1234567890abcdef0` werden die Details für jede Benutzersitzung angezeigt, und der `mary.w-abcdef01234567890.021345abcdef6789` Protokollstream enthält die Details für den Workflow.

Im Folgenden finden Sie ein Beispiel für einen Protokollstream für `mary.w-abcdef01234567890.021345abcdef6789`, der auf einem Workflow (`w-abcdef01234567890`) basiert, der einen Kopierschritt enthält.

```
{
  "type": "ExecutionStarted",
  "details": {
```



```

        "input": {
            "initialFileLocation": {
                "bucket": "amzn-s3-demo-bucket",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        },
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    },
    {
        "type": "StepStarted",
        "details": {
            "input": {
                "fileLocation": {
                    "backingStore": "S3",
                    "bucket": "amzn-s3-demo-bucket",
                    "key": "mary/workflowSteps2.json",
                    "versionId": "version-id",
                    "etag": "etag-id"
                }
            },
            "stepType": "COPY",
            "stepName": "copyToShared"
        },
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    },
    {
        "type": "StepCompleted",
        "details": {
            "output": {},

```

```

        "stepType": "COPY",
        "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
        "serverId": "server-id",
        "username": "mary",
        "sessionId": "session-id"
    }
},
{
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
        "serverId": "s-server-id",
        "username": "mary",
        "sessionId": "session-id"
    }
}
}

```

CloudWatch Metriken für Workflows

AWS Transfer Family bietet mehrere Metriken für Workflows. Sie können Messwerte darüber anzeigen, wie viele Workflow-Ausführungen in der letzten Minute gestartet, erfolgreich abgeschlossen und fehlgeschlagen sind. Alle CloudWatch Metriken für Transfer Family werden unter [beschrieben](#) [Verwenden von CloudWatch Metriken für Transfer Family Family-Server](#).

Erstellen Sie einen Workflow aus einer Vorlage

Sie können einen CloudFormation Stapel bereitstellen, der aus einer Vorlage einen Workflow und einen Server erstellt. Dieses Verfahren enthält ein Beispiel, mit dem Sie schnell einen Workflow bereitstellen können.

Um einen CloudFormation Stack zu erstellen, der einen AWS Transfer Family Workflow und einen Server erstellt

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Speichern Sie den folgenden Code in einer Datei.

YAML

```

AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
    Properties:
      WorkflowDetails:
        OnUpload:
          - ExecutionRole: workflow-execution-role-arn
            WorkflowId: !GetAtt
              - TransferWorkflow
              - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
    Properties:
      Description: Transfer Family Workflows Blog
      Steps:
        - Type: COPY
          CopyStepDetails:
            Name: copyToUserKey
            DestinationFileLocation:
              S3FileLocation:
                Bucket: archived-records
                Key: ${transfer:UserName}/
              OverwriteExisting: 'TRUE'
        - Type: TAG
          TagStepDetails:
            Name: tagFileForArchive
            Tags:
              - Key: Archive
                Value: yes
        - Type: CUSTOM
          CustomStepDetails:
            Name: transferExtract
            Target: arn:aws:lambda:region:account-id:function:function-name
            TimeoutSeconds: 60
        - Type: DELETE
          DeleteStepDetails:
            Name: DeleteInputFile
            SourceFileLocation: '${original.file}'
      Tags:
        - Key: Name

```

Value: TransferFamilyWorkflows

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "SFTPServer": {
      "Type": "AWS::Transfer::Server",
      "Properties": {
        "WorkflowDetails": {
          "OnUpload": [
            {
              "ExecutionRole": "workflow-execution-role-arn",
              "WorkflowId": {
                "Fn::GetAtt": [
                  "TransferWorkflow",
                  "WorkflowId"
                ]
              }
            ]
          ]
        }
      }
    },
    "TransferWorkflow": {
      "Type": "AWS::Transfer::Workflow",
      "Properties": {
        "Description": "Transfer Family Workflows Blog",
        "Steps": [
          {
            "Type": "COPY",
            "CopyStepDetails": {
              "Name": "copyToUserKey",
              "DestinationFileLocation": {
                "S3FileLocation": {
                  "Bucket": "archived-records",
                  "Key": "${transfer:UserName}/"
                }
              },
              "OverwriteExisting": "TRUE"
            }
          ]
        }
      }
    }
  }
}
```

```

        {
            "Type": "TAG",
            "TagStepDetails": {
                "Name": "tagFileForArchive",
                "Tags": [
                    {
                        "Key": "Archive",
                        "Value": "yes"
                    }
                ]
            }
        },
        {
            "Type": "CUSTOM",
            "CustomStepDetails": {
                "Name": "transferExtract",
                "Target": "arn:aws:lambda:region:account-
id:function:function-name",
                "TimeoutSeconds": 60
            }
        },
        {
            "Type": "DELETE",
            "DeleteStepDetails": {
                "Name": "DeleteInputFile",
                "SourceFileLocation": "${original.file}"
            }
        }
    ],
    "Tags": [
        {
            "Key": "Name",
            "Value": "TransferFamilyWorkflows"
        }
    ]
}
}
}
}
}

```

3. Ersetzen Sie die folgenden Elemente durch Ihre tatsächlichen Werte.

- Ersetzen Sie *workflow-execution-role-arn* mit dem ARN für eine tatsächliche Workflow-Ausführungsrolle. Beispiel: `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
 - `arn:aws:lambda:region:account-id:function:function-name` Ersetzen Sie es durch den ARN für Ihre Lambda-Funktion. Beispiel, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.
4. Folgen Sie den Anweisungen zum Bereitstellen eines CloudFormation Stacks anhand einer vorhandenen Vorlage unter [Auswahl einer Stack-Vorlage](#) im AWS CloudFormation Benutzerhandbuch.

Nachdem der Stack bereitgestellt wurde, können Sie Details dazu auf der Registerkarte Ausgaben in der CloudFormation Konsole einsehen. Die Vorlage erstellt einen neuen AWS Transfer Family SFTP-Server, der vom Service verwaltete Benutzer verwendet, sowie einen neuen Workflow und ordnet den Workflow dem neuen Server zu.

Einen Workflow von einem Transfer Family Family-Server entfernen

Wenn Sie einem Transfer Family Family-Server einen Workflow zugeordnet haben und diese Zuordnung nun entfernen möchten, können Sie dies mithilfe der Konsole oder programmgesteuert tun.

Console

So entfernen Sie einen Workflow von einem Transfer Family Family-Server

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server aus.
3. Wählen Sie den Bezeichner für den Server in der Spalte Server-ID aus.
4. Scrollen Sie auf der Detailseite für den Server nach unten zum Abschnitt Zusätzliche Details und wählen Sie dann Bearbeiten aus.
5. Löschen Sie auf der Seite Zusätzliche Details bearbeiten im Abschnitt Verwaltete Workflows die Informationen für alle Einstellungen:

- Wählen Sie den Bindestrich (-) aus der Liste der Workflows für den Workflow für vollständige Datei-Uploads aus.
- Falls nicht bereits deaktiviert, wählen Sie den Bindestrich (-) aus der Liste der Workflows für den Workflow für unvollständige Datei-Uploads aus.
- Wählen Sie den Bindestrich (-) aus der Rollenliste für die Ausführungsrolle Verwaltete Workflows aus.

Wenn Sie den Gedankenstrich nicht sehen, scrollen Sie nach oben, bis Sie ihn sehen, da er der erste Wert in jedem Menü ist.

Der Bildschirm sollte wie folgt aussehen.

6. Scrollen Sie nach unten und wählen Sie Speichern, um Ihre Änderungen zu speichern.

CLI

Sie verwenden den Aufruf `update-server` (oder `UpdateServer` für API) und geben leere Argumente für die `OnPartialUpload` Parameter `OnUpload` und an.

Führen Sie in der den folgenden Befehl aus: AWS CLI

```
aws transfer update-server --server-id your-server-id --workflow-details
'{"OnPartialUpload":[], "OnUpload":[]}'
```

your-server-id Ersetzen Sie es durch die ID für Ihren Server. Wenn Ihre Server-ID beispielsweise `-01234567890abcdef`, lautet der Befehl wie folgt:

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details  
'{"OnPartialUpload":[], "OnUpload":[]}'
```

Einschränkungen und Einschränkungen verwalteter Workflows

Einschränkungen

Die folgenden Einschränkungen gelten derzeit für Workflows zur Verarbeitung nach dem Upload für AWS Transfer Family.

- Cross-account und regionsübergreifende AWS Lambda Funktionen werden nicht unterstützt. Sie können jedoch kontenübergreifend kopieren, sofern Ihre AWS Identity and Access Management (IAM-) Richtlinien korrekt konfiguriert sind.
- Für alle Workflow-Schritte müssen sich alle Amazon S3 S3-Buckets, auf die der Workflow zugreift, in derselben Region wie der Workflow selbst befinden.
- Für einen Entschlüsselungsschritt muss das Entschlüsselungsziel mit der Quelle für Region und Backing-Store übereinstimmen (wenn die zu entschlüsselnde Datei beispielsweise in Amazon S3 gespeichert ist, muss sich das angegebene Ziel auch in Amazon S3 befinden).
- Nur asynchrone benutzerdefinierte Schritte werden unterstützt.
- Die Timeouts für benutzerdefinierte Schritte sind ungefähre Angaben. Das heißt, das Timeout kann etwas länger dauern als angegeben. Darüber hinaus ist der Workflow von der Lambda-Funktion abhängig. Wenn die Funktion während der Ausführung verzögert wird, ist sich der Workflow der Verzögerung daher nicht bewusst.
- Wenn Sie Ihr Drosselungslimit überschreiten, fügt Transfer Family der Warteschlange keine Workflow-Operationen hinzu.
- Workflows werden für Dateien mit einer Größe von 0 nicht initiiert. Dateien mit einer Größe von mehr als 0 initiieren den zugehörigen Workflow.
- Sie können einen Dateiverarbeitungs-Workflow an einen Transfer Family Family-Server anhängen, der das AS2-Protokoll verwendet. AS2-Nachrichten führen jedoch keine Workflows aus, die an den Server angehängt sind.

Einschränkungen

Darüber hinaus gelten die folgenden Funktionseinschränkungen für Workflows für Transfer Family:

- Die Anzahl der Workflows pro Region und Konto ist auf 10 begrenzt.
- Das maximale Timeout für benutzerdefinierte Schritte beträgt 30 Minuten.
- Die maximale Anzahl von Schritten in einem Workflow beträgt 8.
- Die maximale Anzahl von Tags pro Workflow beträgt 50.
- Die maximale Anzahl gleichzeitiger Ausführungen, die einen Entschlüsselungsschritt enthalten, beträgt 250 pro Workflow.
- Sie können maximal 3 private PGP-Schlüssel pro Transfer Family Family-Server pro Benutzer speichern.
- Die maximale Größe für eine entschlüsselte Datei beträgt 10 GB.
- Wir drosseln die neue Ausführungsrate mithilfe eines [Token-Bucket-Systems](#) mit einer Burst-Kapazität von 100 und einer Nachfüllrate von 1.
- Jedes Mal, wenn Sie einen Workflow von einem Server entfernen und ihn durch einen neuen ersetzen oder die Serverkonfiguration aktualisieren (was sich auf die Ausführungsrolle eines Workflows auswirkt), müssen Sie etwa 10 Minuten warten, bevor Sie den neuen Workflow ausführen. Der Transfer Family Family-Server speichert die Workflow-Details im Cache, und es dauert 10 Minuten, bis der Server seinen Cache aktualisiert hat.

Darüber hinaus müssen Sie sich von allen aktiven SFTP-Sitzungen abmelden und sich nach Ablauf der 10-minütigen Wartezeit wieder anmelden, um die Änderungen zu sehen.

Server verwalten

In diesem Abschnitt finden Sie Informationen zum Anzeigen einer Liste Ihrer Server, zum Anzeigen Ihrer Serverdetails, zum Bearbeiten Ihrer Serverdetails und zum Ändern des Hostschlüssels für Ihren SFTP-enabled Server.

Themen

- [Eine Liste von Servern anzeigen](#)
- [Löschen Sie einen Server](#)
- [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#)
- [AS2-Serverdetails anzeigen](#)
- [IPv6-Unterstützung für Transfer Family Family-Server](#)
- [Serverdetails bearbeiten](#)
- [Konfiguration des Identitätsanbieters bearbeiten](#)
- [Hostschlüssel für Ihren SFTP-enabled Server verwalten](#)
- [Überwachung der Nutzung in der Konsole](#)

Eine Liste von Servern anzeigen

Auf der AWS Transfer Family Konsole finden Sie eine Liste all Ihrer Server, die sich in der von Ihnen ausgewählten AWS Region befinden.

Um eine Liste Ihrer Server zu finden, die in einer AWS Region existieren

- Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.

Wenn Sie einen oder mehrere Server in der aktuellen AWS Region haben, öffnet sich die Konsole und zeigt eine Liste Ihrer Server an. Wenn Sie keine Serverliste sehen, stellen Sie sicher, dass Sie sich in der richtigen Region befinden. Sie können auch im Navigationsbereich Servers (Server) auswählen.

Weitere Informationen zum Anzeigen Ihrer Serverdetails finden Sie unter [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#).

Löschen Sie einen Server

In diesem Verfahren wird erklärt, wie Sie einen Transfer Family Family-Server mithilfe der AWS Transfer Family Konsole oder löschen AWS CLI.

Important

Ihnen wird jedes Protokoll, das für den Zugriff auf Ihren Endpunkt aktiviert ist, in Rechnung gestellt, bis Sie den Server löschen.

Warning

Das Löschen eines Servers hat zur Folge, dass alle seine Benutzer gelöscht werden. Daten in dem Bucket, auf den über den Server zugegriffen wurde, werden nicht gelöscht und sind weiterhin für AWS Benutzer zugänglich, die über Berechtigungen für diese Amazon S3 S3-Buckets verfügen.

Console

Um einen Server mithilfe der Konsole zu löschen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server aus.
3. Aktivieren Sie das Kontrollkästchen des Servers, den Sie löschen möchten.
4. Klicken Sie bei Actions auf Delete.
5. Geben Sie im daraufhin angezeigten Bestätigungsdiaologfeld das Wort **delete**, und klicken Sie dann auf Löschen, um zu bestätigen, dass Sie den Server löschen möchten.

Der Server wird von der Seite Server gelöscht und es wird Ihnen nichts mehr in Rechnung gestellt.

AWS CLI

So löschen Sie einen Server mit der CLI

1. (Optional) Führen Sie den folgenden Befehl aus, um die Details für den Server anzuzeigen, den Sie dauerhaft löschen möchten.

```
aws transfer describe-server --server-id your-server-id
```

Dieser `describe-server` Befehl gibt alle Details für Ihren Server zurück.

2. Führen Sie den folgenden Befehl aus, um den Server zu löschen.

```
aws transfer delete-server --server-id your-server-id
```

Bei Erfolg löscht der Befehl den Server und gibt keine Informationen zurück.

SFTP-, FTPS- und FTP-Serverdetails anzeigen

Sie finden eine Liste mit Details und Eigenschaften für einen einzelnen AWS Transfer Family Server. Zu den Servereigenschaften gehören Protokolle, Identitätsanbieter, Status, Endpunkttyp, benutzerdefinierter Hostname, Endpunkt, Benutzer, Protokollierungsrolle, Serverhostschlüssel und Tags.

Um Serverdetails anzuzeigen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen (siehe unten).

Sie können die Eigenschaften des Servers auf dieser Seite ändern, indem Sie Bearbeiten wählen. Weitere Informationen zum Bearbeiten von Serverdetails finden Sie unter [Serverdetails bearbeiten](#). Die Detailseite für AS2-Server unterscheidet sich geringfügig. Informationen zu AS2-Servern finden Sie unter [AS2-Serverdetails anzeigen](#)

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

Note

Die Werte für die Beschreibung des Server-Host-Schlüssels und das Importdatum sind seit September 2022 neu. Diese Werte wurden eingeführt, um die Funktion für mehrere Hostschlüssel zu unterstützen. Diese Funktion erforderte die Migration aller einzelnen Hostschlüssel, die vor der Einführung mehrerer Hostschlüssel verwendet wurden.

Der Wert Importdatum für einen migrierten Server-Hostschlüssel ist auf das Datum der letzten Änderung für den Server festgelegt. Das heißt, das Datum, das Sie für Ihren migrierten Hostschlüssel sehen, entspricht dem Datum, an dem Sie den Server vor der Migration des Server-Host-Schlüssels zuletzt geändert haben.

Der einzige Schlüssel, der migriert wurde, ist Ihr ältester oder einziger Server-Hostschlüssel. Alle zusätzlichen Schlüssel haben ihr aktuelles Datum, ab dem Sie sie importiert haben. Darüber hinaus enthält der migrierte Schlüssel eine Beschreibung, anhand derer er leicht als migriert identifiziert werden kann.

Die Migration fand zwischen dem 2. und 13. September statt. Das tatsächliche Migrationsdatum innerhalb dieses Bereichs hängt von der Region Ihres Servers ab.

Additional details

[Edit](#)

Log group

[/aws/transfer/s-](#) 

Logging role

[Info](#)
-

Security Policy

[Info](#)
TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner

[View the display message](#)

Optimized directories

[Info](#)
ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

AS2-Serverdetails anzeigen

Sie finden eine Liste mit Details und Eigenschaften für einen einzelnen AWS Transfer Family Server. Zu den Servereigenschaften gehören Protokolle, Status und mehr. Bei AS2-Servern können Sie auch die asynchronen MDN-Ausgangs-IP-Adressen von AS2 anzeigen.

Protocols

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

Edit

 **AS2 Auth**
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

Jedem AS2-Server werden drei statische IP-Adressen zugewiesen. Verwenden Sie diese IP-Adressen, um asynchrone mDNS über AS2 an Ihre Handelspartner zu senden.

AS2 asynchronous MDN egress IP details

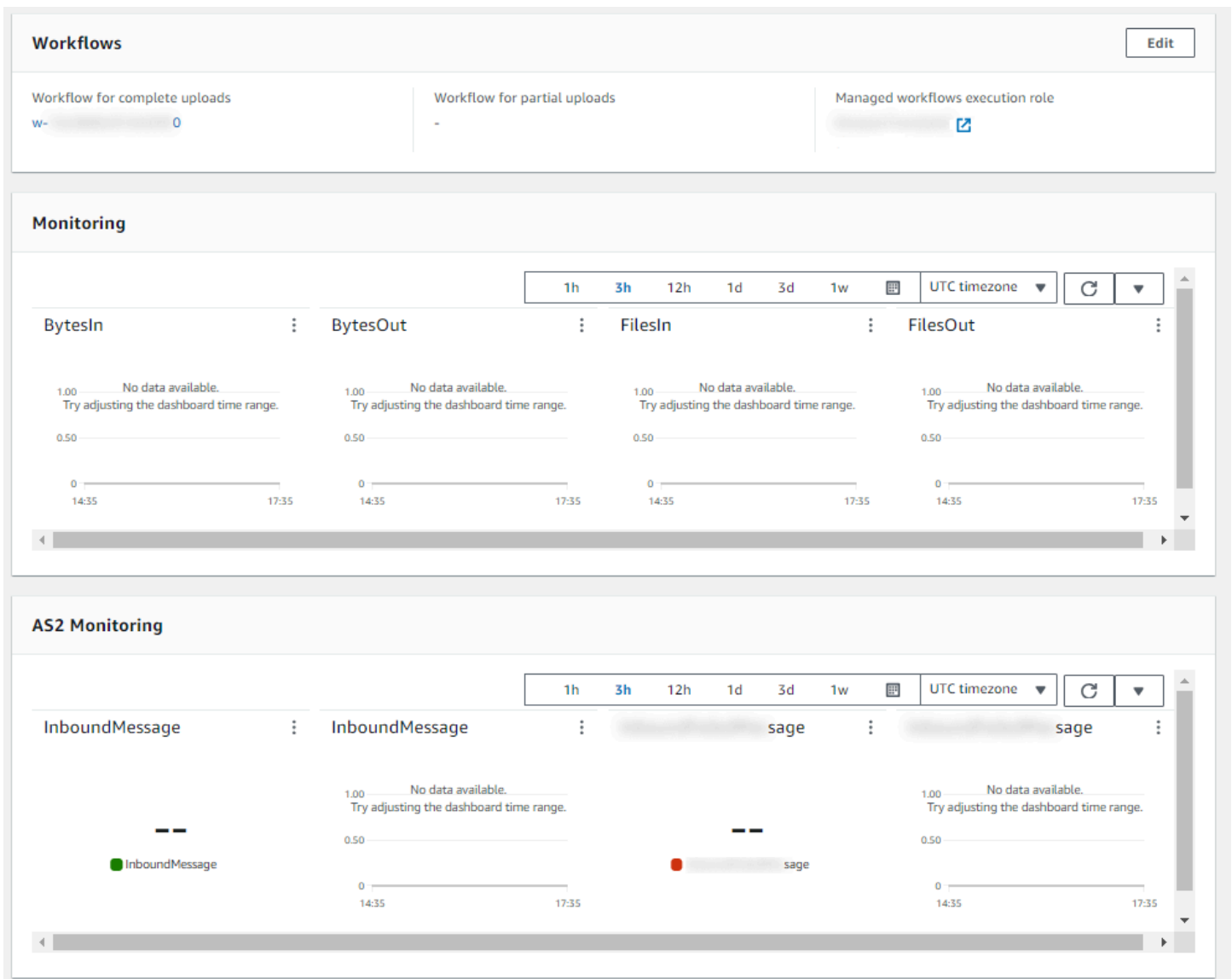
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2







Der untere Teil der Seite mit den AS2-Serverdetails enthält Details zu allen angehängten Workflows sowie Überwachungs- und Tagging-Informationen.



IPv6-Unterstützung für Transfer Family Family-Server

AWS Transfer Family unterstützt Dual-Stack-Endpunkte (IPv4 und IPv6) für die folgenden Ressourcen:

- Öffentliche SFTP-Endpunkte
- Interne VPC-Endpunkte für alle Protokolle (SFTP/FTPS/FTP und AS2)
- Öffentliche Endpunkte für AS2-enabled Transfer Family Family-Server mithilfe der unter [Verwendung eines Application Load Balancer für Dual-Stack-AS2-Serverkonnektivität](#)
- API-Endpunkte

Dank der Dual-Stack-Unterstützung können Ihre Transfer Family Family-Endpunkte sowohl mit IPv4- als auch mit IPv6-fähigen Clients kommunizieren. Auf diese Weise können Sie schrittweise von IPv4- zu IPv6-basierten Systemen wechseln, ohne auf einmal wechseln zu müssen, die IPv6-Konformitätsanforderungen zu erfüllen und teure Netzwerkgeräte für die Adressübersetzung zwischen IPv4 und IPv6 überflüssig zu machen. Einzelheiten finden Sie unter [DNS und Endpunkte](#) in der API-Referenz.AWS Transfer Family Eine vollständige Liste der verfügbaren Endpunkte finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine AWS-Referenz

IPv6-Einschränkungen

Die folgenden Transfer Family Family-Ressourcen unterstützen IPv6 derzeit nicht:

- VPC-Internet Endpunkte
- Endpunkttyp VPC_ENDPOINT (veraltet)

Das FTPS-Protokoll unterstützt die Befehle PASV und EPSV zum Anfordern eines offenen Datenports für Operationen zum Auflisten, Abrufen und Einfügen von Dateien. PASV funktioniert jedoch nicht mit IPv6, da dafür eine Antwort erforderlich ist. IPv4-specific EPSV funktioniert weiterhin, da es nur Portinformationen zurückgibt.

Um FTPS zu verwenden, empfehlen wir eine der folgenden Methoden:

- Konfigurieren Sie Ihren FTPS-Client für die Verwendung von EPSV
- Verwenden Sie IPv4 anstelle von IPv6

SFTP unterstützt sowohl IPv4 als auch IPv6. Wir empfehlen, SFTP anstelle von FTPS zu verwenden, wenn Sie mit Dual-Stack-Endpunkten arbeiten.

Konfiguration von IPv6 für Server

Wenn Sie einen neuen Server erstellen oder einen vorhandenen Server aktualisieren, können Sie den IP-Adresstyp wählen:

- IPv4 (Standard): Aus Gründen der Abwärtskompatibilität akzeptiert der Server nur IPv4-Verbindungen.
- Dual-stack: Der Server akzeptiert sowohl IPv4- als auch IPv6-Verbindungen.

Um den IP-Adresstyp eines vorhandenen Servers zu aktualisieren:

1. Stoppen Sie den Server.
2. Bearbeiten Sie die Endpunktdetails.
3. Ändern Sie den IP-Adresstyp in Dual-stack.
4. Starten Sie den -Server.

 Note

Für VPC-Internet Endgeräte wird der Dual-Stack-Modus derzeit nicht unterstützt.

Verwendung eines Application Load Balancer für Dual-Stack-AS2-Serverkonnektivität

Sie können Dual-Stack-Konnektivität (IPv4 und IPv6) zu Ihrem AS2-Server aktivieren, indem Sie einen Application Load Balancer verwenden, der über einen öffentlich zugänglichen Endpunkt verfügt. Auf diese Weise können Handelspartner entweder über IPv4 oder IPv6 eine Verbindung zu Ihrem AS2-Server herstellen.

So richten Sie einen Dual-Stack-Application Application Load Balancer für Ihren AS2-Server ein

1. Erstellen Sie eine VPC mit den folgenden Einstellungen:
 - Nur VPC
 - Manuelle IPv4-CIDR-Eingabe
 - Amazon-provided IPv6-CIDR-Block
2. Erstellen Sie mindestens zwei Subnetze in verschiedenen Availability Zones:
 - Fügen Sie IPv6-CIDRs zu den Subnetzen hinzu
 - Weisen Sie beim Erstellen von Subnetzen nur eine Teilmenge der VPC-Adressen zu, damit IPv4/IPv6 Adressen für weitere Subnetze verfügbar bleiben
3. Erstellen Sie ein Internet-Gateway für die VPC.
4. Bearbeiten Sie die Routentabelle und fügen Sie zwei Routen hinzu:
 - Eine Route mit Ziel `0.0.0.0/0`
 - Eine Route mit Ziel `:::/0`

- Stellen Sie beide Routenziele auf das Internet-Gateway ein, das Sie erstellt haben
5. Erstellen Sie einen AS2-enabled Server in der VPC, die Sie in Schritt 1 erstellt haben. Stellen Sie sicher, dass Sie das `IpAddressType` als `DUALSTACK` angeben.

Einzelheiten zum Erstellen eines Transfer Family Family-Servers, der das AS2-Protokoll verwendet, finden Sie unter [Erstellen Sie einen AS2-Server](#).

6. Erstellen Sie eine Zielgruppe:
- Konfigurieren Sie für Gruppendetails angeben:
 - Zieltyp: IP-Adressen
 - Name: Geben Sie einen Namen ein
 - Protokoll: HTTP
 - Port: 5080
 - VPC: Wählen Sie die VPC aus, die Sie erstellt haben
 - Protokollversion: HTTP1
 - Gesundheitschecks: Standardwerte verwenden
 - Für Registerziele:
 - Geben Sie die private IPv4-Adresse Ihres AS2-Servers ein
 - Wählen Sie unten „Als ausstehend einschließen“
7. Erstellen Sie einen Application Load Balancer:
- Geben Sie einen Namen ein
 - Wählen Sie für Schema Internet-facing
 - Wählen Sie als IP-Adresstyp Dualstack
 - Für Netzwerk-Mapping:
 - Wählen Sie die VPC aus, die Sie erstellt haben
 - Wählen Sie die Availability Zones aus, in denen Sie Subnetze erstellt haben
 - Wählen Sie für Sicherheitsgruppen eine Sicherheitsgruppe aus, die eingehenden IPv4- und IPv6-Verkehr von einer beliebigen IP-Adresse an Port 80 zulässt
 - Für Listener und Routing:
 - Protokoll: HTTP
 - Port: 80
 - Standardaktion: An die von Ihnen erstellte Zielgruppe weiterleiten

- Wählen Sie Load Balancer erstellen

Nachdem Sie den Application Load Balancer erstellt haben, können Handelspartner seinen DNS-Namen verwenden, um Traffic an Ihren AS2-Server zu senden. Diese Konfiguration ermöglicht es Ihrem AS2-Server, Verbindungen sowohl von IPv4- als auch von IPv6-Clients über den Dual-Stack-Application Load Balancer zu akzeptieren.

Serverdetails bearbeiten

Nachdem Sie einen AWS Transfer Family Server erstellt haben, können Sie die Serverkonfiguration bearbeiten.

Themen

- [Bearbeiten Sie die Dateiübertragungsprotokolle](#)
- [Bearbeiten Sie den Serverendpunkt](#)
- [Bearbeiten Sie Ihre Logging-Konfiguration](#)
- [Bearbeiten Sie die Sicherheitsrichtlinie](#)
- [Ändern Sie den verwalteten Workflow für Ihren Server](#)
- [Ändern Sie die Display-Banner für Ihren Server](#)
- [Schalten Sie Ihren Server online oder offline](#)

Um die Konfiguration eines Servers zu bearbeiten

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server aus.
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen (siehe unten).

Sie können die Eigenschaften des Servers auf dieser Seite ändern, indem Sie Bearbeiten wählen:

- Informationen zum Ändern der Protokolle finden Sie unter [Bearbeiten Sie die Dateiübertragungsprotokolle](#).
- Für den Identitätsanbieter können Sie jetzt zwischen beliebigen Identitätsanbietertypen (vom Dienst verwaltet, AWS Directory Service oder benutzerdefinierter Identitätsanbieter) wechseln.

Einzelheiten zum Ändern der Identitätsanbieterarten und die erforderlichen Informationen für jeden Übergang finden Sie unter [Konfiguration des Identitätsanbieters bearbeiten](#).

- Informationen zum Ändern des Endpunkttyps oder des benutzerdefinierten Hostnamens finden Sie unter [Bearbeiten Sie den Serverendpunkt](#).
- Um eine Vereinbarung hinzuzufügen, müssen Sie zunächst AS2 als Protokoll zu Ihrem Server hinzufügen. Details hierzu finden Sie unter [Bearbeiten Sie die Dateiübertragungsprotokolle](#).
- Informationen zur Verwaltung von Hostschlüsseln für Ihren Server finden Sie unter [Hostschlüssel für Ihren SFTP-enabled Server verwalten](#).
- Unter Zusätzliche Details können Sie die folgenden Informationen bearbeiten:
 - Informationen zum Ändern der Protokollierungsrolle finden Sie unter [Bearbeiten Sie Ihre Logging-Konfiguration](#).
 - Informationen zum Ändern der Sicherheitsrichtlinie finden Sie unter [Bearbeiten Sie die Sicherheitsrichtlinie](#).
 - Informationen zum Ändern des Server-Host-Schlüssels finden Sie unter [Hostschlüssel für Ihren SFTP-enabled Server verwalten](#).
 - Informationen zum Ändern des verwalteten Workflows für Ihren Server finden Sie unter [Ändern Sie den verwalteten Workflow für Ihren Server](#).
 - Informationen zum Bearbeiten der Display-Banner für Ihren Server finden Sie unter [Ändern Sie die Display-Banner für Ihren Server](#).
- Unter Zusätzliche Konfiguration können Sie die folgenden Informationen bearbeiten:
 - SetStat Option: Aktivieren Sie diese Option, um den Fehler zu ignorieren, der generiert wird, wenn ein Client versucht, eine Datei SETSTAT zu verwenden, die Sie in einen Amazon S3 S3-Bucket hochladen. Weitere Informationen finden Sie in der SetStatOption Dokumentation im [ProtocolDetails](#) Thema.
 - Wiederaufnahme der TLS-Sitzung: bietet einen Mechanismus zur Wiederaufnahme oder gemeinsamen Nutzung eines ausgehandelten geheimen Schlüssels zwischen der Kontroll- und Datenverbindung für eine FTPS-Sitzung. Weitere Informationen finden Sie in der TlsSessionResumptionMode Dokumentation zum Thema. [ProtocolDetails](#)
 - Passive IP: steht für den passiven Modus für FTP- und FTPS-Protokolle. Geben Sie eine einzelne IPv4-Adresse ein, z. B. die öffentliche IP-Adresse einer Firewall, eines Routers oder eines Load Balancers. Weitere Informationen finden Sie in der PassiveIp Dokumentation zum [ProtocolDetails](#) Thema.

 Note

Vermeiden Sie es, Network Load Balancer (NLBs) oder NAT-Gateways vor Servern zu platzieren. AWS Transfer Family Diese Konfiguration erhöht die Kosten und kann zu Leistungsproblemen führen. Weitere Details finden Sie unter [Vermeiden Sie es, AWS Transfer Family NLBs und NATs vor Servern zu platzieren](#).

- Informationen zum Starten oder Stoppen Ihres Servers finden Sie unter [Schalten Sie Ihren Server online oder offline](#).
- Informationen zum Löschen eines Servers finden Sie unter [Löschen Sie einen Server](#).
- Informationen zum Bearbeiten der Eigenschaften eines Benutzers finden Sie unter [Verwaltung von Zugriffssteuerungen](#).

Protocols[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider[Edit](#)

Identity provider type
Service managed

 Note

Die Werte für die Beschreibung des Server-Host-Schlüssels und das Importdatum sind seit September 2022 neu. Diese Werte wurden eingeführt, um die Funktion für mehrere Hostschlüssel zu unterstützen. Diese Funktion erforderte die Migration aller einzelnen Hostschlüssel, die vor der Einführung mehrerer Hostschlüssel verwendet wurden. Der Wert Importdatum für einen migrierten Server-Hostschlüssel ist auf das Datum der letzten Änderung für den Server festgelegt. Das heißt, das Datum, das Sie für Ihren migrierten Hostschlüssel sehen, entspricht dem Datum, an dem Sie den Server vor der Migration des Server-Host-Schlüssels zuletzt geändert haben. Der einzige Schlüssel, der migriert wurde, ist Ihr ältester oder einziger Server-Hostschlüssel. Alle zusätzlichen Schlüssel haben ihr aktuelles Datum, ab dem Sie sie importiert haben. Darüber hinaus enthält der migrierte Schlüssel eine Beschreibung, anhand derer er leicht als migriert identifiziert werden kann.

Die Migration fand zwischen dem 2. und 13. September statt. Das tatsächliche Migrationsdatum innerhalb dieses Bereichs hängt von der Region Ihres Servers ab.

Additional details
Edit

Log group /aws/transfer/s-	Domain Amazon S3	SetStat option Ignore TLS session resumption - Passive IP -
Logging role Info -	Login display banner View the display message	
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	

Bearbeiten Sie die Dateiübertragungsprotokolle

Auf der AWS Transfer Family Konsole können Sie das Dateiübertragungsprotokoll bearbeiten. Das Dateiübertragungsprotokoll verbindet den Client mit dem Endpunkt Ihres Servers.

Um die Protokolle zu bearbeiten

1. Wählen Sie auf der Seite mit den Serverdetails neben Protokolle die Option Bearbeiten aus.
2. Aktivieren oder deaktivieren Sie auf der Seite Protokolle das oder die Kontrollkästchen für das Protokoll, um die folgenden Dateiübertragungsprotokolle hinzuzufügen oder zu entfernen:

- Secure Shell (SSH) File Transfer Protocol (SFTP) — Dateiübertragung über SSH

Weitere Informationen zu SFTP finden Sie unter [Erstellen Sie einen SFTP-enabled Server](#)

- File Transfer Protocol Secure (FTPS) — Dateiübertragung mit TLS-Verschlüsselung

Weitere Informationen zu FTP finden Sie unter [Einen FTPS-enabled Server erstellen](#).

- File Transfer Protocol (FTP) — unverschlüsselte Dateiübertragung

Weitere Informationen zu FTPS finden Sie unter [Erstellen Sie einen FTP-enabled Server](#)

Note

Wenn Sie einen vorhandenen Server haben, der nur für SFTP aktiviert ist, und Sie FTPS und FTP hinzufügen möchten, müssen Sie sicherstellen, dass Sie über die richtigen

Einstellungen für Identitätsanbieter und Endpunkttyp verfügen, die mit FTPS und FTP kompatibel sind.

Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#)[Save](#)

Wenn Sie FTPS auswählen, müssen Sie ein in AWS Certificate Manager (ACM) gespeichertes Zertifikat auswählen, das zur Identifizierung Ihres Servers verwendet wird, wenn Clients über FTPS eine Verbindung zu ihm herstellen.

Informationen zum Anfordern eines neuen öffentlichen Zertifikats finden Sie unter [Anfordern eines öffentlichen Zertifikats](#) im AWS Certificate Manager Benutzerhandbuch.

Informationen zum Importieren eines vorhandenen Zertifikats in ACM finden Sie unter [Zertifikate in ACM importieren](#) im AWS Certificate Manager Benutzerhandbuch.

Informationen zum Anfordern eines privaten Zertifikats für die Verwendung von FTPS über private IP-Adressen finden Sie unter [Anfordern eines privaten Zertifikats](#) im AWS Certificate Manager Benutzerhandbuch.

Zertifikate mit den folgenden kryptografischen Algorithmen und Schlüsselgrößen werden unterstützt:

- 2048-Bit-RSA (RSA_2048)
- 4096-Bit-RSA (RSA_4096)
- Elliptic Prime Curve 256-Bit (EC_prime256v1)
- Elliptic Prime Curve 384-Bit (EC_secp384r1)
- Elliptic Prime Curve 521-Bit (EC_secp521r1)

 Note

Das Zertifikat muss ein gültiges Zertifikat der SSL/TLS X.509 Version 3 mit angegebenem FQDN oder IP-Adresse sein und Informationen über den Aussteller enthalten.

3. Wählen Sie Speichern. Sie kehren zur Seite mit den Serverdetails zurück.

Bearbeiten Sie den Serverendpunkt

Auf der AWS Transfer Family Konsole können Sie den Serverendpunkttyp und den benutzerdefinierten Hostnamen ändern. Darüber hinaus können Sie für VPC-Endpoints die Informationen zur Verfügbarkeitszone bearbeiten.

Um die Serverendpunktdetails zu bearbeiten

1. Wählen Sie auf der Seite mit den Serverdetails neben Endpunktdetails die Option Bearbeiten aus.
2. Bevor Sie den Endpunkttyp bearbeiten können, müssen Sie zuerst den Server beenden. Anschließend können Sie auf der Seite Endpunktkonfiguration bearbeiten für Endpunkttyp einen der folgenden Werte wählen:
 - Öffentlich — Mit dieser Option ist Ihr Server über das Internet zugänglich.
 - VPC — Diese Option macht Ihren Server in Ihrer Virtual Private Cloud (VPC) zugänglich. Hinweise zu VPC finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).
3. Wählen Sie für Benutzerdefinierter Hostname eine der folgenden Optionen:
 - Keine — Wenn Sie keine benutzerdefinierte Domain verwenden möchten, wählen Sie Keine.

Sie erhalten einen Server-Hostnamen, der von bereitgestellt wird AWS Transfer Family. Der Server-Host-Name hat das Format `serverId.server.transfer.regionId.amazonaws.com`.

- Amazon Route 53 DNS-Alias — Um einen DNS-Alias zu verwenden, der in Route 53 automatisch für Sie erstellt wurde, wählen Sie diese Option.
- Anderes DNS — Um einen Hostnamen, den Sie bereits besitzen, in einem externen DNS-Service zu verwenden, wählen Sie Anderes DNS.

Wenn Sie Amazon Route 53 DNS-Alias oder Anderes DNS wählen, geben Sie die Methode zur Namensauflösung an, die dem Endpunkt Ihres Servers zugeordnet werden soll.

Beispiel: Die benutzerdefinierte Domäne heißt `sftp.inbox.example.com`. Ein benutzerdefinierter Host-Name verwendet einen von Ihnen bereitgestellten DNS-Namen, der von einem DNS-Service aufgelöst werden kann. Sie können Route 53 als Ihren DNS-Resolver verwenden oder Ihren eigenen DNS-Dienstanbieter verwenden. Informationen darüber, wie Route 53 AWS Transfer Family verwendet wird, um Traffic von Ihrer benutzerdefinierten Domain zum Serverendpunkt weiterzuleiten, finden Sie unter [Mit benutzerdefinierten Hostnamen arbeiten](#).

Endpoint configuration Info

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted Info
Access controlled using Security Groups

Access Info

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

Select a VPC ID [Create a VPC](#)

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel Save

4. Für VPC-Endpoints können Sie die Informationen im Bereich Availability Zones ändern.
5. Wählen Sie Speichern. Sie kehren zur Seite mit den Serverdetails zurück.

Bearbeiten Sie Ihre Logging-Konfiguration

Auf der AWS Transfer Family Konsole können Sie Ihre Protokollierungskonfiguration ändern.

 Note

Wenn Transfer Family beim Erstellen eines Servers eine CloudWatch Protokollierungs-IAM-Rolle für Sie erstellt hat, wird die IAM-Rolle aufgerufen. `AWSTransferLoggingAccess` Sie können es für alle Ihre Transfer Family Family-Server verwenden.

Um Ihre Logging-Konfiguration zu bearbeiten

1. Wählen Sie auf der Seite mit den Serverdetails neben **Zusätzliche Details** die Option **Bearbeiten** aus.
2. Wählen Sie je nach Konfiguration zwischen einer Logging-Rolle, einer strukturierten JSON-Protokollierung oder beidem. Weitere Informationen finden Sie unter [Die Protokollierung für einen Server aktualisieren](#).

Bearbeiten Sie die Sicherheitsrichtlinie

In diesem Verfahren wird erklärt, wie Sie die Sicherheitsrichtlinie eines Transfer Family Family-Servers mithilfe der AWS Transfer Family Konsole oder ändern AWS CLI.

 Note

Wenn Ihr Endpunkt dies ist FIPS-enabled, können Sie die FIPS-Sicherheitsrichtlinie nicht in eine Nicht-FIPS-Sicherheitsrichtlinie ändern.

Console

Um die Sicherheitsrichtlinie mithilfe der Konsole zu bearbeiten

1. Wählen Sie auf der Seite mit den Serverdetails neben **Zusätzliche Details** die Option **Bearbeiten** aus.
2. Wählen Sie im Abschnitt **Optionen für kryptografische Algorithmen** eine Sicherheitsrichtlinie aus, die die kryptografischen Algorithmen enthält, die für die Verwendung durch Ihren Server aktiviert sind.

Weitere Informationen zu Sicherheitsrichtlinien finden Sie unter [Sicherheitsrichtlinien für Server AWS Transfer Family](#).

3. Wählen Sie Speichern.

Sie kehren zur Seite mit den Serverdetails zurück, auf der Sie die aktualisierte Sicherheitsrichtlinie sehen können.

AWS CLI

So bearbeiten Sie die Sicherheitsrichtlinie mit der CLI

1. Führen Sie den folgenden Befehl aus, um die aktuelle Sicherheitsrichtlinie anzuzeigen, die mit Ihrem Server verknüpft ist.

```
aws transfer describe-server --server-id your-server-id
```

Dieser `describe-server` Befehl gibt alle Details für Ihren Server zurück, einschließlich der folgenden Zeile:

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

In diesem Fall lautet die Sicherheitsrichtlinie für den `ServerTransferSecurityPolicy-2018-11`.

2. Stellen Sie sicher, dass Sie den genauen Namen der Sicherheitsrichtlinie für den Befehl angeben. Führen Sie beispielsweise den folgenden Befehl aus, um den Server auf zu aktualisieren `TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name  
"TransferSecurityPolicy-2023-05"
```

Note

Die Namen der verfügbaren Sicherheitsrichtlinien sind unter [aufgeführt](#) Sicherheitsrichtlinien für Server AWS Transfer Family.

Bei Erfolg gibt der Befehl den folgenden Code zurück und aktualisiert die Sicherheitsrichtlinie Ihres Servers.

```
{  
  "ServerId": "your-server-id"  
}
```

Ändern Sie den verwalteten Workflow für Ihren Server

Auf der AWS Transfer Family Konsole können Sie den verwalteten Workflow ändern, der dem Server zugeordnet ist.

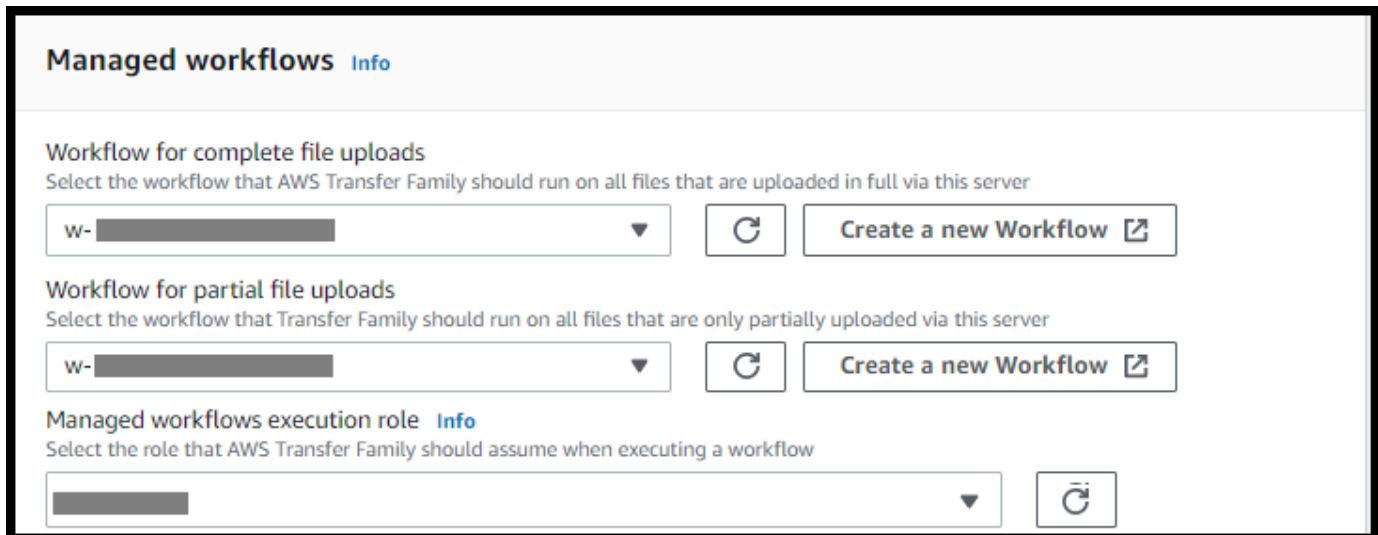
Um den verwalteten Workflow zu ändern

1. Wählen Sie auf der Seite mit den Serverdetails neben **Zusätzliche Details** die Option **Bearbeiten** aus.
2. Wählen Sie auf der Seite **Zusätzliche Details bearbeiten** im Abschnitt **Verwaltete Workflows** einen Workflow aus, der für alle Uploads ausgeführt werden soll.

Note

Wenn Sie noch keinen Workflow haben, wählen Sie **Neuen Workflow erstellen** aus, um einen zu erstellen.

- a. Wählen Sie die zu verwendende Workflow-ID aus.
- b. Wählen Sie eine Ausführungsrolle aus. Diese Rolle nimmt Transfer Family bei der Ausführung der Workflow-Schritte ein. Weitere Informationen finden Sie unter [IAM-Richtlinien für Workflows](#). Wählen Sie **Save (Speichern)** aus.



Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#) [external link]

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#) [external link]

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

3. Wählen Sie Speichern. Sie kehren zur Seite mit den Serverdetails zurück.

Ändern Sie die Display-Banner für Ihren Server

Auf der AWS Transfer Family Konsole können Sie die dem Server zugewiesenen Display-Banner ändern.

Um die Display-Banner zu ändern

1. Wählen Sie auf der Seite mit den Serverdetails neben Zusätzliche Details die Option Bearbeiten aus.
2. Geben Sie auf der Seite Zusätzliche Details bearbeiten im Abschnitt Display-Banner den Text für die verfügbaren Display-Banner ein.
3. Wählen Sie Speichern. Sie kehren zur Seite mit den Serverdetails zurück.

Schalten Sie Ihren Server online oder offline

Auf der AWS Transfer Family Konsole können Sie Ihren Server online oder offline schalten.

Um Ihren Server online zu schalten

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).

3. Aktivieren Sie das Kontrollkästchen des Servers, der offline ist.
4. Wählen Sie für Actions (Aktionen) die Option Start.

Es kann einige Minuten dauern, bis ein Server von offline auf online umgestellt wird.

 Note

Wenn Sie einen Server anhalten, um ihn offline zu schalten, fallen derzeit immer noch Servicegebühren für diesen Server an. Um zusätzliche serverbasierte Gebühren zu vermeiden, löschen Sie diesen Server.

Um Ihren Server offline zu schalten

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Klicken Sie im Navigationsbereich auf Servers (Server).
3. Aktivieren Sie das Kontrollkästchen des Servers, der online ist.
4. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp).

Während ein Server gestartet oder heruntergefahren wird, sind Server nicht für Dateioperationen verfügbar. Die Konsole zeigt den Start- oder Stopp-Status nicht an.

Wenn Sie den Fehler finden `START_FAILED` oder `STOP_FAILED`, wenden Sie sich an uns, AWS Support um Ihre Probleme zu lösen.

Konfiguration des Identitätsanbieters bearbeiten

Sie können den Identitätsanbietertyp Ihres Servers von einem beliebigen Typ auf einen beliebigen anderen Typ ändern. Die verfügbaren Identitätsanbietertypen sind:

- Dienst verwaltet — Benutzeranmeldeinformationen innerhalb des Dienstes speichern
- AWS Directory Service — Verwenden Sie AWS Managed Microsoft AD oder AWS Directory Service für Entra ID Domain Services
- Benutzerdefiniert — Verwenden Sie die Lambda-Funktion oder Amazon API Gateway zur Integration mit Ihrem bestehenden Identitätsanbieter

Wenn Sie die Typen von Identitätsanbietern ändern, müssen Sie je nach Umstellung spezifische Informationen angeben. In den folgenden Abschnitten werden die erforderlichen Informationen für jede Art von Änderung beschrieben.

 Important

Überlegungen beim Wechsel des Identitätsanbieters:

- **Benutzermigration** — Beim Ändern der Identitätsanbietertypen werden bestehende Benutzerkonfigurationen nicht automatisch migriert. Sie müssen Benutzer im neuen Identitätsanbietersystem einrichten.
- **Testen** — Testen Sie die neue Identitätsanbieter-Konfiguration gründlich, bevor Sie die Änderung in Produktionsumgebungen vornehmen.
- **Berechtigungen** — Stellen Sie sicher, dass der neue Identitätsanbieter über die erforderlichen IAM-Berechtigungen und -Rollen verfügt, bevor Sie die Änderung vornehmen.

Umstellung auf einen vom Service verwalteten Identitätsanbieter

Wenn Sie von einem anderen Identitätsanbietertyp zu einem vom Dienst verwalteten Anbieter wechseln, müssen Sie:

- Wählen Sie als Identitätsanbietertyp „Service managed“ aus
- Erstellen Sie neue Benutzer direkt AWS Transfer Family nach Abschluss der Änderung, da vorhandene Benutzerkonfigurationen von anderen Identitätsanbietern nicht übertragen werden

Beispiel: Wenn Sie von einem benutzerdefinierten Identitätsanbieter zu einem vom Dienst verwalteten Identitätsanbieter wechseln, müssen Sie alle Benutzerkonten und die zugehörigen Berechtigungen innerhalb des AWS Transfer Family Dienstes neu erstellen.

Wechsel zum AWS Directory Service

Wenn Sie von einem anderen Identitätsanbietertyp zu AWS Directory Service wechseln, müssen Sie Folgendes angeben:

- **Verzeichnis** — Wählen Sie ein vorhandenes AWS Managed Microsoft AD- oder AWS Directory Service for Entra ID Domain Services-Verzeichnis aus

- **Zugriff** — Wählen Sie aus, ob der Zugriff auf eine bestimmte Gruppe beschränkt oder allen Benutzern im Verzeichnis der Zugriff gewährt werden soll
- **Zugriffsrolle** — Eine IAM-Rolle, die AWS Transfer Family den Zugriff auf Ihr Verzeichnis ermöglicht

Beispiel: Wenn Sie von service-managed zu AWS Directory Service wechseln, würden Sie Ihr vorhandenes `d-1234567890` Verzeichnis auswählen, den Zugriff auf die `TransferUsers` Gruppe einschränken und die `TransferDirectoryAccessRole` IAM-Rolle angeben.

Wechseln Sie zum benutzerdefinierten Identitätsanbieter

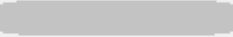
Wenn Sie von einem anderen Identitätsanbietertyp zu einem benutzerdefinierten Identitätsanbieter wechseln, müssen Sie zwischen Lambda-Funktion oder Amazon API Gateway wählen und die erforderliche Konfiguration angeben:

Lambda-Funktion verwenden

Geben Sie für die Lambda-Funktionsintegration Folgendes an:

- **Funktion** — Wählen Sie eine vorhandene Lambda-Funktion aus, die die Authentifizierung abwickelt
- **Authentifizierungsmethode** (für das SFTP-Protokoll) — Wählen Sie ein Passwort, einen öffentlichen Schlüssel oder beides

Beispiel: Wenn Sie von AWS Directory Service zu einem benutzerdefinierten Lambda-Identitätsanbieter wechseln, würden Sie Ihre `TransferCustomAuth` Funktion auswählen und Password als Authentifizierungsmethode wählen.

Transfer Family > Servers > s- > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

- ☐ Service managed
Create and manage users within the service
- ☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

- ☒ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization
- ☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function





Authentication methods

Choose which authentication methods are required for users to connect to your server

- ☒ Password OR public key
- ☐ Password ONLY
- ☐ Public Key ONLY
- ☐ Password AND public key

 Either a valid password or valid private key will be required during user authentication

Cancel

Save

Amazon API Gateway verwenden

Geben Sie für die Amazon API Gateway Gateway-Integration Folgendes an:

- API-Gateway-URL — Die Aufruf-URL Ihres API-Gateway-Endpunkts

- **Aufrufrolle** — Eine IAM-Rolle, mit der AWS Transfer Family Sie Ihr API Gateway aufrufen können
- **Authentifizierungsmethode** (für das SFTP-Protokoll) — Wählen Sie ein Passwort, einen öffentlichen Schlüssel oder beides

Beispiel: Wenn Sie von Service-Managed zu API Gateway wechseln, geben Sie die URL `anhttps://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, geben die `TransferApiGatewayInvocationRole` IAM-Rolle an und wählen Public Key als Authentifizierungsmethode.

Transfer Family > Servers > s-[REDACTED] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

☐ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel Save

Wechsel von Amazon API Gateway zur Lambda-Funktion

Ein gängiger Übergang ist der Wechsel von Amazon API Gateway zur Lambda-Funktion für die Integration benutzerdefinierter Identitätsanbieter. Diese Änderung ermöglicht es Ihnen, Ihre Architektur zu vereinfachen und gleichzeitig dieselbe Authentifizierungslogik beizubehalten.

Die wichtigsten Überlegungen zu diesem Übergang:

- Gleiche Funktion, unterschiedliche Berechtigungen — Sie können dieselbe Lambda-Funktion sowohl für API Gateway als auch für die direkte Lambda-Integration verwenden, aber die Ressourcenrichtlinie muss aktualisiert werden.
- Anforderungen an die Ressourcenrichtlinie — Beim Wechsel zur direkten Lambda-Integration muss die Ressourcenrichtlinie der Funktion zusätzlich zu die `transfer.amazonaws.com` Berechtigung zum Aufrufen der Funktion gewähren. `apigateway.amazonaws.com`

Um diese Änderung vorzunehmen

1. Aktualisieren Sie die Ressourcenrichtlinie Ihrer Lambda-Funktion, damit `transfer.amazonaws.com` die Funktion aufgerufen werden kann.
2. Ändern Sie in der AWS Transfer Family Konsole den Identitätsanbieter von API Gateway zu Lambda-Funktion.
3. Wählen Sie Ihre bestehende Lambda-Funktion aus.
4. Testen Sie die Konfiguration, um sicherzustellen, dass die Authentifizierung korrekt funktioniert.

Beispiel für eine Ressourcenrichtlinie für die direkte Lambda-Integration:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Benutzererhaltung bei Übergängen zum Identitätsanbieter

Beim Wechsel zwischen Identitätsanbietertypen werden bestehende Benutzerkonfigurationen in bestimmten Szenarien beibehalten, um bei Problemen ein effizientes Rollback zu ermöglichen:

- Service-managed zum benutzerdefinierten Identitätsanbieter und zurück — Wenn Sie von einem vom Dienst verwalteten zu einem benutzerdefinierten Identitätsanbieter und dann zurück zu einem vom Dienst verwalteten Identitätsanbieter wechseln, bleiben alle Benutzer in ihrer letzten bekannten Konfiguration erhalten.
- AWS Directory Service zum benutzerdefinierten Identitätsanbieter und zurück — Wenn Sie von AWS Directory Service einem benutzerdefinierten Identitätsanbieter und dann zurück zu wechseln AWS Directory Service, werden alle Definitionen für Gruppen mit delegiertem Zugriff in ihrer letzten bekannten Konfiguration beibehalten.

Dieses Beibehaltungsverhalten ermöglicht es Ihnen, benutzerdefinierte Identitätsanbieter-Konfigurationen sicher zu testen und zu Ihrer vorherigen Konfiguration zurückzukehren, ohne die Benutzerzugriffskonfigurationen zu verlieren.

Wichtige Überlegungen beim Wechsel des Identitätsanbieters

- Benutzermigration — Beim Ändern der Identitätsanbietertypen werden bestehende Benutzerkonfigurationen nicht automatisch migriert. Sie müssen Benutzer im neuen Identitätsanbietersystem einrichten.
- Testen — Testen Sie die neue Identitätsanbieter-Konfiguration gründlich, bevor Sie die Änderung in Produktionsumgebungen vornehmen.
- Berechtigungen — Stellen Sie sicher, dass der neue Identitätsanbieter über die erforderlichen IAM-Berechtigungen und -Rollen verfügt, bevor Sie die Änderung vornehmen.

Hostschlüssel für Ihren SFTP-enabled Server verwalten

Server-Hostschlüssel sind private Schlüssel, die vom Transfer Family Family-Server verwendet werden, um dem Anrufer eine eindeutige Identität zu geben und sicherzustellen, dass es sich um den richtigen Server handelt. Diese Garantie wird durch das Vorhandensein des richtigen öffentlichen Schlüssels in der Datei des Anrufers durchgesetzt. `known_hosts` (Die `known_hosts` Datei ist eine Standardfunktion, die von den meisten SSH-Clients verwendet wird, um die öffentlichen Schlüssel für die Server zu speichern, mit denen Sie eine Verbindung hergestellt haben.) Sie können den

öffentlichen Schlüssel, der Ihrem Server-Host-Schlüssel entspricht, abrufen, indem Sie ihn `ssh-keyscan` für Ihren Server ausführen.

 Important

Das versehentliche Ändern des Host-Schlüssels eines Servers kann zu Unterbrechungen führen. Je nachdem, wie Ihr SFTP-Client konfiguriert ist, kann er sofort fehlschlagen, mit der Meldung, dass kein vertrauenswürdiger Hostschlüssel vorhanden ist, oder es werden drohende Eingabeaufforderungen angezeigt. Wenn es Skripts für die Automatisierung von Verbindungen gibt, würden diese höchstwahrscheinlich ebenfalls fehlschlagen.

AWS Transfer Family Generiert standardmäßig Hostschlüssel für Ihren SFTP-enabled Server. Sie können Server-Hostschlüssel importieren, um die Hostidentität zu wahren und zu vermeiden, dass Client-Vertrauensspeicher aktualisiert werden. [Wann müssen Hostschlüssel importiert werden](#) listet einige Gründe auf, warum Sie dies tun sollten. Wenn Sie keine Hostschlüssel angeben, werden neue für Sie generiert.

AWS Transfer Family unterstützt mehrere Hostschlüssel verschiedener Typen (RSA, ECDSA und ED25519), um die Kompatibilität mit einer breiteren Palette von Client-Host-Signaturalgorithmen zu gewährleisten. Verschiedene Schlüsseltypen ermöglichen spezifische Algorithmen: RSA-Schlüssel ermöglichen RSA-*-Algorithmen, ECDSA-Schlüssel ermöglichen ECDSA-*-Algorithmen und ED25519-Schlüssel ermöglichen ED25519-Algorithmen. Planen Sie Ihre Schlüsseltypen bei der Servererstellung, da die Einführung zusätzlicher Schlüsseltypen, nachdem die Clients mit dem Server begonnen haben, für einige Clients störend sein kann und genauso problematisch sein kann wie das Ersetzen vorhandener Hostschlüssel.

Um zu verhindern, dass Ihre Benutzer erneut aufgefordert werden, die Authentizität Ihres SFTP-enabled Servers zu überprüfen, importieren Sie den Hostschlüssel für Ihren lokalen Server auf den SFTP-enabled Server. Dies verhindert auch, dass Ihre Benutzer eine Warnung in Bezug auf einen potentiellen Man-in-the-Middle-Angriff erhalten.

Als zusätzliche Sicherheitsmaßnahme können Sie die Hostschlüssel auch regelmäßig wechseln. Details hierzu finden Sie unter [Rotiert die Server-Hostschlüssel](#).

 Note

Server-Hostschlüssel werden von Servern verwendet, die das SFTP-Protokoll unterstützen.

Wann müssen Hostschlüssel importiert werden

Hostschlüssel AWS Transfer Family können zwar automatisch generiert werden, es gibt jedoch mehrere Szenarien, in denen der Import Ihrer eigenen Hostschlüssel betriebliche Vorteile bietet:

- **Servermigration** — Sie migrieren von einem vorhandenen Server zu einem vorhandenen Server AWS Transfer Family und möchten vermeiden, dass die Client-Vertrauensspeicher (known_hostsDateien) für bestehende Clients aktualisiert werden.
- **Notfallwiederherstellung und Failover** — Sie haben mehrere AWS Transfer Family Server (z. B. einen in USA Ost (Ohio) und einen in USA West (Oregon)), die denselben öffentlichen DNS-Namen verwenden. Die Verwendung derselben Hostschlüssel auf beiden Servern gewährleistet einen reibungslosen Failover ohne Fehler bei der Client-Authentifizierung.
- **Betriebskontinuität** — Sie möchten, dass das Host-Schlüsselmateriale in future für die Verwendung mit anderen Servern (AWS Transfer Family oder anderweitig) verfügbar ist, um eine konsistente Serveridentität in Ihrer gesamten Infrastruktur aufrechtzuerhalten.
- **Algorithmuskontrolle** — Sie möchten mehr Client-Kompatibilität erreichen, indem Sie mehr Host-Schlüsselalgorithmen bereitstellen, oder Sie möchten kontrollieren, welche Algorithmen Clients verwenden können, indem Sie nur Schlüssel anbieten, die mit bestimmten Algorithmen kompatibel sind.

Die folgenden Themen enthalten detaillierte Verfahren für die Verwaltung von Server-Hostschlüsseln:

- [Fügen Sie einen zusätzlichen Server-Hostschlüssel hinzu](#)- Fügen Sie Ihrem Server zusätzliche Hostschlüssel hinzu
- [Löscht einen Server-Hostschlüssel](#)- Entfernen Sie Hostschlüssel von Ihrem Server
- [Rotiert die Server-Hostschlüssel](#)- Rotieren Sie die Hostschlüssel für mehr Sicherheit
- [Zusätzliche Schlüsselinformationen zum Server-Host](#)- Host-Schlüsseldetails anzeigen und verwalten

Fügen Sie einen zusätzlichen Server-Hostschlüssel hinzu

Auf der AWS Transfer Family Konsole können Sie zusätzliche Server-Hostschlüssel hinzufügen. Das Hinzufügen zusätzlicher Hostschlüssel in unterschiedlichen Formaten kann nützlich sein, um einen Server zu identifizieren, wenn Clients eine Verbindung zu ihm herstellen, und um Ihr Sicherheitsprofil zu verbessern. Wenn Ihr Originalschlüssel beispielsweise ein RSA-Schlüssel ist, können Sie einen zusätzlichen ECDSA-Schlüssel hinzufügen.

Note

Der SFTP-Client stellt die Verbindung mit dem ältesten Schlüssel in der Konfiguration her, der dem Algorithmus des Schlüssels entspricht. Der älteste Schlüssel für jeden Schlüsseltyp (RSA, ECDSA oder ED25519) ist der aktive Schlüssel für den Server für diesen Typ.

Sicherheitshinweis, wenn ein Transfer Family Family-Server über mehrere Arten von Hostschlüsseln verfügt

Wenn ein Server über mehrere Arten von Hostschlüsseln verfügt, kann der SFTP-Client eine Präferenz nach Typ zuweisen. Wenn also RSA-, ECDSA- und ED25519-Hostschlüssel für den Server vorhanden sind, hängt die Auswahl von der Präferenz nach Typ ab.

Moderne SFTP-Clients bevorzugen ECDSA- und ED25519-Hostschlüssel, sofern sie existieren. Dies wird wichtig, wenn Sie einen ECDSA- oder ED25519-Schlüssel hinzufügen möchten, obwohl der Server zuvor nur über RSA-Schlüssel verfügte. Das Hinzufügen des neuen ECDSA- oder ED25519-Schlüssels würde sich möglicherweise als Sicherheitswarnung für einen Client äußern.

Für den Client wird der Schlüssel so aussehen, als hätte er sich geändert, obwohl er in Wirklichkeit nicht geändert wurde: Der neue Schlüssel wurde zusätzlich zum vorhandenen RSA-Schlüssel hinzugefügt. Denken Sie daran, wenn Sie neue Typen von Server-Host-Schlüsseln hinzufügen möchten.

Um einen zusätzlichen Server-Host-Schlüssel hinzuzufügen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann einen Server aus, der das SFTP-Protokoll verwendet.
3. Scrollen Sie auf der Seite mit den Serverdetails nach unten zum Abschnitt Server-Hostschlüssel.

Server host keys (2)							Actions	Add host key
Find resources							< 1 >	
☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	Default host key	hostkey- [redacted]	SHA256: [redacted]	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey- [redacted]	SHA256: [redacted]	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

4. Wählen Sie Hostschlüssel hinzufügen aus.

Die Seite Server-Host-Schlüssel hinzufügen wird angezeigt.

5. Geben Sie im Abschnitt Server-Hostschlüssel einen privaten RSA-, ECDSA- oder ED25519-Schlüssel ein, der zur Identifizierung Ihres Servers verwendet wird, wenn Clients über den Server eine Verbindung zu ihm herstellen. SFTP-enabled

 Note

Wenn Sie einen Server-Host-Schlüssel erstellen, achten Sie darauf, Folgendes anzugeben -N "" (keine Passphrase). Einzelheiten [SSH-Schlüssel auf macOS, Linux oder Unix erstellen](#) zum Generieren von Schlüsselpaaren finden Sie unter.

6. (Optional) Fügen Sie eine Beschreibung hinzu, um zwischen mehreren Server-Hostschlüsseln zu unterscheiden. Sie können Ihrem Schlüssel auch Tags hinzufügen.
7. Wählen Sie Schlüssel hinzufügen. Sie kehren zur Seite mit den Serverdetails zurück.

Um einen Hostschlüssel mithilfe von AWS Command Line Interface (AWS CLI) hinzuzufügen, verwenden Sie die [ImportHostKey](#) API-Operation und geben Sie den neuen Hostschlüssel an. Wenn Sie einen neuen SFTP-enabled Server erstellen, geben Sie Ihren Hostschlüssel als Parameter in der [CreateServer](#) API-Operation an. Sie können den auch verwenden AWS CLI , um die Beschreibung für einen vorhandenen Hostschlüssel zu aktualisieren.

Der folgende `import-host-key` AWS CLI Beispielbefehl importiert einen Hostschlüssel für den angegebenen SFTP-enabled Server.

```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

Löscht einen Server-Hostschlüssel

Auf der AWS Transfer Family Konsole können Sie einen Server-Hostschlüssel löschen.

Um einen Server-Host-Schlüssel zu löschen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Wählen Sie im linken Navigationsbereich Server und dann einen Server aus, der das SFTP-Protokoll verwendet.
3. Scrollen Sie auf der Seite mit den Serverdetails nach unten zum Abschnitt Server-Hostschlüssel.

Server host keys (2)							Actions ▾	Add host key
Find resources							< 1 >	
☐	Name	Host key ID ▾	Fingerprint Info	Description ▾	Key type ▾	Date imported ▾		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

- Wählen Sie im Abschnitt Server-Hostschlüssel einen Schlüssel aus, und klicken Sie dann unter Aktionen auf Löschen.
- Geben Sie im daraufhin angezeigten Bestätigungsdialogfeld das Wort **delete**, und klicken Sie dann auf Löschen, um zu bestätigen, dass Sie den Hostschlüssel löschen möchten.

Der Hostschlüssel wird von der Serverseite gelöscht.

Um den Hostschlüssel mithilfe von zu löschen AWS CLI, verwenden Sie den [DeleteHostKey](#) API-Vorgang und geben Sie die Server-ID und die Hostschlüssel-ID ein.

Der folgende `delete-host-key` AWS CLI Beispielbefehl löscht einen Hostschlüssel für den angegebenen SFTP-enabled Server.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Rotiert die Server-Hostschlüssel

In regelmäßigen Abständen können Sie Ihren Server-Host-Schlüssel rotieren. In diesem Thema wird beschrieben, wie der Server auswählt, welcher Schlüssel verwendet werden soll, und wie diese Schlüssel rotiert werden.

Wie der Client einen Server-Host-Schlüssel auswählt

Die Art und Weise, wie Transfer Family den anzuwendenden Serverschlüssel auswählt, hängt von den Bedingungen für den SFTP-Client ab, wie hier erklärt wird. Es wird davon ausgegangen, dass es einen älteren und einen neueren Schlüssel gibt.

- Ein SFTP-Client hat zuvor keinen öffentlichen Hostschlüssel für den Server. Wenn der Client zum ersten Mal eine Verbindung zum Server herstellt, tritt einer der folgenden Fälle ein:
 - Der Client schlägt die Verbindung fehl, wenn er dafür konfiguriert ist.
 - Oder der Client wählt den ersten Schlüssel aus, der den möglichen verfügbaren Algorithmen entspricht, und fragt den Benutzer, ob dieser Schlüssel vertrauenswürdig ist. Wenn ja, aktualisiert der Client die `known_hosts` Datei (oder die lokale Konfigurationsdatei oder

Ressource, die der Client zum Aufzeichnen von Vertrauensentscheidungen verwendet) automatisch und gibt diesen Schlüssel ein.

- Ein SFTP-Client hat einen älteren Schlüssel in seiner `known_hosts` Datei. Der Client bevorzugt es, diesen Schlüssel zu verwenden, auch wenn ein neuerer Schlüssel existiert, entweder für den Algorithmus dieses Schlüssels oder für einen anderen Algorithmus. Das liegt daran, dass der Client dem Schlüssel, der sich in seiner `known_hosts` Datei befindet, ein höheres Maß an Vertrauen entgegenbringt.
- Ein SFTP-Client hat den neuen Schlüssel (in einem der verfügbaren Algorithmen) in seiner `known_hosts` Schlüsseldatei. Der Client ignoriert ältere Schlüssel, weil sie nicht vertrauenswürdig sind, und verwendet den neuen Schlüssel.
- Ein SFTP-Client hat beide Schlüssel in seiner `known_hosts` Datei. Der Client wählt den ersten Schlüssel anhand des Index aus, der der vom Server angebotenen Liste der verfügbaren Schlüssel entspricht.

Transfer Family bevorzugt es, dass der SFTP-Client alle Schlüssel in seiner `known_hosts` Datei hat, da dies die größte Flexibilität bei der Verbindung zu einem Transfer Family Family-Server ermöglicht. Die Schlüsselrotation basiert auf der Tatsache, dass mehrere Einträge in der `known_hosts` Datei für denselben Transfer Family Family-Server vorhanden sein können.

Rotieren Sie das Verfahren für den Server-Host-Schlüssel

Nehmen wir als Beispiel an, dass Sie Ihrem Transfer Family Family-Server den folgenden Satz von Server-Hostschlüsseln hinzugefügt haben.

Server-Host-Schlüssel

Typ des Host-Schlüssels	Datum, das dem Server hinzugefügt wurde
RSA	01. April 2020
ECDSA	1. Februar 2020
ED25519	1. Dezember 2019
RSA	1. Oktober 2019
ECDSA	1. Juni 2019
ED25519	1. März 2019

Um den Server-Host-Schlüssel zu rotieren

1. Fügen Sie einen neuen Server-Host-Schlüssel hinzu. Dieses Verfahren wird unter beschrieben[Fügen Sie einen zusätzlichen Server-Hostschlüssel hinzu](#).
2. Löschen Sie einen oder mehrere Hostschlüssel desselben Typs, die Sie zuvor hinzugefügt haben. Dieses Verfahren wird unter beschrieben[Löscht einen Server-Hostschlüssel](#).
3. Alle Tasten sind sichtbar und können je nach dem zuvor unter beschriebenen Verhalten aktiv sein[Wie der Client einen Server-Host-Schlüssel auswählt](#).

Zusätzliche Schlüsselinformationen zum Server-Host

Sie können einen Hostschlüssel auswählen, um Details für diesen Schlüssel anzuzeigen.

Transfer Family > Servers > s-3fe215d89f074ed2a > Hostkey: hostkey-a6fed60bcb704ea9b

hostkey-a6fed60bcb704ea9b

Delete

Host key configuration

Edit

Name

ecdsa-521

Fingerprint

SHA256: [redacted]

Description

ECDSA host key

Key type

ecdsa-sha2-nistp521

Date imported

Thu, 13 Jun 2024 17:08:59 GMT

Amazon Resource Name (ARN)

arn:aws:transfer:us-east-1:[redacted]:host-key/s-[redacted]/hostkey-a

[redacted]

Sie können einen Hostschlüssel löschen oder seine Beschreibung im Aktionsmenü auf dem Bildschirm mit den Serverdetails bearbeiten. Wählen Sie den Host-Schlüssel und dann die entsprechende Aktion aus dem Menü aus.

Server host keys (2)

Find resources

Actions

Edit

Delete

Add host key

< 1 >

	Name	Host key ID	Fingerprint	Description	Key type	Date imported
☐	Default host key	hostkey-[redacted]	SHA256:[redacted]	Default	ssh-rsa	2023-06-30
☒	ecdsa-521	hostkey-[redacted]	SHA256:[redacted]	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

Überwachung der Nutzung in der Konsole

Informationen zu den Messwerten Ihres Servers finden Sie auf der Seite mit den Serverdetails. Auf diese Weise können Sie Ihre Workloads bei Dateiübertragungen von einem zentralen Ort aus überwachen. Mithilfe eines zentralen Dashboards können Sie verfolgen, wie viele Dateien Sie mit Ihren Partnern ausgetauscht haben, und deren Nutzung genau verfolgen. Details hierzu finden Sie unter [SFTP-, FTPS- und FTP-Serverdetails anzeigen](#). In der folgenden Tabelle werden die für Transfer Family verfügbaren Metriken beschrieben.

Namespace	Metrik	Description
AWS/Transfer	BytesIn	Die Gesamtzahl der auf den Server übertragenen Byte. Berichtskriterien: - Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. - Für AS2: wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und diese ausgibt, sobald die Verarbeitung der eingehenden Nachricht abgeschlossen ist Einheiten: Anzahl Zeitraum: 5 Minuten
	BytesOut	Die Gesamtzahl der vom Server übertragenen Byte. Berichtskriterien: Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben.

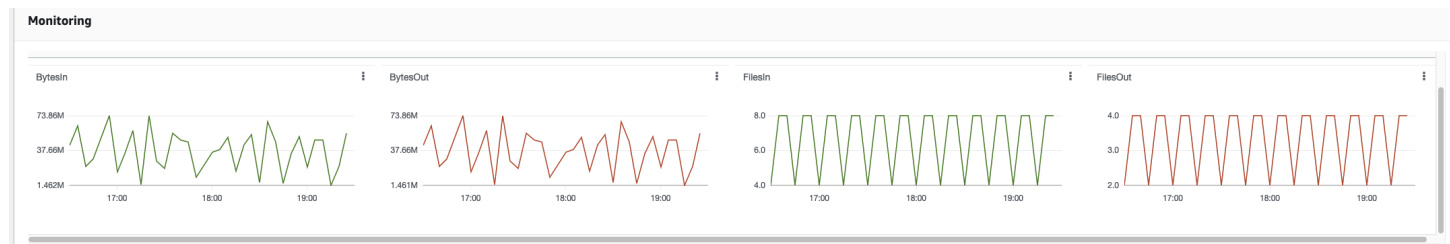
Namespace	Metrik	Description
		Für AS2: wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Anschluss aus anruft und die Nachricht gesendet wird, sobald die Verarbeitung der ausgehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten
	FilesIn	Die Gesamtzahl der auf den Server übertragenen Dateien. Bei Servern, die das AS2-Protokoll verwenden, stellt diese Metrik die Anzahl der empfangenen Nachrichten dar. Berichtskriterien: - Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. - Für AS2: wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und diese ausgibt, sobald die Verarbeitung der eingehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten

Namespace	Metrik	Description
	FilesOut	Die Gesamtzahl der vom Server übertragenen Dateien. Berichtskriterien: • Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. • Für AS2: wenn der Kunde StartFileTransfer von seinem AS2-Anschluss aus anruft und die Nachricht gesendet wird, sobald die Verarbeitung der ausgehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten
	InboundMessage	Die Gesamtzahl der erfolgreich von einem Handelspartner empfangenen AS2-Nachrichten. Berichtskriterien: Wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und versendet, sobald die Verarbeitung der eingehenden Nachricht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten

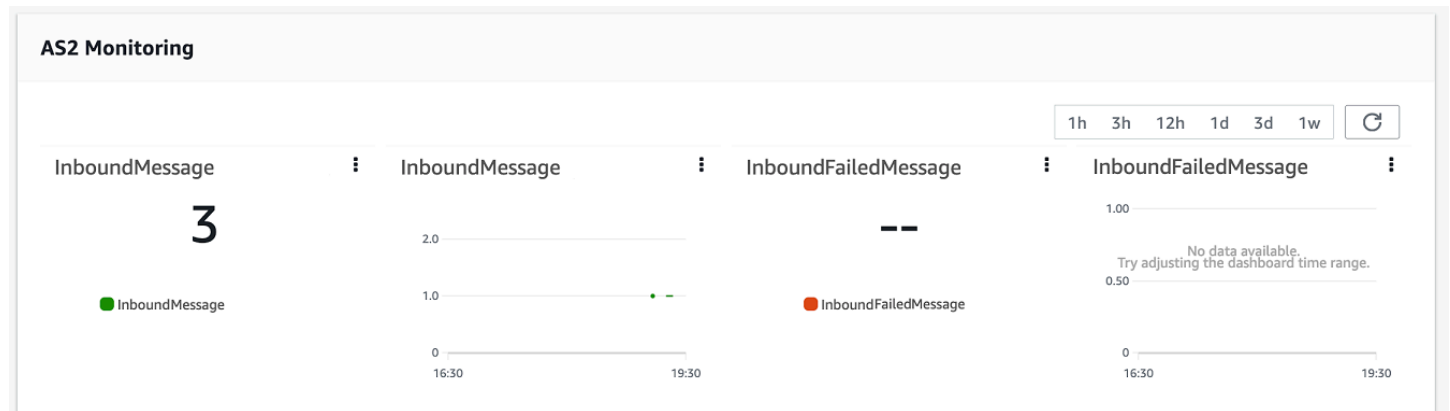
Namespace	Metrik	Description
	InboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die von einem Handelspartner erfolglos empfangen wurden. Das heißt, ein Handelspartner hat eine Nachricht gesendet, aber der Transfer Family Family-Server konnte sie nicht erfolgreich verarbeiten. Berichtskriterien: Wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und sofort nach erfolgloser Verarbeitung der eingehenden Nachricht gesendet wird Einheiten: Anzahl Zeitraum: 5 Minuten
	OnUploadExecutionsStarted	Die Gesamtzahl der auf dem Server gestarteten Workflow-Ausführungen. Berichtskriterien: Wird bei jedem Start einer Ausführung ausgelöst Einheiten: Anzahl Zeitraum: 1 Minute
	OnUploadExecutionsSuccess	Die Gesamtzahl der erfolgreichen Workflow-Ausführungen auf dem Server. Berichtskriterien: Wird jedes Mal ausgelöst, wenn eine Ausführung erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 1 Minute

Namespace	Metrik	Description
	OnUploadExecutionsFailed	Die Gesamtzahl der erfolgreichen Workflow-Ausführungen auf dem Server. Berichtskriterien: Wird jedes Mal ausgelöst, wenn eine Ausführung nicht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 1 Minute
	OutboundMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolgreich an einen Handelspartner gesendet wurden. Berichtskriterien: Wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Connector aus anruft und die Nachricht sendet, sobald die Verarbeitung der ausgehenden Nachricht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten
	OutboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolglos an einen Handelspartner gesendet wurden. Berichtskriterien: Wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Connector aus anruft und die Nachricht sendet, sobald die Verarbeitung der ausgehenden Nachricht erfolglos abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten

Der Abschnitt Monitoring enthält vier einzelne Grafiken. Diese Diagramme zeigen die eingehenden und ausgehenden Byte, die eingehenden und die ausgehenden Dateien.



Für Server, auf denen das AS2-Protokoll aktiviert ist, befindet sich unter den Überwachungsinformationen ein Abschnitt AS2-Überwachung. Dieser Abschnitt enthält Angaben zur Anzahl der eingehenden Nachrichten, sowohl erfolgreicher als auch fehlgeschlagener Nachrichten.



Um das ausgewählte Diagramm in einem eigenen Fenster zu öffnen, wählen Sie das Erweiterungssymbol



Sie können auch auf das vertikale Ellipsensymbol



eines Diagramms klicken, um ein Dropdownmenü mit den folgenden Elementen zu öffnen:

- Vergrößern — Öffnet das ausgewählte Diagramm in einem eigenen Fenster.
- Aktualisieren — Lädt das Diagramm mit den neuesten Daten neu.
- In Metriken anzeigen — Öffnet die entsprechenden Metrikdetails in Amazon CloudWatch.
- Protokolle anzeigen — Öffnet die entsprechende Protokollgruppe in CloudWatch.

Verwaltung von Zugriffssteuerungen

Sie können den Zugriff eines Benutzers auf AWS Transfer Family Ressourcen mithilfe einer AWS Identity and Access Management (IAM-) Richtlinie steuern. Eine IAM-Richtlinie ist eine Aussage, in der Regel im JSON-Format, die eine bestimmte Zugriffsebene auf eine Ressource ermöglicht. Sie verwenden eine IAM-Richtlinie, um zu definieren, welche Dateioperationen Sie Ihren Benutzern gestatten möchten und welche nicht. Sie können auch eine IAM-Richtlinie verwenden, um zu definieren, auf welche Amazon S3 S3-Buckets Sie Ihren Benutzern Zugriff gewähren möchten. Um diese Richtlinien für Benutzer festzulegen, erstellen Sie eine IAM-Rolle, der AWS Transfer Family die IAM-Richtlinie und die Vertrauensbeziehung zugeordnet sind.

Jedem Benutzer wird eine IAM-Rolle zugewiesen. Der verwendete IAM-Rollentyp wird als Servicerolle bezeichnet. AWS Transfer Family Wenn sich ein Benutzer bei Ihrem Server anmeldet, AWS Transfer Family nimmt er die dem Benutzer zugeordnete IAM-Rolle an. Weitere Informationen zum Erstellen einer IAM-Rolle, die einem Benutzer Zugriff auf einen Amazon S3 S3-Bucket gewährt, finden Sie unter [Creating a role to delegate permissions to an AWS service](#) im IAM-Benutzerhandbuch.

Sie können nur Schreibzugriff auf Amazon S3 S3-Objekte gewähren, indem Sie bestimmte Berechtigungen innerhalb einer IAM-Richtlinie verwenden. Details hierzu finden Sie unter [Gewähren Sie die Möglichkeit, nur Dateien zu schreiben und aufzulisten](#).

Der AWS Storage-Blog enthält einen Beitrag, in dem detailliert beschrieben wird, wie der Zugriff mit den geringsten Rechten eingerichtet wird. Einzelheiten finden Sie unter [Implementieren des Zugriffs mit den geringsten Rechten in einem AWS Transfer Family Workflow](#).

Note

Wenn Ihr Amazon S3 S3-Bucket mit AWS Key Management Service (AWS KMS) verschlüsselt ist, müssen Sie in Ihrer Richtlinie zusätzliche Berechtigungen angeben. Details hierzu finden Sie unter [Datenschutz und Verschlüsselung](#). Darüber hinaus finden Sie weitere Informationen zu [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Themen

- [Lese- und Schreibzugriff auf einen Amazon S3 S3-Bucket zulassen](#)
- [Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#)

- [Dynamische Ansätze zur Rechteverwaltung](#)

Lese- und Schreibzugriff auf einen Amazon S3 S3-Bucket zulassen

In diesem Abschnitt wird beschrieben, wie Sie eine IAM-Richtlinie erstellen, die Lese- und Schreibzugriff auf einen bestimmten Amazon S3 S3-Bucket ermöglicht. Wenn Sie Ihrem Benutzer eine IAM-Rolle mit dieser IAM-Richtlinie zuweisen, erhält dieser Benutzer read/write Zugriff auf den angegebenen Amazon S3 S3-Bucket.

Die folgende Richtlinie bietet programmatischen Lese-, Schreib- und Tagging-Zugriff auf einen Amazon S3 S3-Bucket. Die PutObjectACL Anweisungen GetObjectACL und sind nur erforderlich, wenn Sie den kontoübergreifenden Zugriff aktivieren müssen. Das heißt, Ihr Transfer Family Family-Server muss auf einen Bucket in einem anderen Konto zugreifen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

```
]
}
```

Die Aktion `ListBucket` setzt die Berechtigung für den Bucket selbst voraus. Die Aktionen `PUT`, `GET` und `DELETE` setzen Objektberechtigungen voraus. Da es sich um unterschiedliche Ressourcen handelt, werden sie mit unterschiedlichen Amazon-Ressourcennamen (ARNs) angegeben.

Um den Zugriff Ihrer Benutzer nur auf das `home` Präfix des angegebenen Amazon S3 S3-Buckets weiter einzuschränken, siehe [Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#).

Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen

Eine Sitzungsrichtlinie ist eine AWS Identity and Access Management (IAM) -Richtlinie, die Benutzer auf bestimmte Bereiche eines Amazon S3 S3-Buckets beschränkt. Dies geschieht durch Evaluierung des Zugriffs in Echtzeit.

Note

Sitzungsrichtlinien werden nur mit Amazon S3 verwendet. Für Amazon EFS verwenden Sie POSIX-Dateiberechtigungen, um den Zugriff einzuschränken.

Sie können eine Sitzungsrichtlinie verwenden, wenn Sie einer Benutzergruppe denselben Zugriff auf einen bestimmten Teil Ihres Amazon S3 S3-Buckets gewähren müssen. Eine Gruppe von Benutzern soll beispielsweise nur auf das `home`-Verzeichnis zugreifen können. Diese Benutzergruppe teilt sich dieselbe IAM-Rolle.

Note

Die maximale Länge einer Sitzungsrichtlinie beträgt 2048 Zeichen. Weitere Informationen finden Sie unter dem [Anforderungsparameter Policy](#) für die `CreateUser` Aktion in der API-Referenz.

Verwenden Sie die folgenden Richtlinienvariablen in Ihrer IAM-Richtlinie, um eine Sitzungsrichtlinie zu erstellen:

- `${transfer:HomeBucket}`

- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

Sie können die oben genannten Variablen nicht in verwalteten Richtlinien verwenden. Sie können sie auch nicht als Richtlinienvariablen in einer IAM-Rollendefinition verwenden. Sie erstellen diese Variablen in einer IAM-Richtlinie und geben sie direkt bei der Einrichtung Ihres Benutzers an. Außerdem können Sie die `${aws:Username}` Variable in dieser Sitzungsrichtlinie nicht verwenden. Diese Variable bezieht sich auf einen IAM-Benutzernamen und nicht auf den von AWS Transfer Family erforderlichen Benutzernamen.

Beispiel für eine Sitzungsrichtlinie

Der folgende Code zeigt ein Beispiel für eine Sitzungsrichtlinie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    }
  ],
}
```

```

{
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion",
    "s3:GetObjectACL",
    "s3:PutObjectACL"
  ],
  "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
}

```

Note

Im obigen Richtlinienbeispiel wird davon ausgegangen, dass die Basisverzeichnisse der Benutzer so eingestellt sind, dass sie einen abschließenden Schrägstrich enthalten, um anzuzeigen, dass es sich um ein Verzeichnis handelt. Wenn Sie dagegen das eines Benutzers `HomeDirectory` ohne den abschließenden Schrägstrich angeben, sollten Sie es in Ihre Richtlinie aufnehmen.

Beachten Sie in der vorherigen Beispielenrichtlinie die Verwendung der `transfer:HomeFolder` `transfer:HomeDirectory` Richtlinienparameter `transfer:HomeBucket`, und. Diese Parameter werden für den festgelegt `HomeDirectory`, der für den Benutzer konfiguriert ist, wie unter [HomeDirectory](#) und beschrieben [Implementierung Ihrer API-Gateway-Methode](#). Diese Parameter haben die folgenden Definitionen:

- Der `transfer:HomeBucket` Parameter wird durch die erste Komponente von `ersetztHomeDirectory`.
- Der `transfer:HomeFolder` Parameter wird durch die verbleibenden Teile des `HomeDirectory` Parameters ersetzt.

- Für den `transfer:HomeDirectory` Parameter wurde der führende Schrägstrich (/) entfernt, sodass er als Teil eines S3-Amazon-Ressourcennamens (ARN) in einer Resource Anweisung verwendet werden kann.

 Note

Wenn Sie logische Verzeichnisse verwenden, also die Verzeichnisse des `homeDirectoryType` Benutzers, werden LOGICAL diese Richtlinienparameter (`HomeBucketHomeDirectory`, und `HomeFolder`) nicht unterstützt.

Nehmen wir beispielsweise an, dass der `HomeDirectory` Parameter, der für den Transfer Family Family-Benutzer konfiguriert ist `/home/bob/amazon/stuff/`,

- ist `transfer:HomeBucket` auf `/home` gesetzt.
- ist `transfer:HomeFolder` auf `/bob/amazon/stuff/` gesetzt.
- `transfer:HomeDirectory` wird `home/bob/amazon/stuff/`.

Die erste "Sid" ermöglicht es dem Benutzer, alle Verzeichnisse aufzulisten, beginnend mit `/home/bob/amazon/stuff/`.

Die zweite "Sid" schränkt den get Zugriff des Benutzers put auf denselben Pfad ein, `/home/bob/amazon/stuff/`.

Wenn die oben genannte Richtlinie gilt, kann ein Benutzer, wenn er sich anmeldet, nur auf Objekte in seinem Home-Verzeichnis zugreifen. AWS Transfer Family Ersetzt diese Variablen beim Verbindungsaufbau durch die entsprechenden Werte für den Benutzer. Dies erleichtert die Verwendung von Richtliniendokumenten für mehrere Benutzer. Dieser Ansatz reduziert den Aufwand für die IAM-Rollen- und Richtlinienverwaltung für die Verwaltung des Zugriffs Ihrer Benutzer auf Ihren Amazon S3 S3-Bucket.

Sie können auch eine Sitzungsrichtlinie verwenden, um den Zugriff für jeden Ihrer Benutzer an Ihre Geschäftsanforderungen anzupassen. Weitere Informationen finden Sie unter [Berechtigungen für AssumeRole AssumeRoleWithSAML, und AssumeRoleWithWebIdentity](#) im IAM-Benutzerhandbuch.

 Note

AWS Transfer Family speichert den Richtlinien-JSON anstelle des Amazon-Ressourcennamens (ARN) der Richtlinie. Wenn Sie also die Richtlinie in der IAM-Konsole ändern, müssen Sie zur AWS Transfer Family Konsole zurückkehren und Ihre Benutzer über die neuesten Richtlinieninhalte informieren. Sie können den Benutzer auf der Registerkarte Richtlinieninformationen im Abschnitt Benutzerkonfiguration aktualisieren. Wenn Sie den verwenden AWS CLI, können Sie den folgenden Befehl verwenden, um die Richtlinie zu aktualisieren.

```
aws transfer update-user --server-id server --user-name user --policy \  
    "$(aws iam get-policy-version --policy-arn policy --version-id version --  
    output json)"
```

Verschachtelte Ersetzungen für Sitzungsrichtlinien

Verschachtelte Ersetzungen werden in den Sitzungsrichtlinien von Transfer Family nicht durchgeführt. Sitzungsrichtlinien können verschachtelte Variablen verwenden, wie z.

`${transfer:HomeDirectory}` Wenn die Richtlinie verarbeitet wird, kann die äußere Variable (z. B. `${transfer:HomeDirectory}`) durch einen Wert ersetzt werden, der eine andere Variable enthält (z. B. `{amzn-s3-demo-bucket:/${transfer:UserName}}`). Die verschachtelte Variable wird jedoch nicht weiter durch den tatsächlichen Benutzernamen (z. B. johndoe) ersetzt.

Das bedeutet, dass Sie bei der Erstellung von Sitzungsrichtlinien für Transfer Family dieses Verhalten berücksichtigen und sicherstellen müssen, dass die Richtlinienstruktur und die Variablennutzung entsprechend gestaltet sind. Die verschachtelten Variablen werden möglicherweise nicht wie erwartet aufgelöst, und die Richtlinie gewährt möglicherweise nicht die beabsichtigten Berechtigungen. Es ist wichtig, die Sitzungsrichtlinien gründlich zu testen und zu validieren, um sicherzustellen, dass sie wie erwartet funktionieren. Dieses Verhalten ist ein wichtiger Aspekt bei der Implementierung von Zugriffskontrolle und Berechtigungen für Ihre Transfer Family Family-Umgebung.

Eine Lösung für dieses Problem besteht darin, den tatsächlichen Amazon S3 S3-Bucket-Namen in Ihrer Sitzungsrichtlinie zu verwenden. Anstatt dies `${transfer:HomeDirectory}` in Ihrer Sitzungsrichtlinie anzugeben, verwenden Sie beispielsweise Folgendes, wobei `amzn-s3-demo-bucket` Ihr eigentlicher Bucket ist: `${amzn-s3-demo-bucket/transfer:UserName}`

Dynamische Ansätze zur Rechteverwaltung

Grundlegendes zur Berechtigungsarchitektur von Transfer Family

AWS Transfer Family unterstützt dynamisches Berechtigungsmanagement mithilfe von Sitzungsrichtlinien, mit denen Sie die effektiven Berechtigungen von IAM-Rollen zur Laufzeit einschränken können. Dieser Ansatz funktioniert sowohl für vom Service verwaltete Benutzer als auch für Benutzer von benutzerdefinierten Identitätsanbietern, wird jedoch nur unterstützt, wenn Dateien zu oder von Amazon S3 (nicht Amazon EFS) übertragen werden.

Jeder AWS Transfer Family Benutzer arbeitet mit einem Berechtigungsmodell, das aus folgenden Komponenten besteht:

1. IAM-Basisrolle — Definiert die grundlegenden Berechtigungen für den Benutzer
2. Optionale Sitzungsrichtlinie — Schränkt die Basisberechtigungen zur Laufzeit ein (mit eingeschränktem Geltungsbereich)

Die effektiven Berechtigungen sind die Schnittmenge der Basisrollenberechtigungen und der Sitzungsrichtlinienberechtigungen. Sitzungsrichtlinien können nur Berechtigungen einschränken; sie können keine zusätzlichen Berechtigungen gewähren, die über das hinausgehen, was die Basisrolle zulässt.

Diese Architektur gilt für beide Benutzertypen:

- Service-managed Benutzer — Sitzungsrichtlinien können direkt in den Benutzereinstellungen konfiguriert werden
- Benutzer mit benutzerdefiniertem Identitätsanbieter — Sitzungsrichtlinien können als Teil der Authentifizierungsantwort zurückgegeben oder in gespeichert werden AWS Secrets Manager

Zwei Ansätze für die Rechteverwaltung

Beim Entwerfen von Berechtigungen für Transfer Family Family-Benutzer, die spezielle Zugriffsmuster benötigen, können Sie zwischen zwei Hauptansätzen wählen:

Eine Rolle pro Benutzer

Erstellen Sie für jeden Transfer Family Family-Benutzer eine separate IAM-Rolle mit spezifischen Berechtigungen, die auf die Bedürfnisse dieses Benutzers zugeschnitten sind. Verwenden Sie diesen Ansatz, wenn:

- Jeder Benutzer benötigt sehr unterschiedliche Berechtigungen
- Die Verwaltung von Berechtigungen wird von verschiedenen Personen in Ihrer Organisation übernommen
- Sie benötigen eine detaillierte Kontrolle über den individuellen Benutzerzugriff

Gemeinsame Rolle mit Sitzungsrichtlinien

Verwenden Sie eine einzelne IAM-Rolle mit umfassenden Berechtigungen (z. B. Zugriff auf einen gesamten Amazon S3 S3-Bucket mit mehreren Benutzerstartverzeichnissen) und wenden Sie Sitzungsrichtlinien an, um jeden Benutzer auf seinen spezifischen Bereich zu beschränken. Dieser Ansatz reduziert den Verwaltungsaufwand im Vergleich zur Verwaltung separater Rollen für jeden Benutzer erheblich. Verwenden Sie diesen Ansatz, wenn:

- Benutzer benötigen ähnliche Zugriffsarten, jedoch auf unterschiedliche Ressourcen (z. B. benötigen alle Benutzer read/write Zugriff, aber jeder nur auf seinen eigenen Ordner)
- Sie möchten die Rollenverwaltung vereinfachen und vermeiden, Dutzende oder Hunderte von Einzelrollen zu erstellen
- Benutzer sollten nur innerhalb eines gemeinsam genutzten Buckets auf ihre zugewiesenen Home-Verzeichnisse zugreifen
- Die Rechteverwaltung ist innerhalb Ihrer Organisation zentralisiert

Anstatt beispielsweise separate Rollen für die Benutzer „Alice“, „Bob“ und „Charlie“ zu erstellen, können Sie eine Rolle mit Zugriff auf den gesamten `s3://company-transfers/` Bucket erstellen und dann mithilfe von Sitzungsrichtlinien den Zugriff auf Alice `s3://company-transfers/alice/s3://company-transfers/bob/`, Bob auf usw. einschränken.

Implementieren von Sitzungsrichtlinien

Sitzungsrichtlinien funktionieren, indem sie die effektiven Berechtigungen der einem Benutzer zugewiesenen IAM-Basisrolle einschränken. Die endgültigen Berechtigungen sind die Schnittmenge zwischen den Berechtigungen der Rolle und den Berechtigungen der Sitzungsrichtlinie.

Sie können dynamische Sitzungsrichtlinien auf zwei Arten implementieren:

Substitution durch Variablen

Verwenden Sie `${transfer:HomeBucket}` in Ihren Sitzungsrichtlinien Variablen für die Familienübertragungsrichtlinie wie `${transfer:Username}${transfer:HomeDirectory}`, und. Diese Variablen werden zur Laufzeit automatisch durch die tatsächlichen Werte ersetzt. Weitere Hinweise zu diesen Variablen finden Sie unter [Sitzungsrichtlinie für einen Amazon S3 S3-Bucket erstellen](#).

Dynamische Generierung

Generieren Sie für benutzerdefinierte Identitätsanbieter Sitzungsrichtlinien im laufenden Betrieb als Teil der Authentifizierungsantwort Ihrer Lambda-Funktion oder API-Gateway-Methode. Mit diesem Ansatz können Sie bei der Authentifizierung hochgradig maßgeschneiderte Richtlinien erstellen, die auf Benutzerattributen, Gruppenmitgliedschaften oder externen Datenquellen basieren.

Sie können auch vorgenerierte Sitzungsrichtlinien speichern, AWS Secrets Manager indem Sie einen Schlüssel `Policy` mit dem JSON-Wert für die Sitzungsrichtlinie angeben. Auf diese Weise können Sie dieselbe umfassende IAM-Rolle für mehrere Benutzer verwenden und gleichzeitig benutzerspezifische Zugriffskontrollen beibehalten.

Note

Sitzungsrichtlinien werden nur für Dateiübertragungen zu und von Amazon S3 unterstützt. Sie gelten nicht für Amazon EFS-Dateisysteme. Für Amazon EFS werden die Berechtigungen durch das Dateisystem selbst geregelt UID/GID und die Berechtigungsbits werden innerhalb des Dateisystems selbst angewendet.

Implementierung nach Benutzertyp

Service-managed Benutzer

Für vom Service verwaltete Benutzer können Sie Sitzungsrichtlinien direkt in der Benutzerkonfiguration über die AWS Transfer Family Konsole, API oder CLI angeben. Weitere Informationen finden Sie unter [Arbeiten mit Benutzern, die vom Dienst verwaltet werden](#).

Benutzer mit benutzerdefiniertem Identity Provider

Für Benutzer eines benutzerdefinierten Identitätsanbieters können Sie Sitzungsrichtlinien auf zwei Arten bereitstellen:

- AWS Secrets Manager Indem Sie einen Schlüssel angeben, der Policy zusammen mit der Sitzungsrichtlinie als Wert benannt ist
- Direkt in der Lambda-Funktionsantwort oder der API-Gateway-Antwort als Teil des Authentifizierungsergebnisses

Weitere Informationen finden Sie unter [Lösung für einen benutzerdefinierten Identitätsanbieter](#).

Beispiel: Vereinfachung der Rollenverwaltung mit Sitzungsrichtlinien

Dieses Beispiel zeigt, wie dynamisches Berechtigungsmanagement den Verwaltungsaufwand erheblich reduzieren und gleichzeitig die Sicherheit gewährleisten kann.

Szenario

Ihr Unternehmen hat 50 Benutzer, die SFTP-Zugriff benötigen, um Dateien zu übertragen. Jeder Benutzer sollte nur auf seinen eigenen Ordner innerhalb eines gemeinsam genutzten Amazon S3 S3-Buckets zugreifen, der aufgerufen wird `company-transfers`. Ohne Sitzungsrichtlinien müssten Sie 50 separate IAM-Rollen erstellen.

Herkömmlicher Ansatz (ohne Sitzungsrichtlinien)

- Erstellen Sie 50 IAM-Rollen: `TransferRole-Alice`, `TransferRole-Bob`, `TransferRole-Charlie`, usw.
- Jede Rolle hat spezifische Berechtigungen nur für den Ordner dieses Benutzers
- Die Verwaltung von Berechtigungen erfordert die Aktualisierung einzelner Rollen
- Das Hinzufügen neuer Benutzer erfordert die Erstellung neuer Rollen

Dynamischer Ansatz (mit Sitzungsrichtlinien)

- Erstellen Sie eine IAM-Rolle: `TransferRole-Shared` mit umfassenden Berechtigungen für den gesamten Bucket
- Verwenden Sie Sitzungsrichtlinien, um jeden Benutzer zur Laufzeit auf seinen spezifischen Ordner zu beschränken
- Die Verwaltung von Berechtigungen erfordert die Aktualisierung einer Rollen- oder Sitzungsrichtlinienvorlage

- Das Hinzufügen neuer Benutzer erfordert keine neuen Rollen, sondern lediglich eine Benutzerkonfiguration

Implementierung

So würden Sie den dynamischen Ansatz implementieren (indem Sie den `company-transfers` Bucket als Beispiel verwenden, der durch Ihren tatsächlichen Amazon S3 S3-Bucket ersetzt werden soll):

Um ein dynamisches Berechtigungsmanagement zu implementieren

1. Erstellen Sie eine gemeinsame IAM-Rolle mit umfassenden Amazon S3 S3-Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers"
    }
  ]
}
```

2. Erstellen Sie eine Sitzungsrichtlinienvorlage, die den Zugriff auf den Ordner des Benutzers einschränkt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
},
{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::company-transfers",
    "Condition": {
        "StringLike": {
            "s3:prefix": "${transfer:Username}*"
        }
    }
}
]
}

```

3. Konfigurieren Sie jeden Benutzer mit:

- Die gemeinsame IAM-Rolle
- Die Sitzungsrichtlinie wurde wie folgt angewendet:
 - Service-managed Benutzer: Verwenden Sie die API oder CLI, um den JSON über den Policy-Parameter anzuwenden, wenn Sie Benutzer erstellen oder ändern (die Konsole bietet nur vordefinierte Richtlinienoptionen)
 - Benutzer eines benutzerdefinierten Identitätsanbieters: Geben Sie ihn entweder als Teil der Antwort der Lambda-Funktion während der Authentifizierung zurück oder speichern Sie ihn AWS Secrets Manager als Schlüssel mit dem Namen „Policy“ zusammen mit den Anmeldeinformationen des Benutzers
- Heimatverzeichnis: /company-transfers/\${transfer:Username}/

AWS CloudTrail Protokollierung für AWS Transfer Family

AWS Transfer Family lässt sich sowohl mit Amazon als AWS CloudTrail auch mit Amazon integrieren CloudWatch. CloudTrail und CloudWatch dienen unterschiedlichen, aber sich ergänzenden Zwecken.

- In diesem Thema geht es um die Integration mit CloudTrail einem AWS Dienst, der eine Aufzeichnung der in Ihrem System ausgeführten Aktionen erstellt AWS-Konto. Es überwacht und zeichnet kontinuierlich API-Operationen für Aktivitäten wie Konsolenanmeldungen, AWS Command Line Interface Befehle und SDK/API Operationen auf. Auf diese Weise können Sie protokollieren, wer wann und von wo aus welche Maßnahmen ergriffen hat. CloudTrail hilft bei der Prüfung, beim Zugriffsmanagement und bei der Einhaltung gesetzlicher Vorschriften, indem es einen Verlauf aller Aktivitäten in Ihrer AWS Umgebung bereitstellt. Einzelheiten finden Sie im [AWS CloudTrail Benutzerhandbuch](#).
- [CloudWatch Amazon-Protokollierung für AWS Transfer Family Server](#) behandelt die Integration mit CloudWatch, einem Dienst zur Überwachung von AWS Ressourcen und Anwendungen. Es sammelt Metriken und Protokolle, um einen Überblick über die Ressourcennutzung, die Anwendungsleistung und den allgemeinen Systemzustand zu erhalten. CloudWatch hilft bei betrieblichen Aufgaben wie der Behebung von Problemen, der Einstellung von Alarmen und der automatischen Skalierung. Einzelheiten finden Sie im [CloudWatch Amazon-Benutzerhandbuch](#).

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Operationen, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Transfer Family, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle AWS Transfer Family Aktionen werden von protokolliert CloudTrail und sind in der dokumentiert [ActionsAPI reference](#). Beispielsweise generieren Aufrufe von `ListUsers` und `StopServer` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateServer`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Transfer Family. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Transfer Family, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Themen

- [Aktivieren Sie die AWS CloudTrail Protokollierung](#)
- [Beispiel für einen Protokolleintrag zum Erstellen eines Servers](#)
- [Beispiele für Datenzugriffsprotokolle](#)

Aktivieren Sie die AWS CloudTrail Protokollierung

Sie können AWS Transfer Family API-Operationen überwachen mit AWS CloudTrail. Durch die Überwachung von API-Vorgängen erhalten Sie nützliche Sicherheits- und Betriebsinformationen. Wenn Sie die [Protokollierung auf Objektebene von Amazon S3 aktiviert](#) haben, RoleSessionName ist im Feld Anforderer enthalten als [AWS:Role Unique Identifier]/username.sessionid@server-id. Weitere Informationen zu eindeutigen AWS Identity and Access Management (IAM-) Rollenbezeichnungen finden Sie unter [Eindeutige Identifikatoren im Benutzerhandbuch](#). AWS Identity and Access Management

Important

Die maximale Länge von beträgt 64 Zeichen RoleSessionName. Wenn der länger RoleSessionName ist, server-id wird der gekürzt.

Amazon S3 S3-Datenereignisse aktivieren

Um Dateioperationen nachzuverfolgen, die in Ihren AWS Transfer Family Amazon S3 S3-Buckets ausgeführt wurden, müssen Sie Datenereignisse für diese Buckets aktivieren. Datenereignisse ermöglichen API-Aktivitäten auf Objektebene und eignen sich besonders für die Nachverfolgung von Datei-Uploads, Downloads und anderen von Benutzern ausgeführten Vorgängen. AWS Transfer Family

So aktivieren Sie Amazon S3 S3-Datenereignisse für Ihren AWS Transfer Family Server:

1. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Trails aus und wählen Sie dann einen vorhandenen Trail aus, oder erstellen Sie einen neuen.
3. Wählen Sie unter Datenereignisse die Option Bearbeiten aus.
4. Wählen Sie als Datenereignistyp die Option S3 aus.
5. Wählen Sie die Amazon S3 S3-Buckets aus, für die Datenereignisse protokolliert werden sollen. Sie können Datenereignisse für alle Buckets protokollieren oder einzelne Buckets angeben.
6. Wählen Sie aus, ob Leseereignisse, Schreibereignisse oder beides protokolliert werden sollen.
7. Wählen Sie Änderungen speichern aus.

Nachdem Sie Datenereignisse aktiviert haben, können Sie auf diese Protokolle in dem für Ihren CloudTrail Trail konfigurierten Amazon S3 S3-Bucket zugreifen. Die Protokolle enthalten Details wie den Benutzer, der die Aktion ausgeführt hat, den Zeitstempel der Aktion, das betroffene Objekt und das `onBehalfOf` Feld, mit dessen Hilfe die vier durchgeführten Aktionen nachvollzogen werden können. `userId` AWS Transfer Family

Beispiel für einen Protokolleintrag zum Erstellen eines Servers

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag (im JSON-Format), der die `CreateServer` Aktion demonstriert.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHHH6NNWWW:user1",
    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "arn": "arn:aws:iam::123456789102:role/Admin",
        "accountId": "123456789102",
        "userName": "Admin"
      }
    }
  },
  "eventTime": "2024-02-05T19:18:53Z",
  "eventSource": "transfer.amazonaws.com",
  "eventName": "CreateServer",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "11.22.1.2",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36",
  "requestParameters": {
    "domain": "S3",

```

```

    "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "protocols": [
      "SFTP"
    ],
    "protocolDetails": {
      "passiveIp": "AUTO",
      "tlsSessionResumptionMode": "ENFORCED",
      "setStatOption": "DEFAULT"
    },
    "securityPolicyName": "TransferSecurityPolicy-2020-06",
    "s3StorageOptions": {
      "directoryListingOptimization": "ENABLED"
    }
  },
  "responseElements": {
    "serverId": "s-1234abcd5678efghi"
  },
  "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
  "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789102",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}

```

Beispiele für Datenzugriffsprotokolle

Wenn Sie Amazon S3 S3-Datenereignisse für Ihren CloudTrail Trail aktivieren, können Sie die ausgeführten Dateioperationen verfolgen AWS Transfer Family. Mithilfe dieser Protokolle können Sie überwachen, wer wann und wie auf welche Daten zugegriffen hat.

Beispiel für einen Protokolleintrag für einen erfolgreichen Datenzugriff

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für einen erfolgreichen Dateidownload-Vorgang durch AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
  }
}

```

```

    "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ="
  },
  "requestID": "EXAMPLE123456789",
  "eventID": "example12-3456-7890-abcd-ef1234567890",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS::S3::Object",
      "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-
report-2025-Q2.pdf"
    },
    {
      "accountId": "123456789012",
      "type": "AWS::S3::Bucket",
      "ARN": "arn:aws:s3:::my-transfer-bucket"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012",
  "eventCategory": "Data",
  "requestParameters": {
    "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
  }
}

```

Beachten Sie in diesem Beispiel die folgenden wichtigen Felder:

- `eventName`: Zeigt den S3-API-Vorgang an, der ausgeführt wurde (GetObject für einen Dateidownload).
- `requestParameters.bucketName` und `requestParameters.key`: Zeigt an, auf welches S3-Objekt zugegriffen wurde.
- `additionalEventData.bytesTransferredOut`: Zeigt die Größe der heruntergeladenen Datei in Byte an.
- `requestParameters.x-amz-onBehalfOf`: Enthält den AWS Transfer Family Benutzernamen und die Sitzungs-ID, sodass Sie nachvollziehen können, welcher AWS Transfer Family Benutzer die Aktion ausgeführt hat.

Das `x-amz-onBehalfOf` Feld ist besonders wichtig, da es den S3-API-Rückruf mit dem spezifischen AWS Transfer Family Benutzer verknüpft, der die Aktion initiiert hat. Dieses Feld folgt dem Format `username.sessionid@server-id`, wobei:

- `username` ist der AWS Transfer Family Nutzernamen.
- `sessionid` ist eine eindeutige Kennung für die Sitzung des Benutzers.
- `server-id` ist die ID des AWS Transfer Family Servers.

Allgemeine Datenzugriffsvorgänge

Bei der Überwachung des Datenzugriffs über AWS Transfer Family werden in Ihren CloudTrail Protokollen in der Regel die folgenden S3-API-Operationen angezeigt:

Allgemeine S3-Operationen in AWS Transfer Family Protokollen

S3-API-Be- trieb	AWS Transfer Family Aktion	Description
GetObject	Datei herunterladen	Der Benutzer hat eine Datei vom Server heruntergeladen
PutObject	Datei-Upload	Der Benutzer hat eine Datei auf den Server hochgeladen
DeleteObject	Löschen von Dateien	Der Benutzer hat eine Datei vom Server gelöscht
ListObje- cts oder ListObjects V2	Verzeichnisliste	Vom Benutzer aufgelistete Dateien in einem Verzeichnis
CopyObject	Datei kopieren	Der Benutzer hat eine Datei auf den Server kopiert

Durch die Überwachung dieser Vorgänge in Ihren CloudTrail Protokollen können Sie alle Dateiaktivitäten verfolgen, die über Ihren AWS Transfer Family Server ausgeführt werden. So können Sie Compliance-Anforderungen erfüllen und unbefugten Zugriff erkennen.

CloudWatch Amazon-Protokollierung für AWS Transfer Family Server

Amazon CloudWatch ist ein leistungsstarker Überwachungs- und Beobachtbarkeitsservice, der einen umfassenden Einblick in Ihre AWS Ressourcen bietet, darunter AWS Transfer Family:

- **Real-time Überwachung:** CloudWatch überwacht die Ressourcen und Anwendungen der Transfer Family in Echtzeit, sodass Sie deren Leistung verfolgen und analysieren können.
- **Erfassung von Kennzahlen:** CloudWatch sammelt und verfolgt verschiedene Kennzahlen für Ihre Ressourcen und Anwendungen. Dabei handelt es sich um Variablen, die Sie messen und für Analysen verwenden können.
- **CloudWatch Startseite:** Auf der CloudWatch Startseite werden automatisch Metriken zu Transfer Family und anderen von Ihnen verwendeten AWS Diensten angezeigt, sodass Sie Ihre Überwachungsdaten zentral einsehen können.
- **Benutzerdefinierte Dashboards:** Sie können benutzerdefinierte Dashboards erstellen, CloudWatch um Metriken anzuzeigen, die für Ihre benutzerdefinierten Anwendungen und die Ressourcen, die Sie überwachen möchten, spezifisch sind.
- **Alarme und Benachrichtigungen:** CloudWatch ermöglicht es Ihnen, Alarme zu erstellen, die Ihre Messwerte überwachen und Benachrichtigungen oder automatisierte Aktionen auslösen, wenn bestimmte Schwellenwerte überschritten werden. Dies kann nützlich sein, um die Dateiübertragungsaktivitäten auf Ihren Transfer Family Family-Servern zu überwachen und Ressourcen entsprechend zu skalieren.
- **Kostenoptimierung:** Sie können die von gesammelten Daten verwenden, CloudWatch um nicht ausgelastete Ressourcen zu identifizieren und Maßnahmen wie das Stoppen oder Löschen von Instanzen zu ergreifen, um Ihre Kosten zu optimieren.

Insgesamt ist es aufgrund der umfassenden Überwachungsfunktionen ein wertvolles Tool für die Verwaltung und Optimierung Ihrer Transfer Family Family-Infrastruktur und der darauf ausgeführten Anwendungen. CloudWatch

Einzelheiten zur CloudWatch Protokollierung für Transfer Family Family-Web-Apps finden Sie unter [CloudTrail Protokollierung für Transfer Family Family-Web-Apps](#).

Arten der CloudWatch Protokollierung für Transfer Family

Transfer Family bietet zwei Möglichkeiten, Ereignisse zu protokollieren CloudWatch:

- JSON-strukturierte Protokollierung
- Protokollierung über eine Protokollierungsrolle

Für Transfer Family Family-Server können Sie den Protokollierungsmechanismus wählen, den Sie bevorzugen. Für Konnektoren und Workflows werden nur Protokollierungsrollen unterstützt.

Strukturierte JSON-Protokollierung

Für die Protokollierung von Serverereignissen empfehlen wir die Verwendung der strukturierten JSON-Protokollierung. Dies bietet ein umfassenderes Protokollierungsformat, das das Abfragen von CloudWatch Protokollen ermöglicht. Für diese Art der Protokollierung muss die IAM-Richtlinie für den Benutzer, der den Server erstellt (oder die Protokollierungskonfiguration des Servers bearbeitet), die folgenden Berechtigungen enthalten:

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

Es folgt eine Beispielrichtlinie .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
```

```

        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
    ],
    "Resource": "*"
}
]
}

```

Einzelheiten zur Einrichtung der strukturierten JSON-Protokollierung finden Sie unter. [Protokollierung für Server erstellen, aktualisieren und anzeigen](#)

Rolle „Protokollierung“

Um Ereignisse für einen verwalteten Workflow, der an einen Server angehängt ist, sowie für Connectors zu protokollieren, müssen Sie eine Protokollierungsrolle angeben. Um den Zugriff festzulegen, erstellen Sie eine ressourcenbasierte IAM-Richtlinie und eine IAM-Rolle, die diese Zugriffsinformationen bereitstellt. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die Serverereignisse AWS-Konto protokollieren kann.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}

```

Einzelheiten zur Konfiguration einer Protokollierungsrolle zum Protokollieren von Workflow-Ereignissen finden Sie unter [Verwaltung der Protokollierung für Workflows](#).

Protokollierung für Server erstellen, aktualisieren und anzeigen

Für alle AWS Transfer Family Server bieten wir eine strukturierte Protokollierung an. Wir empfehlen, die strukturierte Protokollierung für alle neuen und vorhandenen Transfer Family Family-Server zu verwenden. Die Verwendung der strukturierten Protokollierung bietet unter anderem folgende Vorteile:

- Empfangen Sie Protokolle in einem strukturierten JSON-Format.
- Fragen Sie Ihre Logs mit Amazon CloudWatch Logs Insights ab, das automatisch Felder im JSON-Format erkennt.
- Durch die gemeinsame Nutzung von Protokollgruppen für mehrere AWS Transfer Family Ressourcen können Sie Protokollstreams von mehreren Servern zu einer einzigen Protokollgruppe zusammenfassen, was die Verwaltung Ihrer Überwachungskonfigurationen und Einstellungen zur Aufbewahrung von Protokollen erleichtert.
- Erstellen Sie aggregierte Metriken und Visualisierungen, die zu Dashboards hinzugefügt werden können. CloudWatch
- Verfolgen Sie Nutzungs- und Leistungsdaten, indem Sie Protokollgruppen verwenden, um konsolidierte Log-Metriken, Visualisierungen und Dashboards zu erstellen.

Um die Protokollierung für Workflows zu aktivieren, die an Server angeschlossen sind, müssen Sie eine Protokollierungsrolle verwenden.

Note

Wenn Sie eine Protokollierungsrolle hinzufügen, ist die Protokollierungsgruppe immer `/aws/transfer/your-serverID` gültig und kann nicht geändert werden. Das bedeutet, dass Sie, sofern Sie Ihre strukturierten Serverprotokolle nicht an dieselbe Gruppe senden, in zwei separaten Protokollgruppen protokollieren.

Wenn Sie wissen, dass Sie Ihrem Server einen Workflow zuordnen werden und daher eine Protokollierungsrolle hinzufügen müssen, können Sie die strukturierte Protokollierung so einrichten, dass sie in der Standardprotokollgruppe von protokolliert wird `/aws/transfer/your-serverID`.

Informationen zum Ändern Ihrer Logging-Gruppe finden Sie [StructuredLogDestinations](#) in der AWS Transfer Family API-Referenz.

Wenn Sie mit der Transfer Family Family-Konsole einen neuen Server erstellen, ist die Protokollierung standardmäßig aktiviert. Nachdem Sie den Server erstellt haben, können Sie den `UpdateServer` API-Vorgang verwenden, um Ihre Protokollierungskonfiguration zu ändern. Details hierzu finden Sie unter [StructuredLogDestinations](#).

Derzeit müssen Sie für Workflows eine Protokollierungsrolle angeben, wenn Sie die Protokollierung aktivieren möchten:

- Wenn Sie einen Workflow mit einem Server verknüpfen, indem Sie entweder den `UpdateServer` API-Vorgang `CreateServer` oder verwenden, erstellt das System nicht automatisch eine Protokollierungsrolle. Wenn Sie Ihre Workflow-Ereignisse protokollieren möchten, müssen Sie dem Server explizit eine Protokollierungsrolle zuweisen.
- Wenn Sie mit der Transfer Family Family-Konsole einen Server erstellen und einen Workflow anhängen, werden Protokolle an eine Protokollgruppe gesendet, deren Name die Server-ID enthält. Das Format ist `/aws/transfer/server-id` zum Beispiel `/aws/transfer/s-1111aaaa2222bbbb3`. Die Serverprotokolle können an dieselbe oder eine andere Protokollgruppe gesendet werden.

Überlegungen zur Protokollierung beim Erstellen und Bearbeiten von Servern in der Konsole

- Neue Server, die über die Konsole erstellt wurden, unterstützen nur die strukturierte JSON-Protokollierung, es sei denn, ein Workflow ist an den Server angehängt.
- Keine Protokollierung ist keine Option für neue Server, die Sie in der Konsole erstellen.
- Bestehende Server können die strukturierte JSON-Protokollierung jederzeit über die Konsole aktivieren.
- Durch die Aktivierung der strukturierten JSON-Protokollierung über die Konsole wird die bestehende Protokollierungsmethode deaktiviert, sodass Kunden nicht doppelt belastet werden. Die Ausnahme ist, wenn ein Workflow an den Server angehängt ist.
- Wenn Sie die strukturierte JSON-Protokollierung aktivieren, können Sie sie später nicht über die Konsole deaktivieren.
- Wenn Sie die strukturierte JSON-Protokollierung aktivieren, können Sie das Ziel der Protokollgruppe jederzeit über die Konsole ändern.

- Wenn Sie die strukturierte JSON-Protokollierung aktivieren, können Sie die Protokollierungsrolle nicht über die Konsole bearbeiten, wenn Sie beide Protokollierungstypen über die API aktiviert haben. Die Ausnahme ist, wenn an Ihren Server ein Workflow angehängt ist. Die Rolle „Protokollierung“ wird jedoch weiterhin unter Zusätzliche Details angezeigt.

Überlegungen zur Protokollierung beim Erstellen und Bearbeiten von Servern mithilfe der API oder des SDK

- Wenn Sie über die API einen neuen Server erstellen, können Sie eine oder beide Arten der Protokollierung konfigurieren oder keine Protokollierung auswählen.
- Für bestehende Server können Sie die strukturierte JSON-Protokollierung jederzeit aktivieren und deaktivieren.
- Sie können die Protokollgruppe jederzeit über die API ändern.
- Sie können die Protokollierungsrolle jederzeit über die API ändern.

Um die strukturierte Protokollierung zu aktivieren, müssen Sie bei einem Konto mit den folgenden Berechtigungen angemeldet sein

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

Eine Beispielrichtlinie ist im Abschnitt verfügbar [Konfigurieren Sie die CloudWatch Protokollierungsrolle](#).

Themen

- [Protokollierung für Server erstellen](#)
- [Die Protokollierung für einen Server aktualisieren](#)

- [Serverkonfiguration anzeigen](#)

Protokollierung für Server erstellen

Wenn Sie einen neuen Server erstellen, können Sie auf der Seite **Zusätzliche Details konfigurieren** eine vorhandene Protokollgruppe angeben oder eine neue erstellen.

The screenshot shows the 'Configure additional details' page in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and has a 'Logging' section. Under 'Logging', there is a 'Log group' section with the instruction 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. It offers two options: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below these is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Logging role' section below it says 'Choose the IAM role that will be used to deliver events to your CloudWatch logs' and offers 'Create a new role' (unselected) and 'Choose an existing role' (unselected). A blue information box at the bottom states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Wenn Sie „Protokollgruppe erstellen“ wählen, wird in der CloudWatch Konsole (<https://console.aws.amazon.com/cloudwatch/>) die Seite „Protokollgruppe erstellen“ geöffnet. Einzelheiten finden Sie unter [Protokollgruppe erstellen in CloudWatch Logs](#).

Die Protokollierung für einen Server aktualisieren

Die Einzelheiten der Protokollierung hängen vom Szenario für Ihr Update ab.

Note

Wenn Sie sich für die strukturierte JSON-Protokollierung entscheiden, kann es in seltenen Fällen zu Verzögerungen kommen, bei denen Transfer Family die Protokollierung im alten Format beendet, es jedoch einige Zeit dauert, bis die Protokollierung im neuen JSON-Format gestartet wird. Dies kann dazu führen, dass Ereignisse nicht protokolliert werden. Es wird keine Dienstunterbrechungen geben, aber Sie sollten vorsichtig sein, wenn Sie Dateien in der

ersten Stunde nach der Änderung Ihrer Protokollierungsmethode übertragen, da Protokolle gelöscht werden könnten.

Wenn Sie einen vorhandenen Server bearbeiten, hängen Ihre Optionen vom Status des Servers ab.

- Auf dem Server ist bereits eine Protokollierungsrolle aktiviert, aber die strukturierte JSON-Protokollierung ist nicht aktiviert.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

i Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



i Workflows events will be delivered to a log group labelled with the server ID.

- Auf dem Server ist keine Protokollierung aktiviert.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- Auf dem Server ist die strukturierte JSON-Protokollierung bereits aktiviert, es wurde jedoch keine Protokollierungsrolle angegeben.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/ ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- Auf dem Server ist die strukturierte JSON-Protokollierung bereits aktiviert, und es wurde auch eine Protokollierungsrolle angegeben.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

 Workflows events will be delivered to a log group labelled with the server ID.

Serverkonfiguration anzeigen

Die Details für die Serverkonfigurationsseite hängen von Ihrem Szenario ab:

Je nach Szenario könnte die Serverkonfigurationsseite wie eines der folgenden Beispiele aussehen:

- Es ist keine Protokollierung aktiviert.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- Die strukturierte JSON-Protokollierung ist aktiviert.

Additional details
Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- Die Protokollierungsrolle ist aktiviert, aber die strukturierte JSON-Protokollierung ist nicht aktiviert.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted] execution-role [redacted]	Passive IP -

- Beide Arten der Protokollierung (Protokollierungsrolle und strukturierte JSON-Protokollierung) sind aktiviert.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Verwaltung der Protokollierung für Workflows

CloudWatch bietet eine konsolidierte Prüfung und Protokollierung des Fortschritts und der Ergebnisse von Workflows. Darüber hinaus AWS Transfer Family bietet es mehrere Metriken für Workflows. Sie können Messwerte darüber anzeigen, wie viele Workflow-Ausführungen in der letzten Minute gestartet, erfolgreich abgeschlossen und fehlgeschlagen sind. Alle CloudWatch Metriken für Transfer Family werden unter beschrieben [Verwenden von CloudWatch Metriken für Transfer Family Family-Server](#).

CloudWatch Amazon-Protokolle für Workflows anzeigen

1. Öffnen Sie die CloudWatch Amazon-Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im linken Navigationsbereich Logs und anschließend Log-Gruppen aus.
3. Wählen Sie auf der Seite Protokollgruppen in der Navigationsleiste die richtige Region für Ihren AWS Transfer Family Server aus.
4. Wählen Sie die Protokollgruppe aus, die Ihrem Server entspricht.

Wenn Ihre Server-ID beispielsweise lautet `-1234567890abcdef0`, ist Ihre Protokollgruppe `/aws/transfer/s-1234567890abcdef0`.

5. Auf der Seite mit den Protokollgruppendetails für Ihren Server werden die neuesten Protokollstreams angezeigt. Es gibt zwei Protokollstreams für den Benutzer, den Sie untersuchen:

- Einer für jede Secure Shell (SSH) File Transfer Protocol (SFTP) -Sitzung.
- Eine für den Workflow, der für Ihren Server ausgeführt wird. Das Format für den Protokollstream für den Workflow ist `username.workflowID.uniqueStreamSuffix`.

Wenn Ihr Benutzer beispielsweise `mary-major`, haben Sie die folgenden Protokollstreams:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

Die in diesem Beispiel aufgeführten 16-stelligen alphanumerischen Identifikatoren sind fiktiv. Die Werte, die Sie bei Amazon sehen, CloudWatch sind unterschiedlich.

Auf der Seite Ereignisse protokollieren für `mary-major-usa-east.1234567890abcdef0` werden die Details für jede Benutzersitzung angezeigt, und der `mary.w-abcdef01234567890.021345abcdef6789` Protokollstream enthält die Details für den Workflow.

Im Folgenden finden Sie ein Beispiel für einen Protokollstream für `mary.w-abcdef01234567890.021345abcdef6789`, der auf einem Workflow (`w-abcdef01234567890`) basiert, der einen Kopierschritt enthält.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
},
```

```

    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepStarted",
    "details": {
      "input": {
        "fileLocation": {
          "backingStore": "S3",
          "bucket": "amzn-s3-demo-bucket",
          "key": "mary/workflowSteps2.json",
          "versionId": "version-id",
          "etag": "etag-id"
        }
      },
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepCompleted",
    "details": {
      "output": {},
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  }
}

```

```

    }
  },
  {
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  }
}

```

Konfigurieren Sie die CloudWatch Protokollierungsrolle

Um den Zugriff festzulegen, erstellen Sie eine ressourcenbasierte IAM-Richtlinie und eine IAM-Rolle, die diese Zugriffsinformationen bereitstellt.

Um die CloudWatch Amazon-Protokollierung zu aktivieren, erstellen Sie zunächst eine IAM-Richtlinie, die die CloudWatch Protokollierung aktiviert. Anschließend erstellen Sie eine IAM-Rolle und fügen ihr die Richtlinie hinzu. Sie können dies tun, wenn Sie [einen Server erstellen](#) oder indem Sie [einen vorhandenen Server bearbeiten](#). Weitere Informationen zu CloudWatch finden Sie unter [Was ist Amazon CloudWatch?](#) und [Was ist Amazon CloudWatch Logs?](#) im CloudWatch Amazon-Benutzerhandbuch.

Verwenden Sie die folgenden IAM-Beispielrichtlinien, um die CloudWatch Protokollierung zu ermöglichen.

Use a logging role

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
  }
]
}

```

Use structured logging

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}

```

In der vorherigen Beispielrichtlinie ersetzen Sie für **Resource** die das *region-id* und *AWS-Konto* durch Ihre Werte. Beispiel: **"Resource": "arn:aws::logs:us-east-1:11112223333:log-group:/aws/transfer/*"**

Anschließend erstellen Sie eine Rolle und fügen die CloudWatch Logs-Richtlinie hinzu, die Sie erstellt haben.

So erstellen Sie eine IAM-Rolle und fügen dieser eine Richtlinie an

1. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.

Vergewissern Sie sich, dass auf der Seite Rolle erstellen der AWS Dienst ausgewählt ist.

2. Wählen Sie in der Service-Liste Transfer (Übertragung) und dann Next: Permissions (Weiter: Berechtigungen) aus. Dadurch wird eine Vertrauensbeziehung zwischen AWS Transfer Family und der IAM-Rolle hergestellt. Fügen Sie außerdem Schlüssel hinzu `aws:SourceAccount` und geben Sie `aws:SourceArn` ihnen Bedingungen, um sich vor dem Problem mit dem verwirrten Stellvertreter zu schützen. Weitere Informationen finden Sie in der folgenden Dokumentation:
 - Verfahren zum Aufbau einer Vertrauensbeziehung mit AWS Transfer Family: [So stellen Sie eine Vertrauensbeziehung her](#)
 - Beschreibung des Problems mit dem verwirrten Stellvertreter: das Problem [des verwirrten Stellvertreters](#)
3. Suchen Sie im Abschnitt Zugriffsrichtlinien anhängen nach der CloudWatch Protokollrichtlinie, die Sie gerade erstellt haben, wählen Sie sie aus und klicken Sie dann auf Weiter: Tags.
4. (Optional) Geben Sie einen Schlüssel und einen Wert für ein Tag ein und wählen Sie Next: Review (Weiter: Prüfen) aus.
5. Geben Sie auf der Seite Review (Prüfen) einen Namen und eine Beschreibung für die neue Rolle ein und wählen Sie dann Create role (Rolle erstellen) aus.
6. Um die Protokolle anzuzeigen, wählen Sie die Server-ID aus, um die Serverkonfigurationsseite zu öffnen, und wählen Sie Protokolle anzeigen. Sie werden zur CloudWatch Konsole weitergeleitet, wo Sie Ihre Log-Streams sehen können.

Auf der CloudWatch Seite für Ihren Server finden Sie Aufzeichnungen zur Benutzerauthentifizierung (Erfolg und Misserfolg), zu Datenuploads (PUTOperationen) und zu Datendownloads (GETOperationen).

Protokollstreams von Transfer Family anzeigen

So zeigen Sie Ihre Transfer Family Family-Serverprotokolle an

1. Navigieren Sie zur Detailseite eines Servers.
2. Wählen Sie Protokolle anzeigen aus. Dadurch wird Amazon geöffnet CloudWatch.
3. Die Protokollgruppe für den ausgewählten Server wird angezeigt.

CloudWatch ×

CloudWatch > Log groups > /aws/transfer/s-

/aws/transfer/s- Actions View in Logs Insights Search log group

Log group details

ARN arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-:*	Metric filters 0 Subscription filters 0 Contributor Insights rules -	Data protection - new Inactive Sensitive data found - new - KMS key ID -

Creation time
2 years ago

Retention
Never expire

Stored bytes
39.39 MB

Log streams Metric filters Subscription filters Contributor Insights Tags Data protection - new

Log streams (10) [Refresh] [Delete] [Create log stream] [Search all log streams]

Filter log streams or try prefix search ☐ Exact match ☐ Show expired Info < 1 > [Settings]

☐ Log stream	Last event
☐ ERRORS	2023-
☐ scooterstack4-	2023-
☐ scooterstack4-	2023-
☐ scooterstack4-	2023-

4. Sie können einen Protokollstream auswählen, um Details und einzelne Einträge für den Stream anzuzeigen.
 - Wenn es eine Liste für FEHLER gibt, können Sie diese auswählen, um Details zu den neuesten Fehlern auf dem Server anzuzeigen.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear

1m

30m

1h

12h

Custom

📅

Display ▾

⚙️

▶	Timestamp	Message	
There are older events to load. Load more.			
▶	2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
▼	2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
		ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=	Copy
▼	2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▼	2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▶	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Wählen Sie einen anderen Eintrag, um einen Beispiel-Logstream zu sehen.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear

1m

30m

1h

12h

Custom

📅

Display ▾

⚙️

▶	Timestamp	Message	
No older events at this moment. Retry			
▼	2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=	Copy
▼	2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED	Copy
No newer events at this moment. Auto retry paused. Resume			

Protokollstreams von Transfer Family anzeigen

623

- Wenn Ihrem Server ein verwalteter Workflow zugeordnet ist, können Sie die Protokolle der Workflow-Ausführungen anzeigen.

Note

Das Format für den Protokollstream für den Workflow ist `username.workflowId.uniqueStreamSuffix`. Beispielsweise könnte `decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` der Name eines Protokollstreams für Benutzer und Workflow sein. **decrypt-user w-a1111222233334444**

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
2023-03-21T13:37:57.795-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:02.850-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": {}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-

Note

Für jeden erweiterten Protokolleintrag können Sie den Eintrag in die Zwischenablage kopieren, indem Sie Kopieren wählen. Weitere Informationen zu CloudWatch Protokollen finden Sie unter [Protokolldaten anzeigen](#).

CloudWatch Amazon-Alarme erstellen

Das folgende Beispiel zeigt, wie CloudWatch Amazon-Alarme mithilfe der AWS Transfer Family Metrik erstellt FilesIn werden.

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Protokollierung Amazon S3 S3-API-Vorgängen in S3-Zugriffsprotokollen

Note

Dieser Abschnitt gilt nicht für Transfer Family Family-Web-Apps.

Wenn Sie [Amazon S3 S3-Zugriffsprotokolle verwenden, um S3-Anfragen zu identifizieren](#), die im Namen Ihrer Dateiübertragungsbenutzer gestellt wurden, `RoleSessionName` wird verwendet, um anzuzeigen, welche IAM-Rolle für die Bearbeitung der Dateiübertragungen übernommen wurde. Außerdem werden zusätzliche Informationen wie der Benutzername, die Sitzungs-ID und die Server-ID angezeigt, die für die Übertragungen verwendet wurden. Das Format ist `[AWS:Role Unique Identifier]/username.sessionid@server-id` und ist im Feld `Requester` enthalten. Im Folgenden finden Sie beispielsweise den Inhalt eines Beispielfeldes „Requester“ aus einem S3-Zugriffsprotokoll für eine Datei, die in den S3-Bucket kopiert wurde.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

Im obigen Feld `Requester` wird die aufgerufene IAM-Rolle angezeigt. `IamRoleName` Weitere Informationen zu den eindeutigen Identifikatoren der IAM-Rolle finden Sie unter [Eindeutige Identifikatoren](#) im Benutzerhandbuch.AWS Identity and Access Management

Beispiele zur Begrenzung des Problems mit verwirrtem Stellvertreter

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiere Entität zur Durchführung der Aktion zwingen kann. In AWS Fällen kann ein dienststellenübergreifender Identitätswechsel zum Problem des verwirrten Stellvertreters führen. Weitere Details finden Sie unter [Cross-service verwirrter Stellvertreter, Prävention](#).

Note

Ersetzen Sie in den folgenden Beispielen jedes durch Ihre *user input placeholder* eigenen Informationen.

In diesen Beispielen können Sie die ARN-Details für einen Workflow entfernen, wenn an Ihren Server keine Workflows angehängt sind.

Die folgende logging/invoke Beispielformatze ermöglicht es jedem Server (und Workflow) im Konto, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

Die folgende logging/invoke Beispielformatze ermöglicht es einem bestimmten Server (und Workflow), die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AllowSpecificServerWithWorkflowAttached",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"
        ]
      }
    }
  }
}

```

CloudWatch Protokollstruktur für Transfer Family

In diesem Thema werden die Felder beschrieben, die in Transfer Family Family-Protokollen aufgefüllt werden: sowohl für strukturierte JSON-Protokolleinträge als auch für ältere Protokolleinträge.

Themen

- [Strukturierte JSON-Logs für Transfer Family](#)
- [Legacy-Protokolle für Transfer Family](#)

Strukturierte JSON-Logs für Transfer Family

Die folgende Tabelle enthält Details zu Protokolleintragsfeldern für Transfer Family SFTP/FTP/FTPS Family-Aktionen im neuen strukturierten JSON-Protokollformat.

Feld	Description	Beispieleintrag
Aktivitätstyp	Die Aktion des Benutzers	Die verfügbaren Aktivitätstypen lauten wie folgt: AUTH_FAILURE CONNECTED ,DISCONNECTED ,ERROR,EXIT_REASON ,CLOSE,CREATE_SYMLINK ,DELETE,MKDIR,OPEN,PARTIALLOSE ,RENAME,RMDIR,SETSTAT,TLS_E_FAILURE .
eingebundene Bytes	Anzahl der vom Benutzer hochgeladenen Byte	29238420042
Byte raus	Anzahl der vom Benutzer heruntergeladenen Byte	23094032490328
ciphers	Gibt die für die Verbindung ausgehandelte SSH-Chiffre an (die verfügbaren Verschlüsselungen sind unter aufgeführt) Kryptografische Algorithmen	aes256-gcm@openssh.com
Client	Die Client-Software des Benutzers	SSH-2.0-OpenSSH_7.4
Home-Verzeichnis	Das Verzeichnis, in dem der Endbenutzer landet, wenn er eine Verbindung zum Endpunkt herstellt, wenn sein Home-Verzeichnistyp wie PATH folgt lautet: Wenn er ein logisches Home-Verzeichnis hat, ist dieser Wert immer /	/user-home- bucket/test
kex	Gibt den ausgehandelten SSH-Schlüsselaustausch	diffie-hellman-group14-sha256

Feld	Description	Beispieleintrag
	(KEX) für die Verbindung an (die verfügbaren KEX sind unter aufgeführt) Kryptogra- fische Algorithmen	
Nachricht	Stellt weitere Informationen zu dem Fehler bereit	<i><string></i>
Methode	Die Authentifizierungsmethode	publickey
mode	Gibt an, wie ein Client eine Datei öffnet	ERSTELLEN KÜRZEN SCHREIBEN
operation	Die Client-Operation für eine Datei	ÖFFNEN SCHLIESSEN
Pfad	Der tatsächliche Dateipfad ist betroffen	bucket/test/amzn-s3-demo- - file-1.pdf
Öffentlicher ssh-Schlüssel	Der öffentliche Schlüssel für den Benutzer, der eine Verbindung herstellt	AAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl

Feld	Description	Beispieleintrag
ssh-public-key-fingerabdruck	Der Fingerabdruck des öffentlichen Schlüssels, wie er in der Konsole für vom Service verwaltete Benutzer angezeigt wird, wenn sie ihre Benutzerschlüssel auflisten.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0
 Note In der Konsole wird der Fingerabdruck mit den Füllzeichen (falls vorhanden) angezeigt: 0 bis 3 Gleichheitszeichen (=) am Ende. Im Protokolleintrag wird diese Polsterung aus der Ausgabe entfernt.		
Typ des öffentlichen ssh-Schlüssels	Art des öffentlichen Schlüssels: Transfer Family unterstützt RSA-, ECDSA- und Schlüssel ED25519-formatted	ssh-ed25519
Ressource-ARN	Ein vom System zugewiesener, eindeutiger Bezeichner für eine bestimmte Ressource (z. B. einen Server)	arn:aws:transfer:ap-northeast-1:12346789012:-1234567890akeu2js2 server/s
role	Die IAM-Rolle des Benutzers	arn:aws:iam: :0293883675: -role role/testuser

Feld	Description	Beispieleintrag
Sitzungs-ID	Ein vom System zugewiesener, eindeutiger Bezeichner für eine einzelne Sitzung	9ca9a0e1cec6ad9d
Quell-IP	Client-IP-Adresse	18.323.0.129
user	Der Nutzernamen des Endbenutzers	mein Name 192
Benutzerrichtlinie	Die für den Endbenutzer angegebenen Berechtigungen: Dieses Feld wird ausgefüllt, wenn es sich bei der Benutzerrichtlinie um eine Sitzungsrichtlinie handelt.	Der JSON-Code für die Sitzungsrichtlinie, die verwendet wird

Legacy-Protokolle für Transfer Family

Die folgende Tabelle enthält Details zu Protokolleinträgen für verschiedene Transfer-Family-Aktionen.

Note

Diese Einträge liegen nicht im neuen strukturierten JSON-Protokollformat vor.

Die folgende Tabelle enthält Details zu Protokolleinträgen für verschiedene Transfer Family Family-Aktionen im neuen strukturierten JSON-Protokollformat.

Action	Entsprechende Protokolle in Amazon CloudWatch Logs
Authentication failures (Authentifizierungsfehler)	FEHLER AUTH_FAILURE METHOD=PublicKey user=LHR MESSAGE="RSA +b7 +A+HxG0C7L1JIZ0" sourceIP=3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE

Action	Entsprechende Protokolle in Amazon CloudWatch Logs
COPY/TAG/DELETE/DECRYPT Arbeitsablauf	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/lhr/regex.py" }, "stepType": "TAG", "stepName": "successful_tag_step", "workflowId": "w-1111a-aaa2222bbbb3", "Ausführungs-ID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-1234abcd5678efghi", "username": "lhr", "sessionId": "1234567890abcdef0" } } } }</pre>
Arbeitsablauf für benutzerdefinierte Schritte	<pre>{ "type": "CustomStepInvoked", "details": { "output": { "token": "" }, "stepType": "BENUTZERDEFINIERT", "stepName": "efs-s3_copy_2", "workflowId": "MzM4Mjg5YWUtYTEzMy00YjIzLWI3OGMtYzU4OGI2ZjQyMzE5", "Ausführungs-ID": "w-9283e49d33297c3f7", "Ausführungs-ID": "1234abcd-1234-efgh-5678-ijklmno7pq90", "transferDetails": { "serverId": "s-zzzz111aaaa22223", "username": "lhr", "sessionId": "1234567890abcdef0" } } }</pre>
Löschvorgänge	<pre>lhr.33a8fb495ffb383b LÖSCHEN Pfad=/bucket/user /123.jpg</pre>
Downloads	<pre>lhr.33a8fb495ffb383b PFAD=/ /123.jpg MODE=LESEN bucket/user lhr.33a8fb495ffb383b SCHLIESSEN Pfad=/ /123.jpg =3618546 bucket/user BytesOut</pre>

Action	Entsprechende Protokolle in Amazon CloudWatch Logs
Logins/Logouts	user.914984e553bcddb6 VERBUNDEN sourceIP=1.22.111.222 user=LHR =LOGICAL Client= _7.4 role=arn:aws: :iam: :12345678 9012: -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcddb6 ABGEBROCHEN
Benennt um	lhr.33a8fb495ffb383b UMBENENNEN Pfad=/ / lambo.png =/ /ferrari.png bucket/user NewPath bucket/user
Beispiel für ein Workflow-Fehlerprotokoll	<pre>{ "type": "StepErrored", "details": { "errorType": "BAD_REQUEST", "errorMessage": "EFS-Datei kann nicht taggt werden", "stepType": "TAG", "stepName": "successful_tag_step", "workflowId": "w-1234abcd5678efghi", "executionId": "81234abcd-1234-efghi", "executionId": "81234abcd-1234-efghi-gh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-1234abcd5678efghi", "username": "lhr", "sessionId": "1234567890abcdef0" } } }</pre>
Symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs- /pqr.jpg =abc.jpg LinkPath 12345678/lhr TargetPath
Uploads	lhr.33a8fb495ffb383b ÖFFNEN Path=/ /123.jpg mode=ERSTELLEN Kürzen Schreiben bucket/ user lhr.33a8fb495ffb383b SCHLIESSEN Pfad=/ /123.jpg =3618546 bucket/user BytesIn

Action	Entsprechende Protokolle in Amazon CloudWatch Logs
Arbeitsabläufe	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initial FileLocation": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/lhr/regex.py" }, "workflowId": "w-1111aaaa2222bbbb3", "Ausführungs-ID": "1234abcd-1234-efghbb3", "Ausführungs-ID": "1234abcd-1234-efghgh3-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-zzzz1111aaaa22223", "username": "lhr", "sessionId": "1234567890abcdef0" } } } }</pre> <pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/lhr/regex.py" }, "stepType": "BENUTZERDEFINIERT", "stepName": "efs-s3_copy_2", "workflowID": "w-9283e49d33297c3f7", "Ausführungs-ID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-18ca49dce5d842e0b", "username": "lhr", "sessionId": "1234567890abcdef0" } } } }</pre>

Beispiel für CloudWatch Protokolleinträge

In diesem Thema werden Beispielprotokolleinträge vorgestellt.

Themen

- [Beispiele für Protokolleinträge für Übertragungssitzungen](#)
- [Beispielprotokolleinträge für SFTP-Konnektoren](#)
- [Beispielprotokolleinträge für VPC-Lattice-Konnektoren](#)
- [Beispiel für Protokolleinträge für Fehler beim Schlüsselaustausch-Algorithmus](#)

Beispiele für Protokolleinträge für Übertragungssitzungen

In diesem Beispiel stellt ein SFTP-Benutzer eine Verbindung zu einem Transfer Family Family-Server her, lädt eine Datei hoch und trennt dann die Verbindung zur Sitzung.

Der folgende Protokolleintrag spiegelt einen SFTP-Benutzer wider, der eine Verbindung zu einem Transfer Family Family-Server herstellt.

```
{
  "role": "arn:aws:iam::500655546075:role/transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/s-3fe215d89f074ed2a",
  "home-dir": "/test/log-me",
  "ssh-public-key":
    "AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrqpDY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Der folgende Protokolleintrag spiegelt den SFTP-Benutzer wider, der eine Datei in seinen Amazon S3 S3-Bucket hochlädt.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Die folgenden Protokolleinträge geben an, dass der SFTP-Benutzer die Verbindung zu seiner SFTP-Sitzung beendet hat. Zuerst schließt der Client die Verbindung zum Bucket und dann trennt der Client die SFTP-Sitzung.

```
{
  "path": "/test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "bytes-in": "121",
  "session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Note

Die verfügbaren Aktivitätstypen lauten wie folgt:

AUTH_FAILURE, RECONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK, DELETE, RENAMERMDIR, SETSTAT, TLS_RESUME_FAILURE

Beispielprotokolleinträge für SFTP-Konnektoren

Dieser Abschnitt enthält Beispielprotokolle für eine erfolgreiche und eine erfolglose Übertragung. Protokolle werden in einer Protokollgruppe mit dem Namen generiert/aws/transfer/*connector-id*, wobei *connector-id* sich die Kennung für Ihren SFTP-Connector befindet. Protokolleinträge für SFTP-Konnektoren werden generiert, wenn Sie entweder den Befehl `StartFileTransfer` Oder `StartDirectoryListing` ausführen.

Dieser Protokolleintrag bezieht sich auf eine Übertragung, die erfolgreich abgeschlossen wurde.

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T16:33:27.373720Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
```



```

"file-path": "/remotebucket/remotefilepath",
"status-code": "COMPLETED",
"start-time": "2023-10-25T16:33:26.945481Z",
"end-time": "2023-10-25T16:33:27.159823Z",
"account-id": "480351544584",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"local-directory-path": "/connectors-localbucket",
"bytes": 514,
"egress-type": "SERVICE_MANAGED"
}

```

Dieser Protokolleintrag bezieht sich auf eine Übertragung, bei der das Zeitlimit überschritten wurde und die daher nicht erfolgreich abgeschlossen wurde.

```

{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T22:33:47.625703Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "FAILED",
  "failure-code": "TIMEOUT_ERROR",
  "failure-message": "Transfer request timeout.",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

Dieser Protokolleintrag bezieht sich auf einen erfolgreichen SEND-Vorgang.

```

{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
  "status-code": "COMPLETED",
}

```

```

    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

Beschreibungen einiger Schlüsselfelder in den vorherigen Protokollbeispielen.

- `timestamp` gibt an, wann das Protokoll hinzugefügt wird CloudWatch. `start-time` und `end-time` entsprechen dem Zeitpunkt, zu dem der Konnektor eine Übertragung tatsächlich startet und beendet.
- `transfer-id` ist ein eindeutiger Bezeichner, der jeder `start-file-transfer` Anfrage zugewiesen wird. Wenn der Benutzer in einem einzigen `start-file-transfer` API-Vorgang mehrere Dateipfade übergibt, teilen sich alle Dateien dasselbe `transfer-id`.
- `file-transfer-id` ist ein eindeutiger Wert, der für jede übertragene Datei generiert wird. Beachten Sie, dass der erste Teil von `file-transfer-id` derselbe `transfer-id` ist wie `transfer-id`.

Beispielprotokolleinträge für VPC-Lattice-Konnektoren

Dieser Abschnitt enthält Beispielprotokolle für VPC-Lattice-Konnektoren. Für VPC-Lattice-Konnektoren enthalten die Protokolle zusätzliche Felder, die Informationen zur Connectorconfiguration und zur Netzwerkeinrichtung enthalten.

Dieser Protokolleintrag bezieht sich auf einen SEND-Vorgang für einen VPC-Lattice-Connector, der erfolgreich abgeschlossen wurde.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",
  "start-time": "2025-09-05T14:20:19.434072509Z",
  "end-time": "2025-09-05T14:20:19.481453346Z",
  "account-id": "account-id",

```

```

"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/test-bucket/test-folder/",
"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id",
"vpc-lattice-port-number": 22
}

```

Die Protokolle des VPC-Lattice-Connectors enthalten die folgenden zusätzlichen Felder:

- `egress-type`- Art der Ausgangskonfiguration für den Connector
- `vpc-lattice-resource-configuration-arn`- ARN der VPC-Lattice-Ressourcenkonfiguration, die den Ziel-SFTP-Serverstandort definiert
- `vpc-lattice-port-number`- Portnummer für die Verbindung zum SFTP-Server über VPC Lattice

Beispiel für Protokolleinträge für Fehler beim Schlüsselaustausch-Algorithmus

Dieser Abschnitt enthält Beispielprotokolle, bei denen der Schlüsselaustauschalgorithmus (KEX) fehlgeschlagen ist. Dies sind Beispiele aus dem ERRORS-Protokollstream für strukturierte Protokolle.

Dieser Protokolleintrag ist ein Beispiel für einen Fehler beim Typ des Hostschlüssels.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-999999999999999999",
  "message": "no matching host key type found",
  "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}

```

Dieser Protokolleintrag ist ein Beispiel für eine KEX-Diskrepanz.

```

{
  "activity-type": "KEX_FAILURE",

```

```

"source-ip": "999.999.999.999",
"resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
"message": "no matching key exchange method found",
"kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}

```

Verwenden von CloudWatch Metriken für Transfer Family Family-Server

Note

Sie können Metriken für Transfer Family auch in der Transfer Family Family-Konsole selbst abrufen. Details hierzu finden Sie unter [Überwachung der Nutzung in der Konsole](#)

Mithilfe von CloudWatch Metriken können Sie Informationen über Ihren Server abrufen. Eine Metrik steht für einen nach der Zeit geordneten Satz von Datenpunkten, die veröffentlicht werden. CloudWatch Wenn Sie Metriken verwenden, müssen Sie den Transfer Family Family-Namespace, den Metriknamen und die [Dimension](#) angeben. Weitere Informationen zu Metriken finden Sie unter [Metriken](#) im CloudWatch Amazon-Benutzerhandbuch.

In der folgenden Tabelle werden die CloudWatch Metriken für Transfer Family beschrieben.

Namespace	Metrik	Description
AWS/Transfer	BytesIn	Die Gesamtzahl der auf den Server übertragenen Byte. Berichtskriterien: - Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. - Für AS2: wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und diese ausgibt, sobald die

Namespace	Metrik	Description
		Verarbeitung der eingehenden Nachricht abgeschlossen ist Einheiten: Anzahl Zeitraum: 5 Minuten
	BytesOut	Die Gesamtzahl der vom Server übertragenen Byte. Berichtskriterien: • Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. • Für AS2: wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Anschluss aus anruft und die Nachricht gesendet wird, sobald die Verarbeitung der ausgehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten

Namespace	Metrik	Description
	FilesIn	Die Gesamtzahl der auf den Server übertragenen Dateien. Bei Servern, die das AS2-Protokoll verwenden, stellt diese Metrik die Anzahl der empfangenen Nachrichten dar. Berichtskriterien: • Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. • Für AS2: wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und diese ausgibt, sobald die Verarbeitung der eingehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten

Namespace	Metrik	Description
	FilesOut	Die Gesamtzahl der vom Server übertragenen Dateien. Berichtskriterien: - Für SFTP/FTP/FTPS: Wird alle 5 Minuten gesendet, während eine Verbindung zum Transfer Family Family-Server hergestellt wird. Wenn in diesem Zeitraum keine Dateien oder Bytes übertragen werden, wird „0“ ausgegeben. - Für AS2: wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Anschluss aus anruft und die Nachricht gesendet wird, sobald die Verarbeitung der ausgehenden Nachricht abgeschlossen ist. Einheiten: Anzahl Zeitraum: 5 Minuten
	InboundMessage	Die Gesamtzahl der erfolgreich von einem Handelspartner empfangenen AS2-Nachrichten. Berichtskriterien: Wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und versendet, sobald die Verarbeitung der eingehenden Nachricht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten

Namespace	Metrik	Description
	InboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die von einem Handelspartner erfolglos empfangen wurden. Das heißt, ein Handelspartner hat eine Nachricht gesendet, aber der Transfer Family Family-Server konnte sie nicht erfolgreich verarbeiten. Berichtskriterien: Wenn der Kunde eine Nachricht auf seinem AS2-Server empfängt und sofort nach erfolgloser Verarbeitung der eingehenden Nachricht gesendet wird Einheiten: Anzahl Zeitraum: 5 Minuten
	OnUploadExecutionsStarted	Die Gesamtzahl der Workflow-Ausführungen, die auf dem Server gestartet wurden. Berichtskriterien: Wird bei jedem Start einer Ausführung ausgelöst Einheiten: Anzahl Zeitraum: 1 Minute
	OnUploadExecutionsSuccess	Die Gesamtzahl der erfolgreichen Workflow-Ausführungen auf dem Server. Berichtskriterien: Wird jedes Mal ausgelöst, wenn eine Ausführung erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 1 Minute

Namespace	Metrik	Description
	OnUploadExecutionsFailed	Die Gesamtzahl der erfolgreichen Workflow-Ausführungen auf dem Server. Berichtskriterien: Wird jedes Mal ausgelöst, wenn eine Ausführung nicht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 1 Minute
	OutboundMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolgreich an einen Handelspartner gesendet wurden. Berichtskriterien: Wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Connector aus anruft und die Nachricht sendet, sobald die Verarbeitung der ausgehenden Nachricht erfolgreich abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten
	OutboundFailedMessage	Die Gesamtzahl der AS2-Nachrichten, die erfolglos an einen Handelspartner gesendet wurden. Berichtskriterien: Wenn der Kunde <code>StartFileTransfer</code> von seinem AS2-Connector aus anruft und die Nachricht sendet, sobald die Verarbeitung der ausgehenden Nachricht erfolglos abgeschlossen wurde Einheiten: Anzahl Zeitraum: 5 Minuten

Familiendimensionen übertragen

Eine Dimension ist ein name/value Paar, das Teil der Identität einer Metrik ist. Weitere Informationen zu Abmessungen finden Sie unter [Abmessungen](#) im CloudWatch Amazon-Benutzerhandbuch.

In der folgenden Tabelle werden die CloudWatch Abmessungen für Transfer Family beschrieben.

Dimension	Description
ServerId	Die eindeutige ID des Servers.
ConnectorId	Die eindeutige ID des Connectors. Wird für AS2, für OutboundMessage und verwendet OutboundFailedMessage

Wird mit verwendet AWS-Benutzerbenachrichtigungen AWS Transfer Family

Um über AWS Transfer Family Ereignisse informiert [AWS-Benutzerbenachrichtigungen](#) zu werden, können Sie verschiedene Lieferkanäle einrichten. Wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht, erhalten Sie eine Benachrichtigung.

Sie können Benachrichtigungen für Ereignisse über mehrere Kanäle erhalten, einschließlich E-Mail, Chat-Benachrichtigungen von [Amazon Q Developer in Chat-Anwendungen](#) oder [AWS Console Mobile Application](#)-Push-Benachrichtigungen. Sie können Benachrichtigungen auch im [Benachrichtigungscenter der Konsole](#) sehen. Benutzerbenachrichtigungen unterstützt die Aggregation, wodurch die Anzahl der Benachrichtigungen, die Sie bei bestimmten Ereignissen erhalten, reduziert werden kann.

Weitere Informationen finden Sie in den Blogbeiträgen [Anpassen von Benachrichtigungen zur Dateizustellung mithilfe AWS Transfer Family verwalteter Workflows](#) und [Was ist AWS-Benutzerbenachrichtigungen?](#) im AWS-Benutzerbenachrichtigungen Benutzerhandbuch.

Verwenden von Abfragen zum Filtern von Protokolleinträgen

Sie können CloudWatch Abfragen verwenden, um Protokolleinträge für Transfer Family zu filtern und zu identifizieren. Dieser Abschnitt enthält einige Beispiele.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Sie können Abfragen oder Regeln erstellen.
 - Um eine Logs Insights-Abfrage zu erstellen, wählen Sie im linken Navigationsbereich Logs Insights aus und geben Sie dann die Details für Ihre Abfrage ein.
 - Um eine Contributor Insights-Regel zu erstellen, wählen Sie im linken Navigationsbereich Insights > Contributor Insights aus und geben Sie dann die Details für Ihre Regel ein.
3. Führen Sie die Abfrage oder Regel aus, die Sie erstellt haben.

Sehen Sie sich die häufigsten Ursachen für Authentifizierungsfehler an

In Ihren strukturierten Protokollen sieht ein Protokolleintrag für Authentifizierungsfehler in etwa wie folgt aus:

```
{
  "method":"password",
  "activity-type":"AUTH_FAILURE",
  "source-ip":"999.999.999.999",
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message":"Invalid user name or password",
  "user":"exampleUser"
}
```

Führen Sie die folgende Abfrage aus, um die Hauptverursacher von Authentifizierungsfehlern anzuzeigen.

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

Anstatt CloudWatch Logs Insights zu verwenden, können Sie eine CloudWatch Contributors Insights-Regel erstellen, um Authentifizierungsfehler anzuzeigen. Erstellen Sie eine Regel, die der folgenden ähnelt.

```
{
  "Aggregate0n": "Count",
```

```

"Contribution": {
  "Filters": [
    {
      "Match": "$.activity-type",
      "In": [
        "AUTH_FAILURE"
      ]
    }
  ],
  "Keys": [
    "$.user"
  ]
},
"LogFormat": "JSON",
"Schema": {
  "Name": "CloudWatchLogRule",
  "Version": 1
},
"LogGroupARNs": [
  "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
]
}

```

Protokolleinträge anzeigen, in denen eine Datei geöffnet wurde

In Ihren strukturierten Protokollen sieht ein Protokolleintrag zum Lesen einer Datei etwa wie folgt aus:

```

{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id": "0049cd844c7536c06a89"
}

```

Führen Sie die folgende Abfrage aus, um Protokolleinträge anzuzeigen, die darauf hinweisen, dass eine Datei geöffnet wurde.

```

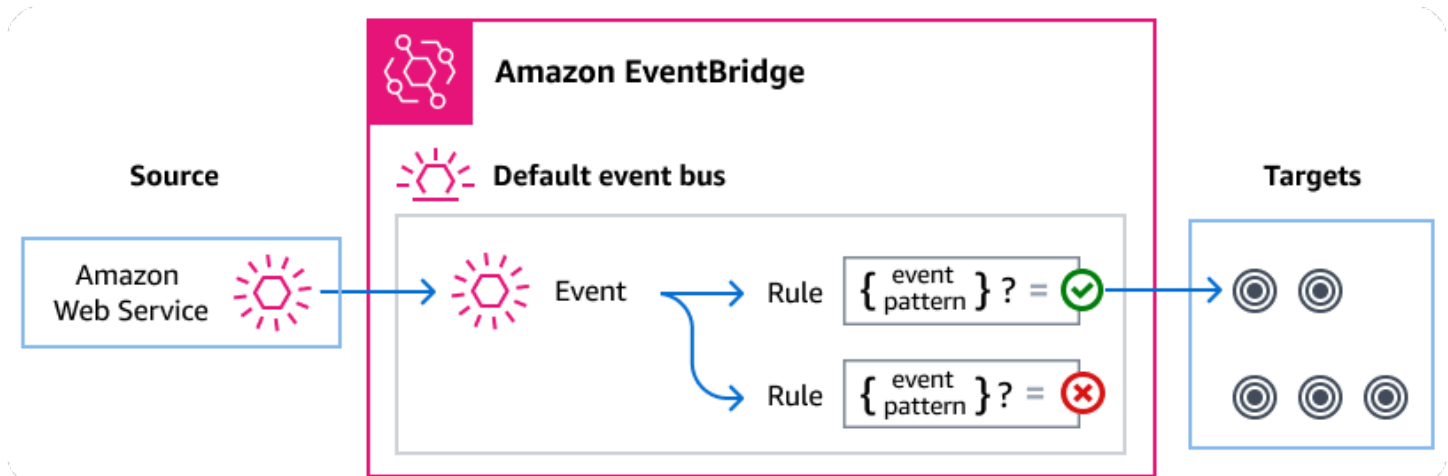
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path

```

Transfer Family Ereignisse verwalten mit Amazon EventBridge

Amazon EventBridge ist ein serverloser Dienst, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden. Dadurch können Sie leichter skalierbare, ereignisgesteuerte Anwendungen erstellen. Event-driven Architektur ist ein Stil, bei dem lose gekoppelte Softwaresysteme aufgebaut werden, die zusammenarbeiten, indem sie Ereignisse aussenden und darauf reagieren. Ereignisse stellen eine Veränderung in einer Ressource oder Umgebung dar.

Transfer Family Generiert wie bei vielen AWS Diensten Ereignisse und sendet sie an den EventBridge Standardereignisbus. Beachten Sie, dass der Standard-Event-Bus automatisch in jedem AWS Konto bereitgestellt wird. Ein Event Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele weiterleitet. Sie geben Regeln für den Event-Bus an, der Ereignisse auswertet, sobald sie eintreffen. Jede Regel prüft, ob ein Ereignis dem Ereignismuster der Regel entspricht. Wenn das Ereignis übereinstimmt, sendet der Event-Bus das Ereignis an ein oder mehrere angegebene Ziele.



Themen

- [Transfer Family Ereignisse](#)
- [Senden von Transfer Family Ereignissen mithilfe von Regeln EventBridge](#)
- [Amazon EventBridge Berechtigungen](#)
- [Zusätzliche EventBridge Ressourcen](#)
- [Transfer Family Referenz mit Einzelheiten zu Ereignissen](#)

Transfer Family Ereignisse

Transfer Family sendet Ereignisse automatisch an den EventBridge Standard-Event-Bus. Sie können Regeln auf dem Event-Bus erstellen, wobei jede Regel ein Ereignismuster und ein oder mehrere Ziele enthält.

Ereignisse, die dem Ereignismuster einer Regel entsprechen, werden entweder nach bestem Wissen und Gewissen an die angegebenen Ziele übermittelt (beachten Sie, dass einige Ereignisse möglicherweise nicht in der richtigen Reihenfolge übertragen werden). Diese Versandarten werden in der Amazon Events-Referenz unter [Lieferstufe für AWS EventBridge Serviceereignisse](#) beschrieben.

- Server-level Ereignisse für SFTP-, FTPS- und FTP-Server werden nach bestem Wissen und Gewissen bereitgestellt.
- Die Ereignisse für den SFTP-Connector werden dauerhaft übertragen.
- Die AS2-Ereignisse werden dauerhaft übertragen.

Die folgenden Ereignisse werden von Transfer Family generiert. Weitere Informationen finden Sie im Amazon EventBridge Benutzerhandbuch unter [EventBridge Ereignisse](#).

SFTP-, FTPS- und FTP-Serverereignisse

In den folgenden Tabellen sind die Ereignisse für SFTP-, FTPS- und FTP-Server nach Ereignistyp geordnet aufgeführt.

Ereignisse beim Hoch- und Herunterladen von Dateien

Ereignisdetailtyp	Description
Das Herunterladen der FTP-Server-Datei ist abgeschlossen	Eine Datei wurde erfolgreich für das FTP-Protokoll heruntergeladen.
Das Herunterladen der FTP-Serverdatei ist fehlgeschlagen	Ein Versuch, eine Datei für das FTP-Protokoll herunterzuladen, ist fehlgeschlagen.
Das Hochladen der Datei auf den FTP-Server ist abgeschlossen	Eine Datei wurde erfolgreich für das FTP-Protokoll hochgeladen.

Ereignisdetailtyp	Description
<u>Das Hochladen der FTP-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei hochzuladen, ist für das FTP-Protokoll fehlgeschlagen.
<u>Das Herunterladen der FTPS-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTPS-Protokoll heruntergeladen.
<u>Das Herunterladen der FTPS-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei für das FTPS-Protokoll herunterzuladen, ist fehlgeschlagen.
<u>Das Hochladen der Datei auf den FTPS-Server ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTPS-Protokoll hochgeladen.
<u>Das Hochladen der FTPS-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei hochzuladen, ist für das FTPS-Protokoll fehlgeschlagen.
<u>Der Download der SFTP-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das SFTP-Protokoll heruntergeladen.
<u>Das Herunterladen der SFTP-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei für das SFTP-Protokoll herunterzuladen, ist fehlgeschlagen.
<u>Das Hochladen der SFTP-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das SFTP-Protokoll hochgeladen.
<u>Das Hochladen der SFTP-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei hochzuladen, ist für das SFTP-Protokoll fehlgeschlagen.

Andere Ereignisse im Zusammenhang mit Dateivorgängen

Ereignisdetailtyp	Description
<u>Die Erstellung des FTP-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis wurde erfolgreich für das FTP-Protokoll erstellt.

Ereignisdetailtyp	Description
<u>Fehler beim Erstellen des FTP-Serververzeichnis</u>	Ein Versuch, ein Verzeichnis für das FTP-Protokoll zu erstellen, ist fehlgeschlagen.
<u>Das Löschen des FTP-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis für das FTP-Protokoll wurde erfolgreich gelöscht.
<u>Das Löschen des FTP-Serververzeichnisses ist fehlgeschlagen</u>	Ein Versuch, ein Verzeichnis für das FTP-Protokoll zu löschen, ist fehlgeschlagen.
<u>Das Löschen der FTP-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTP-Protokoll gelöscht.
<u>Das Löschen der FTP-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei für das FTP-Protokoll zu löschen, ist fehlgeschlagen.
<u>Das Umbenennen der FTP-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTP-Protokoll umbenannt.
<u>Fehler beim Umbenennen der FTP-Serverdatei</u>	Ein Versuch, eine Datei umzubenennen, ist für das FTP-Protokoll fehlgeschlagen.
<u>Die Erstellung des FTPS-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis wurde erfolgreich für das FTPS-Protokoll erstellt.
<u>Fehler beim Erstellen des FTPS-Serververzeichnisses</u>	Ein Versuch, ein Verzeichnis für das FTPS-Protokoll zu erstellen, ist fehlgeschlagen.
<u>Das Löschen des FTPS-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis wurde erfolgreich für das FTPS-Protokoll gelöscht.
<u>Das Löschen des FTPS-Serververzeichnisses ist fehlgeschlagen</u>	Ein Versuch, ein Verzeichnis für das FTPS-Protokoll zu löschen, ist fehlgeschlagen.

Ereignisdetailtyp	Description
<u>Das Löschen der FTPS-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTPS-Protokoll gelöscht.
<u>Das Löschen der FTPS-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei für das FTPS-Protokoll zu löschen, ist fehlgeschlagen.
<u>Die Umbenennung der FTPS-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das FTPS-Protokoll umbenannt.
<u>Fehler beim Umbenennen der FTPS-Serverdatei</u>	Ein Versuch, eine Datei umzubenennen, ist für das FTPS-Protokoll fehlgeschlagen.
<u>Die Erstellung des SFTP-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis wurde erfolgreich für das SFTP-Protokoll erstellt.
<u>Das Erstellen des SFTP-Serververzeichnisses ist fehlgeschlagen</u>	Ein Versuch, ein Verzeichnis für das SFTP-Protokoll zu erstellen, ist fehlgeschlagen.
<u>Das Löschen des SFTP-Serververzeichnisses ist abgeschlossen</u>	Ein Verzeichnis für das SFTP-Protokoll wurde erfolgreich gelöscht.
<u>Das Löschen des SFTP-Serververzeichnisses ist fehlgeschlagen</u>	Ein Versuch, ein Verzeichnis für das SFTP-Protokoll zu löschen, ist fehlgeschlagen.
<u>Das Löschen der SFTP-Serverdatei ist abgeschlossen</u>	Eine Datei für das SFTP-Protokoll wurde erfolgreich gelöscht.
<u>Das Löschen der SFTP-Serverdatei ist fehlgeschlagen</u>	Ein Versuch, eine Datei für das SFTP-Protokoll zu löschen, ist fehlgeschlagen.
<u>Die Umbenennung der SFTP-Serverdatei ist abgeschlossen</u>	Eine Datei wurde erfolgreich für das SFTP-Protokoll umbenannt.

Ereignisdetailtyp	Description
Das Umbenennen der SFTP-Serverdatei ist fehlgeschlagen	Ein Versuch, eine Datei umzubenennen, ist für das SFTP-Protokoll fehlgeschlagen.

Ereignisse des SFTP-Connectors

Note

Diese Ereignisse werden EventBridge auf einem dauerhaften Niveau zugestellt, wie unter [Lieferstufe für AWS Serviceereignisse](#) in der Amazon EventBridge Events-Referenz beschrieben.

Ereignisdetailtyp	Description
Der Versand der SFTP-Connector-Datei ist abgeschlossen	Eine Dateiübertragung von einem Connector zu einem Remote-SFTP-Server wurde erfolgreich abgeschlossen.
Das Senden der SFTP-Connector-Datei ist fehlgeschlagen	Eine Dateiübertragung von einem Connector zu einem Remote-SFTP-Server ist fehlgeschlagen.
Der Abruf der SFTP-Connector-Datei ist abgeschlossen	Eine Dateiübertragung von einem Remote-SFTP-Server zu einem Connector wurde erfolgreich abgeschlossen.
Fehler beim Abrufen der SFTP-Connector-Datei	Eine Dateiübertragung von einem Remote-SFTP-Server zu einem Connector ist fehlgeschlagen.
Die Verzeichnisliste des SFTP-Connectors ist abgeschlossen	Ein Aufruf zum Auflisten des Startdateiverzeichnisses, der erfolgreich abgeschlossen wurde.
Die Verzeichnisliste des SFTP-Connectors ist fehlgeschlagen	Eine Verzeichnisliste für die Startdatei, die fehlgeschlagen ist.

Ereignisdetailtyp	Description
Die Remote-Verschiebung des SFTP-Connectors ist abgeschlossen	Dateien oder Verzeichnisse wurden erfolgreich auf dem Remoteserver verschoben oder umbenannt.
Das Remote-Verschieben des SFTP-Connectors ist fehlgeschlagen	Dateien oder Verzeichnisse konnten auf dem Remoteserver nicht verschoben oder umbenannt werden.
Fernlöschung des SFTP-Connectors abgeschlossen	Dateien oder Verzeichnisse wurden erfolgreich auf dem Remoteserver gelöscht.
Das Remote-Löschen des SFTP-Connectors ist fehlgeschlagen	Dateien oder Verzeichnisse konnten auf dem Remoteserver nicht gelöscht werden.

AS2-Ereignisse

Note

Diese Ereignisse werden EventBridge auf einem dauerhaften Niveau zugestellt, wie unter [Lieferstufe für AWS Serviceereignisse](#) in der Amazon EventBridge Events-Referenz beschrieben.

Ereignisdetailtyp	Description
Empfang der AS2-Nutzlast abgeschlossen	Die Payload für eine AS2-Nachricht wurde empfangen.
Der Empfang der AS2-Nutzdaten ist fehlgeschlagen	Die Payload für eine AS2-Nachricht wurde nicht empfangen.
Der Versand der AS2-Nutzlast ist abgeschlossen	Die Payload für eine AS2-Nachricht wurde erfolgreich gesendet.

Ereignisdetailtyp	Description
Das Senden der AS2-Nutzlast ist fehlgeschlagen	Die Payload für eine AS2-Nachricht konnte nicht gesendet werden.
AS2 MDN-Empfang abgeschlossen	Die Benachrichtigung über die Entsorgung von Nachrichten für eine AS2-Nachricht wurde empfangen.
AS2 MDN-Empfang fehlgeschlagen	Die Benachrichtigung über die Nachrichtenablage für eine AS2-Nachricht wurde nicht empfangen.
AS2 MDN Send abgeschlossen	Die Benachrichtigung über den Nachrichtenzugriff für eine AS2-Nachricht wurde erfolgreich gesendet.
AS2 MDN konnte nicht gesendet werden	Die Benachrichtigung über die Nachrichtenablage für eine AS2-Nachricht konnte nicht gesendet werden.

Senden von Transfer Family Ereignissen mithilfe von Regeln EventBridge

Wenn Sie möchten, dass der EventBridge Standardereignisbus Transfer Family Ereignisse an ein Ziel sendet, müssen Sie eine Regel erstellen, die ein Ereignismuster enthält, das den Daten in Ihren gewünschten Transfer Family Ereignissen entspricht.

Um AWS Transfer Family Ereignisse in Amazon zu erfassen EventBridge

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/>.
2. Wählen Sie im Navigationsbereich Regeln und anschließend Regel erstellen aus.
3. Geben Sie einen aussagekräftigen Namen für die Regel und optional eine Beschreibung ein.
4. Wählen Sie als Regeltyp die Option Regel mit einem Ereignismuster und dann Weiter aus.
5. Wählen Sie im Abschnitt Ereignisquelle AWS Ereignisse oder EventBridge Partnerereignisse aus.
6. Wählen Sie im Abschnitt Erstellungsmethode die Option Musterformular verwenden aus.
7. Geben Sie im Abschnitt Ereignismuster die folgenden Informationen ein.

- a. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
- b. Wählen Sie für AWS Service die Option Transfer aus.
- c. Wählen Sie als Ereignistyp den Ereignistyp „Transfer Family“ aus, der Ihre Regel auslösen soll.

Je nachdem, welchen Ereignistyp Sie ausgewählt haben, wird Ihnen möglicherweise der Abschnitt Ereignistyp-Spezifikation 1 angezeigt.

- d. Wenn Sie den Abschnitt Ereignistyp-Spezifikation 1 sehen, wählen Sie die spezifischen Ereignisse aus, die Sie erfassen möchten (oder wählen Sie Beliebige Ereignis, um alle Ereignisse für den ausgewählten Ereignistyp zu erfassen).
 - e. (Optional) Verwenden Sie den Event-Muster-Editor, um Filter für Eventdetails festzulegen.
 - f. Wählen Sie Weiter aus.
8. Wählen Sie ein Ziel aus den unter Ziele auswählen verfügbaren Optionen aus. Wählen Sie eines der folgenden verfügbaren Ziele aus.
- AWS Dienst. Beliebte Optionen sind Lambda-Funktionen für serverloses Computing, Amazon SQS SQS-Warteschlangen für die Nachrichtenverarbeitung, Amazon SNS SNS-Themen für Benachrichtigungen und für die Orchestrierung von Workflows. AWS Step Functions
 - EventBridge API-Ziel. Wenn Sie Ereignisse an einen HTTP-Endpunkt außerhalb von senden möchten AWS, können Sie ein API-Ziel als Ziel verwenden.
 - EventBridge Event-Bus. Sie können Ereignisse an einen anderen Eventbus senden, entweder in demselben Konto und derselben Region oder in einem anderen Konto oder in einer anderen Region.

Umfassende Anweisungen zur Erstellung von Event-Bus-Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch unter [Regeln erstellen, die auf Ereignisse reagieren](#).

Hilfe bei der Auswahl eines Ziels finden [Sie unter Ziele auswählen](#) im EventBridge Amazon-Benutzerhandbuch.

9. Konfigurieren Sie alle zusätzlichen Optionen für Ihr Ziel und wählen Sie dann Weiter.
10. (Optional) Fügen Sie Ihrer Regel Tags hinzu und wählen Sie Weiter aus.
11. Wenn alles gut aussieht, wählen Sie im Bildschirm Überprüfen und erstellen die Option Regel erstellen aus.

Ereignismuster für Transfer Family Ereignisse erstellen

Wenn ein Ereignis an den Standardereignisbus Transfer Family übermittelt, EventBridge verwendet das für jede Regel definierte Ereignismuster, um zu bestimmen, ob das Ereignis an die Ziele der Regel gesendet werden soll. Ein Ereignismuster entspricht den Daten in den gewünschten Transfer Family Ereignissen. Jedes Ereignismuster ist ein JSON-Objekt, das Folgendes enthält:

- Ein `source`-Attribut, das den Service identifiziert, der das Ereignis sendet. Für Transfer Family Ereignisse ist die Quelle `aws.transfer`.
- (Optional) Ein `detail-type` Attribut, das ein Array der zuzuordnenden Ereignistypen enthält.
- (Optional) Ein `detail` Attribut, das alle anderen Ereignisdaten enthält, für die ein Abgleich erforderlich ist.

Das folgende Ereignismuster entspricht beispielsweise allen Ereignissen von Transfer Family:

```
{
  "source": ["aws.transfer"]
}
```

Das folgende Beispiel für ein Ereignismuster entspricht allen Ereignissen des SFTP-Connectors:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve Completed",
                  "SFTP Connector File Retrieve Failed", "SFTP Connector File Send Failed"]
}
```

Das folgende Beispiel für ein Ereignismuster entspricht allen fehlgeschlagenen Transfer Family Family-Ereignissen:

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

Das folgende Beispiel für ein Ereignismuster entspricht erfolgreichen SFTP-Downloads für den Benutzer *username*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

Weitere Informationen zum Schreiben von Ereignismustern finden Sie unter [Ereignismuster](#) im EventBridge Benutzerhandbuch.

Testen von Ereignismustern für Transfer Family Ereignisse in EventBridge

Sie können die EventBridge Sandbox verwenden, um schnell ein Ereignismuster zu definieren und zu testen, ohne den umfassenderen Prozess der Erstellung oder Bearbeitung einer Regel abschließen zu müssen. Mithilfe der Sandbox können Sie ein Ereignismuster definieren und anhand eines Beispielerignisses überprüfen, ob das Muster den gewünschten Ereignissen entspricht. EventBridge bietet Ihnen die Möglichkeit, eine neue Regel zu erstellen, indem Sie dieses Ereignismuster direkt aus der Sandbox verwenden.

Weitere Informationen finden Sie unter [Testen eines Ereignismusters mithilfe der EventBridge Sandbox](#) im EventBridge Benutzerhandbuch.

Amazon EventBridge Berechtigungen

Transfer Family benötigt keine zusätzlichen Berechtigungen für die Übermittlung von Ereignissen an Amazon EventBridge.

Für die von Ihnen angegebenen Ziele sind möglicherweise bestimmte Berechtigungen oder Konfigurationen erforderlich. Weitere Informationen zur Verwendung bestimmter Dienste für [Amazon EventBridge Ziele](#) finden Sie im Amazon EventBridge Benutzerhandbuch unter Ziele.

Zusätzliche EventBridge Ressourcen

Weitere Informationen zur Verarbeitung und Verwaltung von Ereignissen finden Sie EventBridge in den folgenden Themen im [Amazon EventBridge Benutzerhandbuch](#).

- Ausführliche Informationen zur Funktionsweise von Eventbussen finden Sie unter [Amazon EventBridge Event-Bus](#).

- Informationen zur Veranstaltungsstruktur finden Sie unter [Ereignisse](#).
- Informationen zur Erstellung von Ereignismustern für EventBridge den Abgleich von Ereignissen mit Regeln finden Sie unter [Ereignismuster](#).
- Informationen zum Erstellen von Regeln, mit denen angegeben wird, welche Ereignisse EventBridge verarbeitet werden, finden Sie unter [Regeln](#).
- Informationen darüber, wie Sie angeben, an welche Dienste oder andere Ziele übereinstimmende Ereignisse EventBridge gesendet werden, finden Sie unter [Ziele](#).

Transfer Family Referenz mit Einzelheiten zu Ereignissen

Alle Ereignisse von AWS Diensten haben einen gemeinsamen Satz von Feldern, die Metadaten zu dem Ereignis enthalten. Zu diesen Metadaten können der AWS Dienst gehören, der die Quelle des Ereignisses ist, die Uhrzeit, zu der das Ereignis generiert wurde, das Konto und die Region, in der das Ereignis stattgefunden hat, und andere. Definitionen dieser allgemeinen Felder finden Sie unter [Referenz zur Ereignisstruktur](#) im Amazon EventBridge Benutzerhandbuch.

Darüber hinaus weist jedes Ereignis ein `detail`-Feld auf, das spezifische Daten für das betreffende Ereignis enthält. Die folgende Referenz definiert die Detailfelder für die verschiedenen Transfer Family Ereignisse.

Beachten Sie EventBridge bei der Auswahl und Verwaltung von Transfer Family Ereignissen Folgendes:

- Das `source` Feld für alle Ereignisse von Transfer Family ist auf `aws:transfer`.
- Das Feld `detail-type` gibt den Ereignistyp an.

Beispiel, `FTP Server File Download Completed`.

- Das Feld `detail` enthält die Daten, die für das betreffende Ereignis spezifisch sind.

Informationen zur Erstellung von Ereignismustern, die es Regeln ermöglichen, Transfer Family Ereignissen zuzuordnen, finden Sie im Amazon EventBridge Benutzerhandbuch unter [Ereignismuster](#).

Weitere Informationen zu Ereignissen und deren EventBridge Verarbeitung finden Sie im Amazon EventBridge Benutzerhandbuch unter [Amazon EventBridge Ereignisse](#).

Themen

- [SFTP-, FTPS- und FTP-Serverereignisse](#)
- [Ereignisse des SFTP-Connectors](#)
- [AS2-Ereignisse](#)

SFTP-, FTPS- und FTP-Serverereignisse

Im Folgenden finden Sie die Detailfelder für SFTP-, FTPS- und FTP-Serverereignisse:

- Die Erstellung des FTP-Serververzeichnis ist abgeschlossen
- Das Erstellen des FTP-Serververzeichnis ist fehlgeschlagen
- Das Löschen des FTP-Serververzeichnis ist abgeschlossen
- Das Löschen des FTP-Serververzeichnis ist fehlgeschlagen
- Das Löschen der FTP-Serverdatei ist abgeschlossen
- Das Löschen der FTP-Serverdatei ist fehlgeschlagen
- Das Herunterladen der FTP-Serverdatei ist abgeschlossen
- Das Herunterladen der FTP-Serverdatei ist fehlgeschlagen
- Das Umbenennen der FTP-Serverdatei ist abgeschlossen
- Fehler beim Umbenennen der FTP-Serverdatei
- Das Hochladen der FTP-Serverdatei ist abgeschlossen
- Das Hochladen der FTP-Serverdatei ist fehlgeschlagen
- Die Erstellung des FTPS-Serververzeichnis ist abgeschlossen
- Das Erstellen des FTPS-Serververzeichnis ist fehlgeschlagen
- Das Löschen des FTPS-Serververzeichnis ist abgeschlossen
- Das Löschen des FTPS-Serververzeichnis ist fehlgeschlagen
- Das Löschen der FTPS-Serverdatei ist abgeschlossen
- Das Löschen der FTPS-Serverdatei ist fehlgeschlagen
- Das Herunterladen der FTPS-Serverdatei ist abgeschlossen
- Das Herunterladen der FTPS-Serverdatei ist fehlgeschlagen
- Das Umbenennen der FTPS-Serverdatei ist abgeschlossen
- Das Umbenennen der FTPS-Serverdatei ist fehlgeschlagen

- Das Hochladen der FTPS-Serverdatei ist abgeschlossen
- Das Hochladen der FTPS-Serverdatei ist fehlgeschlagen
- Die Erstellung des SFTP-Serververzeichnisses ist abgeschlossen
- Das Erstellen des SFTP-Serververzeichnisses ist fehlgeschlagen
- Das Löschen des SFTP-Serververzeichnisses ist abgeschlossen
- Das Löschen des SFTP-Serververzeichnisses ist fehlgeschlagen
- Das Löschen der SFTP-Serverdatei ist abgeschlossen
- Das Löschen der SFTP-Serverdatei ist fehlgeschlagen
- Das Herunterladen der SFTP-Serverdatei ist abgeschlossen
- Das Herunterladen der SFTP-Serverdatei ist fehlgeschlagen
- Das Umbenennen der SFTP-Serverdatei ist abgeschlossen
- Das Umbenennen der SFTP-Serverdatei ist fehlgeschlagen
- Das Hochladen der SFTP-Serverdatei ist abgeschlossen
- Das Hochladen der SFTP-Serverdatei ist fehlgeschlagen

Die `detail`-type Felder `source` und `detail` sind unten aufgeführt, da sie spezifische Werte für Transfer Family Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter [Referenz zur Ereignisstruktur](#) im Amazon EventBridge Benutzerhandbuch.

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
```

```
"original-file-path" : "string",
"renamed-file-path" : "string",
"directory-path" : "string",
"server-id" : "string",
"username" : "string",
"session-id" : "string",
"start-timestamp" : "string"
}
}
```

detail-type

Identifiziert den Ereignistyp.

Für dieses Ereignis ist der Wert einer der zuvor aufgeführten SFTP-, FTPS- oder FTP-Serverereignisnamen.

source

Identifiziert den Service, aus dem das Ereignis stammt. Für Transfer Family Family-Veranstaltungen ist dieser Wert `aws.transfer`.

detail

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis umfassen die Daten Folgendes:

failure-code

Kategorie, warum die Übertragung fehlgeschlagen ist. Werte: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

status-code

Ob die Übertragung erfolgreich ist. Werte: `COMPLETED` | `FAILED`.

protocol

Das für die Übertragung verwendete Protokoll. Werte: `SFTP` | `FTPS` | `FTP`

bytes

Die Anzahl der übertragenen Bytes.

`client-ip`

Die IP-Adresse des Clients, der an der Übertragung beteiligt ist

`failure-message`

Bei fehlgeschlagenen Übertragungen die Details, warum die Übertragung fehlgeschlagen ist.

`end-timestamp`

Bei erfolgreichen Übertragungen der Zeitstempel, wann die Verarbeitung der Datei abgeschlossen ist.

`etag`

Das Entity-Tag (wird nur für Amazon S3 S3-Dateien verwendet).

`file-path`

Der Pfad zu der Datei, die übertragen, gelöscht oder anderweitig bearbeitet wird.

`original-file-path`

Bei Ereignissen zum Umbenennen von Dateien der ursprüngliche Pfad der Datei vor dem Umbenennen.

`renamed-file-path`

Bei Ereignissen zum Umbenennen von Dateien der neue Pfad der Datei nach dem Umbenennen.

`directory-path`

Bei Ereignissen zum Erstellen und Löschen von Verzeichnissen der Pfad des Verzeichnisses.

`server-id`

Die eindeutige ID für den Transfer Family Family-Server.

`username`

Der Benutzer, der die Übertragung durchführt.

`session-id`

Die eindeutige Kennung für die Übertragungssitzung.

`start-timestamp`

Bei erfolgreichen Übertragungen der Zeitstempel für den Beginn der Dateiverarbeitung.

Example Beispielereignis: Fehler beim Herunterladen der SFTP-Serverdatei

Das folgende Beispiel zeigt ein Ereignis, bei dem ein Download auf einem SFTP-Server fehlgeschlagen Amazon EFS ist (wird der Speicher verwendet).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Download Failed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T17:20:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "failure-code": "PARTIAL_DOWNLOAD",
    "status-code": "FAILED",
    "protocol": "SFTP",
    "bytes": 4100,
    "client-ip": "IP-address",
    "failure-message": "File was partially downloaded.",
    "end-timestamp": "2024-01-29T17:20:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2024-01-29T17:20:16.706282454Z"
  }
}
```

Example Beispielereignis „Dateiupload abgeschlossen“ auf dem FTP-Server

Das folgende Beispiel zeigt ein Ereignis, bei dem ein Upload auf einem FTP-Server erfolgreich abgeschlossen wurde (Amazon S3 wird der Speicher verwendet).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "FTP Server File Upload Completed",
  "source": "aws.transfer",
  "account": "958412138249",
```

```

    "time": "2024-01-29T16:31:43Z",
    "region": "us-east-1",
    "resources": [
      "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
    ],
    "detail": {
      "status-code": "COMPLETED",
      "protocol": "FTP",
      "bytes": 1048576,
      "client-ip": "10.0.0.141",
      "end-timestamp": "2024-01-29T16:31:43.311866408Z",
      "etag": "b6d81b360a5672d80c27430f39153e2c",
      "file-path": "/amzn-s3-demo-bucket/test/1mb_file",
      "server-id": "s-1111aaaa2222bbbb3",
      "username": "test",
      "session-id": "event-ID",
      "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
  }
}

```

Example Beispiereignis „SFTP-Serverdatei löschen“ abgeschlossen

Das folgende Beispiel zeigt ein Ereignis, bei dem eine Datei erfolgreich auf einem SFTP-Server gelöscht wurde.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
  }
}

```

```

    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}

```

Example Beispiereignis zum Umbenennen der SFTP-Serverdatei abgeschlossen

Das folgende Beispiel zeigt ein Ereignis, bei dem eine Datei auf einem SFTP-Server erfolgreich umbenannt wurde.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Rename Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T15:45:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T15:45:12.749749117Z",
    "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
    "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T15:45:11.706282454Z"
  }
}

```

Example Beispiereignis „SFTP-Serververzeichnis erstellen“ abgeschlossen

Das folgende Beispiel zeigt ein Ereignis, bei dem ein Verzeichnis erfolgreich auf einem SFTP-Server erstellt wurde.

```

{

```

```

    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server Directory Create Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T16:20:05Z",
    "region": "us-east-1",
    "resources": [
      "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
      "status-code": "COMPLETED",
      "protocol": "SFTP",
      "client-ip": "IP-address",
      "end-timestamp": "2025-05-15T16:20:05.749749117Z",
      "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
      "server-id": "s-1234abcd5678efghi",
      "username": "test",
      "session-id": "session-ID",
      "start-timestamp": "2025-05-15T16:20:04.706282454Z"
    }
  }
}

```

Ereignisse des SFTP-Connectors

Note

Diese Ereignisse werden EventBridge auf einem dauerhaften Niveau zugestellt, wie unter [Lieferstufe für AWS Serviceereignisse](#) in der Amazon EventBridge Events-Referenz beschrieben.

Im Folgenden sind die Detailfelder für SFTP-Connector-Ereignisse aufgeführt:

- Das Senden der SFTP-Connector-Datei ist abgeschlossen
- Das Senden der SFTP-Connector-Datei ist fehlgeschlagen
- Der Abruf der SFTP-Connector-Datei ist abgeschlossen
- Fehler beim Abrufen der SFTP-Connector-Datei
- Die Verzeichnisliste für den SFTP-Connector ist abgeschlossen
- Die Verzeichnisliste für den SFTP-Connector ist fehlgeschlagen

- Die Remote-Verschiebung des SFTP-Connectors ist abgeschlossen
- Die Remote-Verschiebung des SFTP-Connectors ist fehlgeschlagen
- Fernlöschung des SFTP-Connectors abgeschlossen
- Das Löschen des SFTP-Connectors per Fernzugriff ist fehlgeschlagen

Die `detail-type` Felder `source` und `detail` sind unten aufgeführt, da sie spezifische Werte für Transfer Family Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter [Referenz zur Ereignisstruktur](#) im Amazon EventBridge Benutzerhandbuch.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string",
    "item-count" : "number",
    "truncated" : "boolean",
    "bytes" : "number",
    "egress-type" : "string",
    "vpc-lattice-resource-configuration-arn" : "string",
    "vpc-lattice-port-number" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",

```

```
    "key" : "string"
  },
  "output-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  }
}
```

detail-type

Identifiziert den Ereignistyp.

Für dieses Ereignis entspricht der Wert einem der zuvor aufgeführten SFTP-Connector-Ereignisnamen.

source

Identifiziert den Service, aus dem das Ereignis stammt. Für Transfer Family Ereignisse ist `aws.transfer` dieser Wert.

detail

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Dienst, der das Ereignis generiert, bestimmt den Inhalt dieses Felds.

Für dieses Ereignis umfassen die Daten Folgendes:

max-items

Die maximale Anzahl von directory/file Namen, die zurückgegeben werden sollen.

operation

Ob die `StartFileTransfer` Anfrage eine Datei sendet oder abruft. Werte: `SEND` | `RETRIEVE`.

connector-id

Die eindeutige Kennung für den verwendeten SFTP-Connector.

output-directory-path

Der Pfad (Bucket und Präfix) in Amazon S3 zum Speichern der Ergebnisse des file/directory Angebots.

listing-id

Eine eindeutige Kennung für den StartDirectoryListing API-Vorgang. Diese Kennung kann verwendet werden, um in den CloudWatch Protokollen den Status der Angebotsanfrage zu überprüfen.

transfer-id

Die eindeutige Kennung für das Übertragungsereignis (eine StartFileTransfer Anfrage).

file-transfer-id

Die eindeutige Kennung für die übertragene Datei.

url

Die URL des AS2- oder SFTP-Endpunkts des Partners.

file-path

Der Speicherort und die Datei, die gesendet oder abgerufen werden.

status-code

Ob die Übertragung erfolgreich ist. Werte: FAILED | COMPLETED.

failure-code

Bei fehlgeschlagenen Übertragungen der Ursachencode, warum die Übertragung fehlgeschlagen ist.

failure-message

Bei fehlgeschlagenen Übertragungen die Details, warum die Übertragung fehlgeschlagen ist.

start-timestamp

Bei erfolgreichen Übertragungen der Zeitstempel für den Beginn der Dateiverarbeitung.

end-timestamp

Bei erfolgreichen Übertragungen der Zeitstempel für den Abschluss der Dateiverarbeitung.

local-directory-path

Bei RETRIEVE Anfragen der Ort, an dem die abgerufene Datei abgelegt werden soll.

`remote-directory-path`

Bei SEND Anfragen das Dateiverzeichnis, in dem die Datei auf dem SFTP-Server des Partners abgelegt werden soll. Dies ist der Wert für den `RemoteDirectoryPath`, den der Benutzer an die `StartFileTransfer` Anfrage übergeben hat. Sie können ein Standardverzeichnis auf dem SFTP-Server des Partners angeben. Wenn ja, ist dieses Feld leer.

`item-count`

Die Anzahl der Elemente (Verzeichnisse und Dateien), die für die Angebotsanfrage zurückgegeben wurden.

`truncated`

Ob die Listenausgabe alle im Remote-Verzeichnis enthaltenen Elemente enthält oder nicht.

`bytes`

Die Anzahl der Byte, die übertragen werden. Der Wert ist 0 für fehlgeschlagene Übertragungen.

`egress-type`

Art der Ausgangskonfiguration für den Connector. Werte: `SERVICE_MANAGED` oder `VPC_LATTICE`.

`vpc-lattice-resource-configuration-arn`

ARN der `VPC_LATTICE`-Ressourcenkonfiguration, die den Ziel-SFTP-Serverstandort definiert. Dieses Feld hat für vom Service verwaltete Connectors den Wert Null.

`vpc-lattice-port-number`

Portnummer für die Verbindung zum SFTP-Server über `VPC_LATTICE`.

`local-file-location`

Dieser Parameter enthält die Details zum Speicherort der Speicherdatei. AWS

`domain`

Der Speicher, der verwendet wird. Derzeit ist der einzige Wert `S3`.

`bucket`

Der Container für das Objekt in Amazon S3.

key

Der dem Objekt in Amazon S3 zugewiesene Name.

output-file-location

Dieser Parameter enthält die Details des AWS Speicherorts, an dem die Ergebnisse der Verzeichnisliste gespeichert werden sollen.

domain

Der Speicher, der verwendet wird. Derzeit ist der einzige Wert S3.

bucket

Der Container für das Objekt in Amazon S3.

key

Der dem Objekt in Amazon S3 zugewiesene Name.

Example Beispielergebnis beim Senden der SFTP-Connector-Datei fehlgeschlagen

Das folgende Beispiel zeigt ein Ereignis, bei dem ein SFTP-Connector beim Versuch, eine Datei an einen Remote-SFTP-Server zu senden, fehlgeschlagen ist.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Send Failed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T19:30:45Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "SEND",
    "connector-id": "c-f1111aaaa2222bbbb3",
    "transfer-id": "transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/testfile.txt",
    "status-code": "FAILED",
```

```

    "failure-code": "CONNECTION_ERROR",
    "failure-message": "Unknown Host",
    "remote-directory-path": "",
    "bytes": 0,
    "start-timestamp": "2024-01-24T18:29:33.658729Z",
    "end-timestamp": "2024-01-24T18:29:33.993196Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}

```

Example Beispiereignis „SFTP-Connector File Retrieve Completed“

Das folgende Beispiel zeigt ein Ereignis, bei dem ein SFTP-Connector erfolgreich eine von einem Remote-SFTP-Server gesendete Datei abgerufen hat.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Retrieve Completed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T18:28:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "RETRIEVE",
    "connector-id": "c-fc68000012345aa18",
    "transfer-id": "file-transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "testfile.txt",
    "status-code": "COMPLETED",
    "local-directory-path": "/amzn-s3-demo-bucket",
    "bytes": 63533,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "local-file-location": {

```

```

        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "testfile.txt"
    }
}

```

Example Beispiereignis mit der Verzeichnisliste des SFTP-Connectors abgeschlossen

Das folgende Beispiel zeigt ein Ereignis, bei dem ein Startaufruf für die Verzeichnisliste eine Auflistungsdatei von einem Remote-SFTP-Server abgerufen hat.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector Directory Listing Completed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T18:28:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "max-items": 10000,
    "connector-id": "c-fc68000012345aa18",
    "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
    "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

    "status-code": "COMPLETED",
    "remote-directory-path": "/home",
    "item-count": 10000,
    "truncated": true,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "output-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
    }
  }
}

```

AS2-Ereignisse

Note

Diese Ereignisse werden EventBridge auf einem dauerhaften Niveau zugestellt, wie unter [Lieferstufe für AWS Serviceereignisse](#) in der Amazon EventBridge Events-Referenz beschrieben.

Im Folgenden sind die Detailfelder für AS2-Ereignisse aufgeführt:

- Empfang der AS2-Nutzlast abgeschlossen
- Der Empfang der AS2-Nutzdaten ist fehlgeschlagen
- Der Versand der AS2-Nutzlast ist abgeschlossen
- Das Senden der AS2-Nutzdaten ist fehlgeschlagen
- AS2 MDN-Empfang abgeschlossen
- AS2 MDN-Empfang fehlgeschlagen
- AS2 MDN-Sendung abgeschlossen
- AS2 MDN-Sendung ist fehlgeschlagen

Die `detail-type` Felder `source` und `detail` sind unten aufgeführt, da sie spezifische Werte für Transfer Family Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter [Referenz zur Ereignisstruktur](#) im Amazon EventBridge Benutzerhandbuch.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
```



```
    "mdn-key" : "string"
  }
  "mdn-subject" : "string",
  "mdn-message-id" : "string",
  "disposition" : "string",
  "bytes" : "number",
  "as2-from" : "string",
  "as2-message-id" : "string",
  "as2-to" : "string",
  "connector-id" : "string",
  "client-ip" : "string",
  "agreement-id" : "string",
  "server-id" : "string",
  "requester-file-name" : "string",
  "message-subject" : "string",
  "start-timestamp" : "string",
  "end-timestamp" : "string",
  "status-code" : "string",
  "failure-code" : "string",
  "failure-message" : "string",
  "transfer-id" : "string"
}
```

detail-type

Identifiziert den Ereignistyp.

Für dieses Ereignis ist der Wert eines der zuvor aufgeführten AS2-Ereignisse.

source

Identifiziert den Service, aus dem das Ereignis stammt. Für Transfer Family Ereignisse ist `aws.transfer` dieser Wert.

detail

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

s3-attributes

Identifiziert den Amazon S3 S3-Bucket und den Schlüssel für die übertragene Datei. Bei MDN-Ereignissen identifiziert es auch den Bucket und den Schlüssel für die MDN-Datei.

file-bucket

Der Container für das Objekt in Amazon S3.

file-key

Der dem Objekt in Amazon S3 zugewiesene Name.

json-bucket

Bei ABGESCHLOSSENEN oder FEHLGESCHLAGENEN Übertragungen der Container für die JSON-Datei.

json-key

Bei ABGESCHLOSSENEN oder FEHLGESCHLAGENEN Übertragungen der Name, der der JSON-Datei in Amazon S3 zugewiesen wurde.

mdn-bucket

Bei MDN-Ereignissen der Container für die MDN-Datei.

mdn-key

Bei MDN-Ereignissen der Name, der der MDN-Datei in Amazon S3 zugewiesen wurde.

mdn-subject

Bei MDN-Ereignissen eine Textbeschreibung für die Nachrichtenverwaltung.

mdn-message-id

Bei MDN-Ereignissen eine eindeutige ID für die MDN-Nachricht.

disposition

Bei MDN-Ereignissen die Kategorie für die Disposition.

bytes

Die Anzahl der Byte in der Nachricht.

as2-from

Der AS2-Handelspartner, der die Nachricht sendet.

as2-message-id

Eine eindeutige Kennung für die AS2-Nachricht, die übertragen wird.

as2-to

Der AS2-Handelspartner, der die Nachricht empfängt.

connector-id

Für AS2-Nachrichten, die von einem Transfer Family Family-Server an einen Handelspartner gesendet werden, wird die eindeutige Kennung für den AS2-Connector verwendet.

client-ip

Bei Serverereignissen (Übertragungen von einem Geschäftspartner zu einem Transfer Family Family-Server) die IP-Adresse des an der Übertragung beteiligten Clients.

agreement-id

Bei Serverereignissen die eindeutige Kennung für die AS2-Vereinbarung.

server-id

Für Serverereignisse eine eindeutige ID nur für den Transfer Family Family-Server.

requester-file-name

Bei Payload-Ereignissen der ursprüngliche Name der Datei, die während der Übertragung empfangen wurde.

message-subject

Eine Textbeschreibung für den Betreff der Nachricht.

start-timestamp

Bei erfolgreichen Übertragungen der Zeitstempel für den Beginn der Dateiverarbeitung.

end-timestamp

Bei erfolgreichen Übertragungen der Zeitstempel für den Abschluss der Dateiverarbeitung.

status-code

Der Code, der dem Status des AS2-Nachrichtenübertragungsprozesses entspricht. Zulässige Werte: COMPLETED | FAILED | PROCESSING.

failure-code

Bei fehlgeschlagenen Übertragungen die Kategorie, warum die Übertragung fehlgeschlagen ist.

failure-message

Bei fehlgeschlagenen Übertragungen die Details, warum die Übertragung fehlgeschlagen ist.

transfer-id

Die eindeutige Kennung für das Übertragungsereignis.

Example Beispielergebnis „AS2 Payload Receive Completed“

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 Payload Receive Completed",
  "source": "aws.transfer",
  "account": "076722215406",
  "time": "2024-02-07T06:47:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/c-1111aaaa2222bbbb3"],
  "detail": {
    "s3-attributes": {
      "file-key": "/inbound/processed/testAs2Message.dat",
      "file-bucket": "amzn-s3-demo-bucket"
    },
    "client-ip": "client-IP-address",
    "requester-file-name": "testAs2MessageVerifyFile.dat",
    "end-timestamp": "2024-02-07T06:47:06.040031Z",
    "as2-from": "as2-from-ID",
    "as2-message-id": "as2-message-ID",
    "message-subject": "Message from AS2 tests",
    "start-timestamp": "2024-02-07T06:47:05.410Z",
    "status-code": "PROCESSING",
    "bytes": 63,
    "as2-to": "as2-to-ID",
    "agreement-id": "a-1111aaaa2222bbbb3",
    "server-id": "s-1234abcd5678efghi"
  }
}
```

Example Beispielergebnis „AS2 MDN Receive Failed“

```
{
```

```

"version": "0",
"id": "event-ID",
"detail-type": "AS2 MDN Receive Failed",
"source": "aws.transfer",
"account": "889901007463",
"time": "2024-02-06T22:05:09Z",
"region": "us-east-1",
"resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
"detail": {
  "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde
to partner ijklmnop987654",
  "s3-attributes": {
    "json-bucket": "amzn-s3-demo-bucket1",
    "file-key": "/as2Integ/TestOutboundWrongCert.dat",
    "file-bucket": "amzn-s3-demo-bucket2",
    "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
  },
  "mdn-message-id": "MDN-message-ID",
  "end-timestamp": "2024-02-06T22:05:09.479878Z",
  "as2-from": "PartnerA",
  "as2-message-id": "as2-message-ID",
  "connector-id": "c-1234abcd5678efghj",
  "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
  "start-timestamp": "2024-02-06T22:05:03Z",
  "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
  "status-code": "FAILED",
  "as2-to": "MyCompany",
  "failure-message": "No public certificate matching message signature could be
found in profile: p-1234abcd5678efghj",
  "transfer-id": "transfer-ID"
}
}

```

Sicherheit in AWS Transfer Family

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Transfer Family. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Transfer Family , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Transfer Family Ressourcen unterstützen.

Wir bieten einen Workshop mit präskriptiven Anleitungen und einem praktischen Lab an, in dem Sie erfahren, wie Sie eine skalierbare und sichere Dateiübertragungsarchitektur aufbauen können, AWS ohne bestehende Anwendungen ändern oder die Serverinfrastruktur verwalten zu müssen. [Die Einzelheiten zu diesem Workshop finden Sie hier.](#)

Themen

- [Sicherheitsvorteile der VPC-Konnektivität](#)
- [Sicherheitsrichtlinien für Server AWS Transfer Family](#)
- [Sicherheitsrichtlinien für SFTP-Konnektoren AWS Transfer Family](#)

- [Verwenden Sie den hybriden Schlüsselaustausch nach dem Quantum mit AWS Transfer Family](#)
- [Datenschutz und Verschlüsselung](#)
- [Verwaltung von SSH- und PGP-Schlüsseln in Transfer Family](#)
- [Identitäts- und Zugriffsmanagement für AWS Transfer Family](#)
- [Konformitätsprüfung für AWS Transfer Family](#)
- [Resilienz in AWS Transfer Family](#)
- [Erstellen Sie eine private Verbindung zwischen einer VPC und APIs AWS Transfer Family](#)
- [Sicherheit der Infrastruktur in AWS Transfer Family](#)
- [Fügen Sie eine Firewall für Webanwendungen hinzu](#)
- [Cross-service verwirrter Stellvertreter, Prävention](#)
- [AWS verwaltete Richtlinien für AWS Transfer Family](#)

Sicherheitsvorteile der VPC-Konnektivität

SFTP-Konnektoren mit VPC-Ausgangstyp bieten erweiterte Sicherheitsvorteile durch Cross-VPC Ressourcenzugriff:

- **Netzwerkisolierung:** Der gesamte Datenverkehr verbleibt in Ihrer VPC-Umgebung, sodass private Endpunktverbindungen vollständig vom öffentlichen Internet isoliert sind.
- **Quell-IP-Steuerung:** Remote-SFTP-Server sehen nur IP-Adressen aus Ihrem VPC-CIDR-Bereich, sodass Sie die volle Kontrolle über die für Verbindungen verwendeten Quell-IP-Adressen haben.
- **Privater Endpunktzugriff:** Stellen Sie über private IP-Adressen eine direkte Verbindung zu SFTP-Servern in Ihrer VPC her und vermeiden so die Gefährdung durch das öffentliche Internet.
- **Hybride Konnektivität:** Greifen Sie über etablierte VPN- oder Direct Connect-Verbindungen sicher auf lokale SFTP-Server zu, ohne dass Sie zusätzlich ins Internet gehen müssen.
- **VPC-Sicherheitskontrollen:** Nutzen Sie bestehende VPC-Sicherheitsgruppen, NACLs und Routing-Richtlinien, um den SFTP-Connector-Traffic zu kontrollieren und zu überwachen.

VPC Lattice-Sicherheitsmodell

Die VPC-Konnektivität für SFTP-Konnektoren verwendet AWS VPC Lattice mit Servicenetzwerken, um einen sicheren Mehrmandantenzugriff zu ermöglichen:

- Vermeidung unberechtigter Stellvertreter: Authentifizierungs- und Autorisierungsprüfungen stellen sicher, dass Konnektoren nur auf die spezifischen Ressourcen zugreifen können, für die sie konfiguriert sind, und verhindern so unbefugten mandantenübergreifenden Zugriff.
- IPv6-only Dienstnetzwerk: Nutzt IPv6-Adressierung, um potenzielle IP-Adresskonflikte zu vermeiden und die Sicherheitsisolierung zu verbessern.
- Forward Access Session (FAS): Durch die temporäre Verarbeitung von Anmeldeinformationen entfällt die Notwendigkeit einer langfristigen Speicherung von Anmeldeinformationen oder der manuellen gemeinsamen Nutzung von Ressourcen.
- Resource-level Zugriffskontrolle: Jeder Connector ist einer bestimmten Ressourcenkonfiguration zugeordnet, wodurch eine detaillierte Zugriffskontrolle auf einzelne SFTP-Server gewährleistet wird.

Bewährte Sicherheitsmethoden für VPC-Konnektivität

Beachten Sie bei der Verwendung von VPC-Ausgangsverbindern die folgenden bewährten Sicherheitsmethoden:

- Sicherheitsgruppen: Konfigurieren Sie Sicherheitsgruppen so, dass SFTP-Verkehr (Port 22) nur zwischen den erforderlichen Ressourcen zugelassen wird. Beschränken Sie die Quell- und Ziel-IP-Bereiche auf das erforderliche Minimum.
- Platzierung von Resource Gateways: Stellen Sie Resource Gateways nach Möglichkeit in privaten Subnetzen bereit und stellen Sie sicher, dass sie sich über mindestens zwei Availability Zones erstrecken, um eine hohe Verfügbarkeit zu gewährleisten.
- Netzwerküberwachung: Verwenden Sie VPC Flow Logs und Amazon CloudWatch , um Netzwerkverkehrsmuster zu überwachen und ungewöhnliche Aktivitäten zu erkennen.
- Zugriffsprotokollierung: Aktivieren Sie die Connector-Protokollierung, um Dateiübertragungsaktivitäten nachzuverfolgen und Prüfprotokolle für Compliance-Anforderungen zu führen.
- Verwaltung der Ressourcenkonfiguration: Überprüfen und aktualisieren Sie die Ressourcenkonfigurationen regelmäßig, um sicherzustellen, dass sie auf die richtigen SFTP-Server verweisen und die entsprechenden Netzwerkeinstellungen verwenden.

Sicherheitsrichtlinien für Server AWS Transfer Family

AWS Transfer Family Mithilfe der Serversicherheitsrichtlinien können Sie die Anzahl der mit Ihrem Server verknüpften kryptografischen Algorithmen (Message Authentication Codes (MACs), Key Exchanges (KEXs), Cipher Suites, Chiffren zur Inhaltsverschlüsselung und Hash-Algorithmen) einschränken.

AWS Transfer Family unterstützt Post-Quantum-Sicherheitsrichtlinien, die hybride Schlüsselaustauschalgorithmen verwenden und traditionelle kryptografische Methoden mit Post-Quanten-Algorithmen kombinieren, um mehr Sicherheit vor future Bedrohungen durch Quantencomputer zu bieten. Weitere Informationen finden Sie unter [Verwenden Sie den hybriden Schlüsselaustausch nach dem Quantum mit AWS Transfer Family](#).

Eine Liste der unterstützten kryptografischen Algorithmen finden Sie unter. [Kryptografische Algorithmen](#) Eine Liste der unterstützten Schlüsselalgorithmen für die Verwendung mit Serverhostschlüsseln und vom Dienst verwalteten Benutzerschlüsseln finden Sie unter. [Verwaltung von SSH- und PGP-Schlüsseln in Transfer Family](#)

Note

Ab 2025 beinhalten alle neuen AWS Transfer Family Sicherheitsrichtlinien kryptografische Unterstützung nach der Quantenumsetzung mithilfe hybrider Schlüsselaustauschalgorithmen. Weitere Informationen zur Post-Quantum-Sicherheit finden Sie unter. [Verwenden Sie den hybriden Schlüsselaustausch nach dem Quantum mit AWS Transfer Family](#)

Note

Wir empfehlen dringend, Ihre Server auf unsere neuesten Sicherheitsrichtlinien zu aktualisieren.

- `TransferSecurityPolicy-2024-01` ist die Standard-Sicherheitsrichtlinie, die Ihrem Server zugewiesen wird, wenn Sie einen Server mithilfe der Konsole, API oder CLI erstellen.
- Wenn Sie einen Transfer Family Family-Server mit der Standardsicherheitsrichtlinie erstellen CloudFormation und diese akzeptieren, wird der Server zugewiesen `TransferSecurityPolicy-2018-11`.

Wenn Sie Bedenken hinsichtlich der Client-Kompatibilität haben, geben Sie bitte ausdrücklich an, welche Sicherheitsrichtlinie Sie bei der Erstellung oder Aktualisierung eines Servers verwenden möchten, anstatt die Standardrichtlinie zu verwenden, die sich ändern kann. Informationen zum Ändern der Sicherheitsrichtlinie für einen Server finden Sie unter.

[Bearbeiten Sie die Sicherheitsrichtlinie](#)

 Note

Die früheren Versionen der Quantenrichtlinien (TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 und TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04) sind veraltet. Wir empfehlen, stattdessen die neuen Richtlinien zu verwenden.

Weitere Informationen zur Sicherheit in Transfer Family finden Sie in den folgenden Blogbeiträgen:

- [Sechs Tipps zur Verbesserung der Sicherheit Ihres AWS Transfer Family Servers](#)
- [Wie Transfer Family Ihnen helfen kann, eine sichere, konforme verwaltete Dateiübertragungslösung zu entwickeln](#)

Themen

- [Kryptografische Algorithmen](#)
- [Einzelheiten zur Sicherheitsrichtlinie](#)

Kryptografische Algorithmen

Für Hostschlüssel unterstützen wir die folgenden Algorithmen:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

- `ssh-ed25519`

Darüber hinaus ermöglichen die folgenden Sicherheitsrichtlinien `ssh-rsa`:

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`
- `TransferSecurityPolicy-FIPS-2023-05`
- `TransferSecurityPolicy-FIPS-2024-01`

 Note

Es ist wichtig, den Unterschied zwischen dem RSA-Schlüsseltyp — der immer gilt — `ssh-rsa` und dem RSA-Host-Schlüsselalgorithmus zu verstehen, bei dem es sich um einen der unterstützten Algorithmen handeln kann.

Im Folgenden finden Sie eine Liste der unterstützten kryptografischen Algorithmen für jede Sicherheitsrichtlinie.

 Note

Beachten Sie in der folgenden Tabelle und den Richtlinien die folgende Verwendung von Algorithmustypen.

- SFTP-Server verwenden nur Algorithmen in den `SshMacsAbschnitten` `SshCiphers` `SshKexs`, und.
- FTPS-Server verwenden in diesem Abschnitt nur Algorithmen. `TlsCiphers`
- FTP-Server verwenden keinen dieser Algorithmen, da sie keine Verschlüsselung verwenden.
- AS2-Server verwenden nur Algorithmen in den `HashAlgorithmsAbschnitten` `ContentEncryptionCiphers` und. In diesen Abschnitten werden Algorithmen definiert, die zum Verschlüsseln und Signieren von Dateiinhalten verwendet werden.
- Die Richtlinien `FIPS-2024-05` und die `FIPS-2024-01` Sicherheitsrichtlinien sind identisch, außer dass `FIPS-2024-05` sie den `ssh-rsa` Algorithmus nicht unterstützen.

- Transfer Family hat neue eingeschränkte Richtlinien eingeführt, die eng mit parallel bestehenden Richtlinien übereinstimmen:
 - Die Richtlinien TransferSecurityPolicy-Restricted-2018-11 und die TransferSecurityPolicy-2018-11 Sicherheitsrichtlinien sind identisch, mit der Ausnahme, dass die eingeschränkte Richtlinie die `chacha20-poly1305@openssh.com` Verschlüsselung nicht unterstützt.
 - Die Sicherheitsrichtlinien TransferSecurityPolicy-Restricted-2020-06 und die TransferSecurityPolicy-2020-06 Sicherheitsrichtlinien sind identisch, mit der Ausnahme, dass die eingeschränkte Richtlinie die `chacha20-poly1305@openssh.com` Verschlüsselung nicht unterstützt.

* In der folgenden Tabelle ist die chacha20-poly1305@openssh.com Chiffre nur in der Richtlinie ohne Einschränkungen enthalten.

Sicherheit srichtli nie	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo	SecurityPo
	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2024-01	licy-2024-01	licy-2023-05	licy-2023-05	licy-2022-06	licy-2020-06	licy-2020-06	licy-2018-11	licy-2018-11
	FIPS	SshA	AS2R	Restricted	FIPS	FIPS	FIPS	FIPS	-03	-06	FIPS	-11	-11
	-2025-08	ditCom	ed	ed	-2024-01/	-2023-05	-2023-05	-2023-05	und	und	-2020-06	und	und
		iant-2025-02	2025-07		TransferS				TransferS		TransferS		TransferS
					ecurityPo				ecurityPo		ecurityPo		ecurityPo
					licy-				licy-		licy-		licy-
					FIPS				Rest		Rest		Rest
					-2024-05				dicted-20		dicted-20		dicted-20

SshCiphers

The image displays two bar charts comparing the performance of two encryption methods: aes128-ctr and aes128-gcm. Both charts have a y-axis labeled 'Time' and an x-axis labeled 'Iterations'.

The top chart, titled 'aes128-ctr', shows 6 bars of varying heights. The bars are black with a white outline. The heights of the bars are approximately: 1.0, 1.5, 1.0, 1.0, 1.0, and 1.5. The x-axis is labeled 'Iterations' and the y-axis is labeled 'Time'.

The bottom chart, titled 'aes128-gcm', shows 12 bars of varying heights. The bars are black with a white outline. The heights of the bars are approximately: 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, and 1.0. The x-axis is labeled 'Iterations' and the y-axis is labeled 'Time'.

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-01	licy-2023-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-06	licy-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
chacha20-poly1305@openssh.com									◆*		◆*	
SshKexs												
mlkem768x25519-sha256	◆		◆									

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurityPo
nie	licy-2025-03	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01	licy-2025-01
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11	
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd	
			iant-2025-02	2025-07		TransferS				TransferS		TransferS	
						ecurityPo				ecurityPo		ecurityPo	
						licy-				licy-		licy-	
						FIPS				Rest		Rest	
						-2024-05				ricted-20		ricted-20	
										20-06		18-11	
mlkem768n	◆			◆									
nistp256-SHA256													
mlkem1024n	◆			◆									
nistp384-sha384													
Kurve 25519-sha256	◆		◆	◆	◆		◆		◆				◆
curve25519-sha256@libssh.org			◆	◆	◆		◆		◆				◆

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	SecurityPo
nie	licy-2025-03	licy-2025-03-FIPS	licy-2025-03-SshA	licy-2025-03-AS2R	licy-2024-01-01	licy-2024-01-01-FIPS	licy-2023-05-05	licy-2023-05-05-FIPS	licy-2023-06-03	licy-2020-06-06	licy-2020-06-06-FIPS	licy-2018-11-11	
		-2025-03-ditComes	-2025-07-02-stricted		-2024-01-01/TransferS		-2023-05-05-ecurityPo		-2023-05-05-ecurityPo	-2020-06-06-und	-2020-06-06-TransferS	-2018-11-11-TransferS	
					licy-2024-05-05-FIPS				-2023-05-05-ecurityPo	-2020-06-06-und	-2020-06-06-TransferS	-2018-11-11-TransferS	
										-2020-06-06-und	-2020-06-06-TransferS	-2018-11-11-TransferS	
diffie-													◆
he													
llman-													
gru													
ppe14-													
sha1													
diffie-										◆	◆	◆	
he													
llman-													
gru													
ppe-14-													
sh													
a256													
diffie-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
he													
llman-													
gru													
ppe-16-													
sh													
a512													

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-01	licy-2023-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-06	licy-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
diffie-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
he												
llman-												
gru												
ppe-18-												
sh												
a512												
Diffie-	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆
He												
llman-												
Gru												
ppenausta												
usch-												
SHA2												
56												
ecdh-	◆	◆		◆	◆	◆				◆	◆	◆
sha2												
-												
nistp256												

Sicherheit	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
tsrichtli	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
nie	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03	licy-2025-03
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11	
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd	
			iant-2025-02	2025-07		TransferS				TransferS		TransferS	
						ecurityPo				ecurityPo		ecurityPo	
						licy-				licy-		licy-	
						FIPS				Rest		Rest	
						-2024-05				ricted-20		ricted-20	
										20-06		18-11	
ecdh-	◆	◆		◆	◆	◆				◆	◆	◆	
sha2													
-													
nistp384													
ecdh-	◆	◆		◆	◆	◆				◆	◆	◆	
sha2													
-													
nistp521													
SshMacs													
hmac-												◆	
sha1													
hmac-												◆	
sha1													
-													
etm@open													
ssh.com													
hmac-								◆	◆	◆	◆		
sha2													
-256													

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-01	licy-2023-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-06	licy-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512									◆	◆	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com										◆		◆
umac-128@openssh.com										◆		◆

Sicherheit	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
tsrichtli	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-11	licy-2018-11	licy-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	restricted		-2024-01/		-2023-05		und	-2020-06	nd
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
umac-64-												◆
e												
tm@openss												
h.com												
umac-64@o												◆
pensssh.co												
m												
Content	Encryption	Ciphers										
aes256-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
aes192-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
aes128-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
3des-	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
cbc												
Hash	Algorithms											
sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Sicherheit	Transfer Policy-2025-03	Transfer Policy-2025-08	Transfer Policy-2025-08	Transfer Policy-2025-07	Transfer Policy-2024-01	Transfer Policy-2024-05	Transfer Policy-2023-05	Transfer Policy-2023-06	Transfer Policy-2020-06	Transfer Policy-2020-11	Transfer Policy-2018-11
tsrichtli	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity	ecurity
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-11	licy-2018-11
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TlsCiphers											
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Sicherheit	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
tsrichtli	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
nie	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-05	licy-2023-05	licy-2023-05	licy-2023-06	licy-2020-06	licy-2020-11	licy-2018-11
		FIPS	SshA	AS2R		FIPS		FIPS			FIPS	
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		und	-2020-06	nd
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
_ECDSA_WITH												
AES_256_GCM_SHA												
384												
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
_RSA_WITH												
AES_128_CBC_SHA256												
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
_RSA_WITH												
AES_128_GCM_SHA256												
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
_RSA_WITH												
AES_256_CBC_SHA384												

Sicherheitsrichtlinie	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-09	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2022-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		FIPS	SshA	AS2R		FIPS	FIPS	FIPS		FIPS	
		-2025-08	ditCom	stricted		-2024-01/	-2023-05		-06	-2020-06	
			iant-2025-02	2025-07		TransferSecurityPolicy-			TransferSecurityPolicy-	TransferSecurityPolicy-	
						FIPS			Rest	Rest	
						-2024-05			ricted-20	ricted-20	
									20-06	18-11	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256										◆	
TLS_RSA_WITH_AES_128_CBC_SHA256										◆	

Einzelheiten zur Sicherheitsrichtlinie

Die folgenden Abschnitte enthalten die JSON-Darstellung der einzelnen Sicherheitsrichtlinien.

TransferSecurityPolicy-2025-03

Im Folgenden wird die TransferSecurityPolicy-2025-03 Sicherheitsrichtlinie dargestellt.

```
{
  "SecurityPolicy": {
```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2025-03",
"SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2025-03

Im Folgenden wird die TransferSecurityPolicy-FIPS-2025-03 Sicherheitsrichtlinie dargestellt.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [

```



```

        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Diese Sicherheitsrichtlinie wurde für AS2-Dateiübertragungen entwickelt, die eine erhöhte Sicherheit erfordern, indem ältere kryptografische Algorithmen ausgeschlossen werden. Sie unterstützt moderne AES-Verschlüsselung und SHA-2 Hash-Algorithmen und entfernt gleichzeitig die Unterstützung für schwächere Algorithmen wie 3DES und SHA-1.

Note

Diese Sicherheitsrichtlinie ist identisch mit TransferSecurityPolicy-2025-03, außer dass sie 3DES (in ContentEncryptionCiphers) und SHA1 (in HashAlgorithms) nicht unterstützt.

umfasst alle Algorithmen aus dem Zeitraum 2025-03, einschließlich kryptografischer Post-Quantum-Algorithmen (mlkem* KEXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512"
    ],
    "TlsCiphers": [
```

```

        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

Im Folgenden wird die TransferSecurityPolicy-SshAuditCompliant-2025-02 Sicherheitsrichtlinie dargestellt.

Note

Diese Sicherheitsrichtlinie basiert auf den Empfehlungen des ssh-audit Tools und entspricht zu 100% dem Tool.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ]
  }
}

```

```

],
"SshKexs": [
  "curve25519-sha256",
  "curve25519-sha256@libssh.org",
  "diffie-hellman-group18-sha512",
  "diffie-hellman-group16-sha512",
  "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
  "hmac-sha2-256-etm@openssh.com",
  "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
  "aes256-cbc",
  "aes192-cbc",
  "aes128-cbc",
  "3des-cbc"
],
"HashAlgorithms": [
  "sha256",
  "sha384",
  "sha512",
  "sha1"
],
"TlsCiphers": [
  "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
  "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
  "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
  "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
  "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
  "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
  "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
],
"Type": "SERVER"
}
}

```

TransferSecurityPolicy-2024-01

Im Folgenden wird die TransferSecurityPolicy-2024-01 Sicherheitsrichtlinie dargestellt.

```
{
```

```
"SecurityPolicy": {
  "Fips": false,
  "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
  "SshCiphers": [
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
  ],
  "SshKexs": [
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group-exchange-sha256"
  ],
  "SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

Im Folgenden werden die Sicherheitsrichtlinien TransferSecurityPolicy-FIPS-2024-01 und die TransferSecurityPolicy-FIPS-2024-05 Sicherheitsrichtlinien aufgeführt.

Note

Der FIPS-Dienstendpunkt TransferSecurityPolicy-FIPS-2024-01 und die TransferSecurityPolicy-FIPS-2024-05 Sicherheitsrichtlinien sind nur in einigen AWS Regionen verfügbar. Weitere Informationen finden Sie unter [AWS Transfer Family -Endpunkte und -Kontingente](#) in der Allgemeine AWS-Referenz.

Der einzige Unterschied zwischen diesen beiden Sicherheitsrichtlinien besteht darin, dass der `ssh-rsa` Algorithmus TransferSecurityPolicy-FIPS-2024-01 unterstützt wird und TransferSecurityPolicy-FIPS-2024-05 nicht.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [

```

```

        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

Im Folgenden wird die TransferSecurityPolicy-2023-05 Sicherheitsrichtlinie dargestellt.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [

```

```

        "curve25519-sha256",
        "curve25519-sha256@libssh.org",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

Die Einzelheiten zur FIPS-Zertifizierung für AWS Transfer Family finden Sie unter <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Im Folgenden werden die TransferSecurityPolicy-FIPS-2023-05 Sicherheitsrichtlinien dargestellt.

 Note

Der FIPS-Dienstendpunkt und die TransferSecurityPolicy-FIPS-2023-05 Sicherheitsrichtlinie sind nur in einigen AWS Regionen verfügbar. Weitere Informationen finden Sie unter [AWS Transfer Family -Endpunkte und -Kontingente](#) in der Allgemeine AWS-Referenz.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
```

```

        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-2022-03

Im Folgenden wird die TransferSecurityPolicy-2022-03 Sicherheitsrichtlinie dargestellt.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [

```

```

    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}

```

TransferSecurityPolicy-2020-06 und TransferSecurityPolicy-Restricted-2020-06

Im Folgenden wird die TransferSecurityPolicy-2020-06 Sicherheitsrichtlinie dargestellt.

Note

Die TransferSecurityPolicy-2020-06 Sicherheitsrichtlinien TransferSecurityPolicy-Restricted-2020-06 und die Sicherheitsrichtlinien sind identisch, mit der Ausnahme, dass die eingeschränkte Richtlinie die `chacha20-poly1305@openssh.com` Verschlüsselung nicht unterstützt.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ]
  }
}

```

```

],
"SshKexs": [
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256"
],
"SshMacs": [
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
]
}
}

```

TransferSecurityPolicy-FIPS-2020-06

Die Einzelheiten zur FIPS-Zertifizierung für AWS Transfer Family finden Sie unter <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Im Folgenden werden die TransferSecurityPolicy-FIPS-2020-06 Sicherheitsrichtlinien dargestellt.

Note

Der FIPS-Dienstendpunkt und die TransferSecurityPolicy-FIPS-2020-06 Sicherheitsrichtlinie sind nur in einigen AWS Regionen verfügbar. Weitere Informationen finden Sie unter [AWS Transfer Family -Endpunkte und -Kontingente](#) in der Allgemeine AWS-Referenz.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
```

```

    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2018-11 und TransferSecurityPolicy-Restricted-2018-11

Im Folgenden wird die TransferSecurityPolicy-2018-11 Sicherheitsrichtlinie dargestellt.

Note

Die TransferSecurityPolicy-2018-11 Sicherheitsrichtlinien TransferSecurityPolicy-Restricted-2018-11 und die Sicherheitsrichtlinien sind identisch, mit der Ausnahme, dass die eingeschränkte Richtlinie die `chacha20-poly1305@openssh.com` Verschlüsselung nicht unterstützt.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
      Restricted-2018-11
    ]
  }
}

```

```
    "aes128-ctr",
    "aes192-ctr",
    "aes256-ctr",
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com"
  ],
  "SshKexs": [
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256",
    "diffie-hellman-group14-sha1"
  ],
  "SshMacs": [
    "umac-64-etm@openssh.com",
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha1-etm@openssh.com",
    "umac-64@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512",
    "hmac-sha1"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
```

```

    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256"
  ]
}
}

```

Sicherheitsrichtlinien für SFTP-Konnektoren AWS Transfer Family

Mit den Sicherheitsrichtlinien für den SFTP-Connector AWS Transfer Family können Sie die Anzahl der mit Ihrem SFTP-Connector verknüpften kryptografischen Algorithmen (Message Authentication Codes (MACs), Key Exchanges (KEXs) und Cipher Suites) einschränken. Im Folgenden finden Sie eine Liste der unterstützten kryptografischen Algorithmen für jede Sicherheitsrichtlinie für den SFTP-Connector.

Note

`TransferSFTPConnectorSecurityPolicy-2024-03` ist die Standardsicherheitsrichtlinie, die auf SFTP-Konnektoren angewendet wird.

Sie können die Sicherheitsrichtlinie für Ihren Connector ändern. Wählen Sie im linken Navigationsbereich der Transfer Family die Option Connectors und wählen Sie Ihren Connector aus. Wählen Sie dann im Abschnitt SFTP-Konfiguration die Option Bearbeiten aus. Wählen Sie im Abschnitt Optionen für kryptografische Algorithmen eine beliebige verfügbare Sicherheitsrichtlinie aus der Dropdownliste im Feld Sicherheitsrichtlinie aus.

Kryptografische Algorithmen

Für Hostschlüssel unterstützen SFTP-Konnektoren alle Algorithmen, die für Transfer Family Family-Server unterstützt werden, mit Ausnahme von `ed25519`:

- `rsa-sha2-256`

- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Darüber hinaus unterstützen wir Hostschlüsselssh-`rsa`, aber nur für `TransferSFTPConnectorSecurityPolicy-2023-07`

Für die Authentifizierung unterstützen SFTP-Konnektoren die folgenden Schlüsseltypen:

- `ssh-rsa`
- `ecdsa`

Einzelheiten zur Sicherheitsrichtlinie für den SFTP-Connector

Die folgende Tabelle zeigt die spezifischen kryptografischen Algorithmen, die von den einzelnen Sicherheitsrichtlinien für den SFTP-Connector unterstützt werden.

Sicherheitsrichtlinie	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Ciphers			
<code>aes128-ctr</code>			◆
<code>aes128-gcm@openssh.com</code>	◆	◆	◆
<code>aes192-ctr</code>		◆	◆
<code>aes256-ctr</code>		◆	◆
<code>aes256-gcm@openssh.com</code>	◆	◆	◆
Kexs			

Sicherheitsrichtlinie	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Kurve 25519-sha256		◆	◆
curve25519-sha256@libssh.org		◆	◆
diffie-hellman-gruppel4-sha1			◆
diffie-hellman-gruppel-16-sha512		◆	◆
diffie-hellman-gruppel-18-sha512		◆	◆
Diffie-Hellman-Gruppenaustausch-SHA256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆

Sicherheitsrichtlinie	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
hmac-sha-196			◆
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

Verwenden Sie den hybriden Schlüsselaustausch nach dem Quantum mit AWS Transfer Family

Transfer Family unterstützt eine hybride Option zur Einrichtung von Post-Quantum-Schlüsseln für das Secure Shell (SSH) -Protokoll. Post-quantum Die Einrichtung eines Schlüssels ist erforderlich, da es bereits möglich ist, den Netzwerkverkehr aufzuzeichnen und für die future Entschlüsselung durch einen Quantencomputer zu speichern, was als Store-Now-Harvest-Later-Attacke bezeichnet wird.

Sie können diese Option verwenden, wenn Sie eine Verbindung zu Transfer Family herstellen, um sichere Dateiübertragungen in und aus dem Amazon Simple Storage Service (Amazon S3) -Speicher oder Amazon Elastic File System (Amazon EFS) durchzuführen. Post-quantum Die hybride Schlüsseletablierung in SSH führt Mechanismen zur Einrichtung von Schlüsseln ein, die erst nach dem Quantenverfahren eingerichtet wurden. Diese werden in Verbindung mit klassischen Schlüsselaustauschalgorithmus verwendet. SSH-Schlüssel, die mit klassischen Verschlüsselungssammlungen erstellt wurden, sind mit der aktuellen Technologie vor Brute-Force-Angriffen geschützt. Es wird jedoch nicht erwartet, dass die klassische Verschlüsselung nach dem Aufkommen von Quantencomputern in future sicher bleibt.

Wenn Ihr Unternehmen auf die langfristige Vertraulichkeit von Daten angewiesen ist, die über eine Transfer Family Family-Verbindung übertragen werden, sollten Sie einen Plan zur Umstellung auf Post-Quanten-Kryptografie in Betracht ziehen, bevor große Quantencomputer für den Einsatz verfügbar sind.

Um heute verschlüsselte Daten vor möglichen future Angriffen zu schützen, beteiligt AWS sich die Kryptografie-Community an der Entwicklung quantenresistenter oder Post-Quanten-Algorithmen. Wir haben in Transfer Family hybride Verschlüsselungssuiten für den Schlüsselaustausch nach dem Quantenaustausch implementiert, die klassische Elemente und Post-Quantum-Elemente kombinieren.

Diese hybriden Verschlüsselungssammlungen sind in den meisten Regionen für den Einsatz auf Ihren Produktions-Workloads verfügbar. AWS Da sich die Leistungsmerkmale und Bandbreitenanforderungen von Hybrid-Cipher Suites jedoch von denen klassischer Schlüsselaustauschmechanismen unterscheiden, empfehlen wir, sie auf Ihren Transfer Family Family-Verbindungen zu testen.

Weitere Informationen zur Post-Quanten-Kryptografie finden Sie im Blogbeitrag [Post-QuantumCryptography](#) Security.

Inhalt

- [Informationen zum hybriden Schlüsselaustausch in SSH nach der Quantenphase](#)
- [So funktioniert die Etablierung hybrider Schlüssel nach der Quantenentwicklung in Transfer Family](#)
 - [Warum? ML-KEM](#)
 - [Post-quantum hybrider SSH-Schlüsselaustausch und kryptografische Anforderungen \(FIPS 140\)](#)
- [Testen des hybriden Schlüsselaustauschs nach dem Quantenprozess in der Transfer Family](#)
 - [Aktivieren Sie den hybriden Schlüsselaustausch nach dem Quantum-Verfahren auf Ihrem SFTP-Endpunkt](#)
 - [Richten Sie einen SFTP-Client ein, der den hybriden Schlüsselaustausch nach dem Quantum-Verfahren unterstützt](#)
 - [Bestätigen Sie den Hybrid-Schlüsselaustausch nach der Quantum-Implementierung in SFTP](#)

Informationen zum hybriden Schlüsselaustausch in SSH nach der Quantenphase

Transfer Family unterstützt Post-Quantum-Hybrid-Schlüsselaustausch-Verschlüsselungssuiten, die sowohl den klassischen [Elliptic Curve Diffie-Hellman \(ECDH\)](#) -Schlüsselaustauschalgorithmus verwenden, als auch. ML-KEM ML-KEM ist ein Algorithmus zur Verschlüsselung und Einrichtung von Schlüsseln nach dem Quantenprozess, den das [National Institute for Standards and Technology \(NIST\) als seinen ersten Standardalgorithmus für](#) die Zeit nach der Quantenschlüsselvereinbarung bezeichnet hat.

Der Client und der Server führen weiterhin einen ECDH-Schlüsselaustausch durch. Darüber hinaus kapselt der Server einen gemeinsamen geheimen Schlüssel für die Zeit nach dem Quantum in den öffentlichen KEM-Schlüssel des Clients ein, der in der SSH-Schlüsselaustauschnachricht des Clients angekündigt wird. Diese Strategie kombiniert die hohe Sicherheit eines klassischen Schlüsselaustauschs mit der Sicherheit des geplanten Schlüsselaustauschs nach dem Quantenaustausch, um sicherzustellen, dass die Handshakes geschützt sind, solange das ECDH oder das gemeinsame geheime Post-Quantum-Geheimnis nicht geknackt werden können.

So funktioniert die Etablierung hybrider Schlüssel nach der Quantenentwicklung in Transfer Family

AWS hat kürzlich die Unterstützung für den Austausch von Schlüsseln nach dem Quantenzugriff bei SFTP-Dateiübertragungen in angekündigt. AWS Transfer Family Transfer Family skaliert sichere Dateiübertragungen von Unternehmen zu AWS Speicherdiensten mithilfe von SFTP und anderen Protokollen. SFTP ist eine sicherere Version des File Transfer Protocol (FTP), das über SSH ausgeführt wird. Die Unterstützung von Transfer Family nach dem Quanten-Schlüsselaustausch legt die Sicherheitslatte für Datenübertragungen über SFTP höher.

Die SFTP-Unterstützung für den Post-Quantum-Hybrid-Schlüsselaustausch in der Transfer Family umfasst die Kombination von Post-Quanten-Algorithmen und mit ECDH über P256- ML-KEM-768 ML-KEM-1024, P384- oder Curve25519-Kurven. [Die folgenden entsprechenden Methoden für den SSH-Schlüsselaustausch sind im Entwurf für den Austausch von SSH-Schlüsseln nach dem Quanten-Hybrid-Verfahren spezifiziert.](#)

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

Warum? ML-KEM

AWS setzt sich für die Unterstützung standardisierter, interoperabler Algorithmen ein. ML-KEM ist der einzige Algorithmus für den Schlüsselaustausch nach dem Quantenaustausch, der vom [NIST Post-Quantum](#) Cryptography Project standardisiert und genehmigt wurde. Normungsgremien sind bereits dabei, sich in Protokolle zu integrieren ML-KEM . AWS unterstützt ML-KEM TLS bereits auf einigen AWS API-Endpunkten.

Im Rahmen dieser Verpflichtung AWS hat das Unternehmen der IETF einen Vorschlagsentwurf für Post-Quanten-Kryptografie vorgelegt, der ML-KEM mit NIST-approved Kurven wie P256 für SSH kombiniert wird. Um die Sicherheit für unsere Kunden zu verbessern, folgt die AWS Implementierung des Post-Quantum-Schlüsselaustauschs in SFTP und SSH diesem Entwurf. Wir planen, future Aktualisierungen zu unterstützen, bis unser Vorschlag von der IETF angenommen wird und ein Standard wird.

Die neuen Schlüsselaustauschmethoden (im Abschnitt aufgeführt [So funktioniert die Etablierung hybrider Schlüssel nach der Quantenentwicklung in Transfer Family](#)) könnten sich ändern, wenn sich der Entwurf in Richtung Standardisierung weiterentwickelt.

Note

Post-quantum Algorithmusunterstützung ist derzeit für den hybriden Schlüsselaustausch nach dem Quantenprozess in TLS für AWS KMS (siehe [Verwenden von hybridem Post-Quantum-TLS mit AWS KMS](#)) und API-Endpunkten AWS Certificate Manager verfügbar. AWS Secrets Manager

Post-quantum hybrider SSH-Schlüsselaustausch und kryptografische Anforderungen (FIPS 140)

Für Kunden, die FIPS-Konformität benötigen, bietet Transfer Family FIPS-approved Kryptografie in SSH mithilfe der AWS FIPS 140-zertifizierten Open-Source-Kryptografiebibliothek -LC. AWS Die in Transfer Family unterstützten Methoden für den hybriden Schlüsselaustausch nach dem TransferSecurityPolicy-FIPS-2025-03 Quantenverfahren sind gemäß [SP 800-56Cr2 von NIST](#) (Abschnitt 2) FIPS-zugelassen. Das deutsche Bundesamt für Sicherheit in der Informationstechnik ([BSI](#)) und die Frankreich Agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) empfehlen ebenfalls solche Methoden für den hybriden Schlüsselaustausch nach dem Quantenverfahren.

Testen des hybriden Schlüsselaustauschs nach dem Quantenprozess in der Transfer Family

In diesem Abschnitt werden die Schritte beschrieben, die Sie unternehmen, um den hybriden Schlüsselaustausch nach dem Quantenverfahren zu testen.

1. [Aktivieren Sie den hybriden Schlüsselaustausch nach dem Quantum-Verfahren auf Ihrem SFTP-Endpunkt.](#)
2. Verwenden Sie einen SFTP-Client (z. B. [Richten Sie einen SFTP-Client ein, der den hybriden Schlüsselaustausch nach dem Quantum-Verfahren unterstützt](#)), der den hybriden Schlüsselaustausch nach dem Quantenverfahren unterstützt, und folgen Sie dabei den Anweisungen im oben genannten Spezifikationsentwurf.
3. Übertragen Sie eine Datei mit einem Transfer Family Family-Server.
4. [Bestätigen Sie den Hybrid-Schlüsselaustausch nach der Quantum-Implementierung in SFTP.](#)

Aktivieren Sie den hybriden Schlüsselaustausch nach dem Quantum-Verfahren auf Ihrem SFTP-Endpunkt

Sie können die SSH-Richtlinie auswählen, wenn Sie einen neuen SFTP-Serverendpunkt in Transfer Family erstellen, oder indem Sie die Optionen für den kryptografischen Algorithmus in einem vorhandenen SFTP-Endpunkt bearbeiten. Der folgende Snapshot zeigt ein Beispiel dafür, AWS-Managementkonsole wo Sie die SSH-Richtlinie aktualisieren.

Cryptographic algorithm options Info

Security Policy

Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 ▲

TransferSecurityPolicy-2018-11
TransferSecurityPolicy-2020-06
TransferSecurityPolicy-2022-03
TransferSecurityPolicy-2023-05
TransferSecurityPolicy-2024-01
TransferSecurityPolicy-2025-03 ✓
TransferSecurityPolicy-Restricted-2018-11
TransferSecurityPolicy-Restricted-2020-06

to it. Additi

Die SSH-Richtliniennamen, die den Schlüsselaustausch nach dem Quantenvorgang unterstützen, lauten und. TransferSecurityPolicy-2025-03 TransferSecurityPolicy-FIPS-2025-03 Weitere Informationen zu den Richtlinien von Transfer Family finden Sie unter [Sicherheitsrichtlinien für Server AWS Transfer Family](#).

Richten Sie einen SFTP-Client ein, der den hybriden Schlüsselaustausch nach dem Quantum-Verfahren unterstützt

Nachdem Sie die richtige Post-Quantum-SSH-Richtlinie in Ihrem SFTP Transfer Family-Endpunkt ausgewählt haben, können Sie in Transfer Family mit Post-Quantum-SFTP experimentieren. Installieren Sie zum Testen den neuesten OpenSSH-Client (z. B. Version 9.9) auf Ihrem lokalen System.

Note

Stellen Sie sicher, dass Ihr Client einen oder mehrere der oben aufgeführten ML-KEM Algorithmen unterstützt. Sie können die unterstützten Algorithmen für Ihre Version von OpenSSH anzeigen, indem Sie diesen Befehl ausführen: `ssh -Q kex`

Sie können den Beispiel-SFTP-Client ausführen, um eine Verbindung zu Ihrem SFTP-Endpunkt herzustellen (z. B. `s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`), indem Sie die Post-Quantum-Methoden für den hybriden Schlüsselaustausch verwenden, wie im folgenden Befehl gezeigt.

```
sftp -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

Ersetzen Sie im vorherigen Befehl die folgenden Elemente durch Ihre eigenen Informationen:

- *username_private_key_PEM_file* Ersetzen Sie durch die private PEM-encoded Schlüsseldatei des SFTP-Benutzers
- Ersetzen Sie es *username* durch den SFTP-Benutzernamen
- *server-id* Durch die Transfer Family Family-Server-ID ersetzen
- *region-id* Ersetzen Sie durch die tatsächliche Region, in der sich Ihr Transfer Family Family-Server befindet

Bestätigen Sie den Hybrid-Schlüsselaustausch nach der Quantum-Implementierung in SFTP

Überprüfen Sie die Client-Ausgabe, um sicherzustellen, dass der hybride Schlüsselaustausch nach dem Quantenverfahren während einer SSH-Verbindung für SFTP zu Transfer Family verwendet wurde. Optional können Sie ein Programm zur Paketerfassung verwenden. Wenn Sie den OpenSSH 9.9-Client verwenden, sollte die Ausgabe etwa wie folgt aussehen (wobei der Kürze halber irrelevante Informationen weggelassen werden):

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
```

```
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or
  directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
  compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
  compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
  ([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

Die Ausgabe zeigt, dass die Client-Verhandlung mithilfe der mlkem768x25519-sha256 Post-Quantum-Hybridmethode stattgefunden hat und erfolgreich eine SFTP-Sitzung eingerichtet wurde.

Datenschutz und Verschlüsselung

Das AWS [Modell](#) der mit gilt für den Datenschutz in AWS Transfer Family (Transfer Family). Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der die gesamte AWS Cloud betrieben wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in

dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für die AWS Dienste, die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im AWS Sicherheitsblog im [Modell der AWS gemeinsamen Verantwortung](#) und im [DSGVO-Blogbeitrag](#).

Aus Datenschutzgründen empfehlen wir Ihnen, Ihre AWS Kontoanmeldeinformationen zu schützen und individuelle Benutzerkonten mit einzurichten AWS IAM Identity Center. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir unterstützen TLS 1.2.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über 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 wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mit Transfer Family oder anderen AWS Diensten über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Konfigurationsdaten, die Sie in die Transfer Family Family-Dienstkonfiguration oder in die Konfigurationen anderer Dienste eingeben, werden möglicherweise zur Aufnahme in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Im Gegensatz dazu werden Daten aus Upload- und Download-Vorgängen zu und von Transfer Family Family-Servern als vollständig privat behandelt und existieren nie außerhalb verschlüsselter Kanäle, wie z. B. einer SFTP- oder FTPS-Verbindung. Diese Daten sind immer nur autorisierten Personen zugänglich.

Datenverschlüsselung in Transfer Family

AWS Transfer Family verwendet die Standardverschlüsselungsoptionen, die Sie für Ihren Amazon S3 S3-Bucket festgelegt haben, um Ihre Daten zu verschlüsseln. Wenn Sie die Standardverschlüsselung für einen Bucket aktivieren, werden alle Objekte verschlüsselt, wenn sie im Bucket gespeichert werden. Die Objekte werden mithilfe serverseitiger Verschlüsselung mit entweder von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder AWS Key Management Service (AWS KMS) verwalteten Schlüsseln (SSE-KMS) verschlüsselt. Informationen zur serverseitigen Verschlüsselung finden Sie unter [Schützen von Daten mithilfe serverseitiger Verschlüsselung](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Die folgenden Schritte zeigen Ihnen, wie Sie Daten in verschlüsseln. AWS Transfer Family

Um die Verschlüsselung in zuzulassen AWS Transfer Family

1. Aktivieren Sie die Standardverschlüsselung für Ihren Amazon S3 S3-Bucket. Anweisungen finden Sie unter [Amazon S3 S3-Standardverschlüsselung für S3-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.
2. Aktualisieren Sie die AWS Identity and Access Management (IAM) -Rollenrichtlinie, die dem Benutzer zugewiesen ist, um die erforderlichen AWS Key Management Service (AWS KMS) Berechtigungen zu gewähren.
3. Wenn Sie eine Sitzungsrichtlinie für den Benutzer verwenden, muss die Sitzungsrichtlinie die erforderlichen AWS KMS Berechtigungen gewähren.

Das folgende Beispiel zeigt eine IAM-Richtlinie, die die Mindestberechtigungen gewährt, die bei der Verwendung AWS Transfer Family mit einem Amazon S3 S3-Bucket erforderlich sind, der für die AWS KMS Verschlüsselung aktiviert ist. Nehmen Sie diese Beispielrichtlinie sowohl in die Benutzer-IAM-Rollenrichtlinie als auch in die Sitzungsrichtlinie auf, falls Sie eine verwenden.

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:GetPublicKey",
    "kms:ListKeyPolicies"
  ],
  "Effect": "Allow",
```

```
"Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

Die KMS-Schlüssel-ID, die Sie in dieser Richtlinie angeben, muss mit der in Schritt 1 für die Standardverschlüsselung angegebenen identisch sein.

Root oder die IAM-Rolle, die für den Benutzer verwendet wird, muss in der AWS KMS Schlüsselrichtlinie zulässig sein. Informationen zur AWS KMS Schlüsselrichtlinie finden Sie unter [Verwenden von Schlüsselrichtlinien in AWS KMS](#) im AWS Key Management Service Entwicklerhandbuch.

AWS Transfer Family Verschlüsselung im Ruhezustand

Da AWS Transfer Family es sich um einen Dateiübertragungsdienst handelt, werden Ihre Speicherdaten im Ruhezustand nicht verwaltet. Die Speicherdienste und -systeme, die AWS Transfer Family unterstützt werden, sind für den Schutz der Daten in diesem Zustand verantwortlich. Es gibt jedoch einige dienstbezogene Daten, die im Ruhezustand AWS Transfer Family verwaltet werden.

Was ist verschlüsselt?

Die einzigen Daten, die im Ruhezustand AWS Transfer Family verarbeitet werden, beziehen sich auf die Details, die für den Betrieb Ihrer Dateiübertragungsserver und die Verarbeitung von Übertragungen erforderlich sind. AWS Transfer Family speichert die folgenden Daten mit vollständiger Verschlüsselung im Ruhezustand in Amazon DynamoDB:

- Serverkonfigurationen (z. B. Servereinstellungen, Protokollkonfigurationen und Endpunktdetails).
- Benutzerauthentifizierungsdaten, einschließlich öffentlicher SSH-Schlüssel und Benutzermetadaten.
- Einzelheiten zur Workflow-Ausführung und Schrittkonfigurationen.
- Konnektorkonfigurationen und Authentifizierungsdaten für Systeme von Drittanbietern. Diese Anmeldeinformationen werden mit AWS Transfer Family verwalteten Verschlüsselungsschlüsseln verschlüsselt.

Schlüsselverwaltung

Sie können die Verschlüsselungsschlüssel nicht verwalten, die zum Speichern von Informationen in DynamoDB AWS Transfer Family verwendet werden, die sich auf den Betrieb Ihrer Server und die Verarbeitung von Übertragungen beziehen. Zu diesen Informationen gehören Ihre Serverkonfigurationen, Benutzerauthentifizierungsdaten, Workflow-Details und Connector-Anmeldeinformationen.

Was ist nicht verschlüsselt?

AWS Transfer Family Es hat zwar keine Kontrolle darüber, wie Ihre Speicherdaten im Ruhezustand verschlüsselt werden, wir empfehlen jedoch, Ihre Speicherorte mit der höchsten Sicherheitsstufe zu konfigurieren, die sie unterstützen. Sie können Objekte beispielsweise mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) oder Schlüsseln () AWS KMS verschlüsseln. SSE-KMS

Erfahren Sie mehr darüber, wie AWS Speicherdienste Daten im Ruhezustand verschlüsseln:

- [Amazon S3](#)
- [Amazon EFS](#)

Verwaltung von SSH- und PGP-Schlüsseln in Transfer Family

In diesem Abschnitt finden Sie Informationen zu SSH-Schlüsseln, einschließlich deren Generierung und Rotation. Einzelheiten zur Verwendung von Transfer Family with AWS Lambda zur Schlüsselverwaltung finden Sie im Blogbeitrag [Aktivieren der Self-Service-Schlüsselverwaltung für Benutzer mit AWS Transfer Family und AWS Lambda](#). Informationen zur automatisierten Bereitstellung und Verwaltung von Benutzern mit mehreren SSH-Schlüsseln finden Sie unter [Terraform-Module der Transfer Family](#)

Note

AWS Transfer Family akzeptiert RSA-, ECDSA- und ED25519-Schlüssel für die SSH-Authentifizierung.

In diesem Abschnitt wird auch beschrieben, wie Sie Pretty Good Privacy (PGP) -Schlüssel generieren und verwalten.

Einen umfassenden Überblick über alle unterstützten Verschlüsselungs- und Schlüsselalgorithmen, einschließlich Empfehlungen für verschiedene Anwendungsfälle, finden Sie unter [Überblick über Verschlüsselung und Schlüsselalgorithmen](#).

Überblick über Verschlüsselung und Schlüsselalgorithmen

AWS Transfer Family unterstützt verschiedene Arten von Algorithmen für unterschiedliche Zwecke. Wenn Sie wissen, welche Algorithmen für Ihren speziellen Anwendungsfall verwendet werden sollten, können Sie sichere und kompatible Dateiübertragungen gewährleisten.

Kurzreferenz zum Algorithmus

Anwendungsfall	Empfohlener Algorithmus	FIPS-konform	Hinweise
SSH/SFTP Authentifizierung	RSA (rsa-sha2-256/512), ECDSA oder ED25519	RSA: Ja, ECDSA: Ja, ED25519: Nein	Kompatibel mit allen SSH-Clients und -Servern
Generierung von PGP-Schlüsseln	RSA oder ECC (NIST)	Ja	Für die Workflow-Entschlüsselung
PGP-Dateiverschlüsselung	AES-256	Ja	Ermittelt durch die PGP-Software

SSH-Authentifizierungsalgorithmen

Diese Algorithmen werden für die SSH/SFTP Authentifizierung zwischen Clients und AWS Transfer Family Servern verwendet. Wählen Sie eines davon aus, wenn Sie SSH-Schlüsselpaare für die Benutzerauthentifizierung oder Server-Hostschlüssel generieren.

RSA (empfohlen)

Kompatibel mit allen SSH-Clients und -Servern und. FIPS-compliant Zur Erhöhung der Sicherheit zusammen mit SHA-2 Hashing verwenden:

- `rsa-sha2-256`- Für die meisten Anwendungsfälle empfohlen

- `rsa-sha2-512`- Höhere Sicherheitsoption

ED25519

Modern und effizient. Kleinere Schlüsselgrößen mit hoher Sicherheit:

- `ssh-ed25519`- Schnell und sicher, aber nicht FIPS-compliant

ECDSA

Option mit elliptischer Kurve. Gute Balance zwischen Sicherheit und Leistung:

- `ecdsa-sha2-nistp256`- Standardkurve
- `ecdsa-sha2-nistp384`- Höhere Sicherheitskurve
- `ecdsa-sha2-nistp521`- Höchste Sicherheitskurve

Note

Wir unterstützen ältere Sicherheitsrichtlinien `ssh-rsa` mit SHA1. Details hierzu finden Sie unter [Kryptografische Algorithmen](#).

Den richtigen SSH-Algorithmus auswählen

- Für die meisten Benutzer: Verwenden Sie RSA mit oder `rsa-sha2-256` `rsa-sha2-512`
- Für FIPS-Konformität: Verwenden Sie RSA- oder ECDSA-Algorithmen
- Für moderne Umgebungen: ED25519 bietet hervorragende Sicherheit und Leistung

PGP-Verschlüsselungs- und Entschlüsselungsalgorithmen

PGP (Pretty Good Privacy) verwendet zwei Arten von Algorithmen, die zusammenarbeiten, um Dateien in Workflows zu verschlüsseln und zu entschlüsseln:

1. Schlüsselpaar-Algorithmen — Werden verwendet, um die public/private Schlüsselpaare für Verschlüsselung und digitale Signaturen zu generieren
2. Symmetrische Algorithmen — Wird verwendet, um die eigentlichen Dateidaten zu verschlüsseln (die Schlüsselpaar-Algorithmen verschlüsseln den symmetrischen Schlüssel)

PGP-Schlüsselpaar-Algorithmen

Wählen Sie einen der folgenden Algorithmen, wenn Sie PGP-Schlüsselpaare für die Workflow-Entschlüsselung generieren:

RSA (empfohlen)

Für die meisten Benutzer empfohlen. Weit verbreitet, gut etabliert und FIPS-compliant. Bietet ein ausgewogenes Verhältnis zwischen Sicherheit und Kompatibilität.

ECC (Elliptische Kurven-Kryptografie)

Effizienter als RSA mit kleineren Schlüsselgrößen bei gleichzeitig hoher Sicherheit:

- NIST-Kurven — Standardkurven werden weitgehend unterstützt und FIPS-compliant
- BrainPool Kurven — Alternative Kurven für spezifische Konformitätsanforderungen
- Curve25519 — Moderne Hochleistungskurve mit hoher Sicherheit bei effizienter Berechnung

ElGamal

Legacy-Algorithmus. Wird aus Gründen der Kompatibilität mit älteren Systemen unterstützt. Verwenden Sie RSA oder ECC für neue Implementierungen.

Ausführliche Anweisungen zur Generierung von PGP-Schlüsseln finden Sie unter. [Generieren Sie PGP-Schlüssel](#)

Symmetrische PGP-Verschlüsselungsalgorithmen

Diese Algorithmen verschlüsseln Ihre eigentlichen Dateidaten. Der verwendete Algorithmus hängt davon ab, wie die PGP-Datei von Ihrer PGP-Software erstellt wurde:

FIPS-compliant Algorithmen (empfohlen für regulierte Umgebungen)

- AES-128, AES-192, AES-256 - Erweiterter Verschlüsselungsstandard (empfohlen)
- 3DES — Triple Data Encryption Standard (veraltet, verwenden Sie nach Möglichkeit AES)

Andere unterstützte Algorithmen

- IDEA, CAST5, Blowfish, DES,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

 Note

Sie wählen den symmetrischen Algorithmus nicht direkt, wenn Sie AWS Transfer Family Workflows verwenden — er wird durch die PGP-Software bestimmt, die zur Erstellung der verschlüsselten Datei verwendet wird. Sie können Ihre PGP-Software jedoch so konfigurieren, dass sie Algorithmen wie bevorzugt FIPS-compliant. AES-256

Weitere Hinweise zu unterstützten symmetrischen Algorithmen finden Sie unter. [Unterstützte symmetrische Verschlüsselungsalgorithmen](#)

Generieren Sie SSH-Schlüssel für vom Service verwaltete Benutzer

Sie können Ihren Server so einrichten, dass Benutzer mithilfe der vom Service verwalteten Authentifizierungsmethode authentifiziert werden, bei der Benutzernamen und SSH-Schlüssel innerhalb des Dienstes gespeichert werden. Der öffentliche SSH-Schlüssel des Benutzers wird als Eigentum des Benutzers auf den Server hochgeladen. Dieser Schlüssel wird vom Server als Teil eines standardmäßigen schlüsselbasierten Authentifizierungsprozesses verwendet. Jeder Benutzer kann mehrere öffentliche SSH-Schlüssel bei einem einzelnen Server registrieren. Informationen zur Begrenzung der Anzahl der Schlüssel, die pro Benutzer gespeichert werden können, finden Sie unter [AWS Transfer Family Endpunkte und Kontingente](#) in der. Allgemeine Amazon Web Services-Referenz

Als Alternative zur vom Dienst verwalteten Authentifizierungsmethode können Sie Benutzer mithilfe eines benutzerdefinierten Identitätsanbieters authentifizieren, oder. AWS Directory Service for Microsoft Active Directory Für weitere Informationen siehe [Mit Anbietern benutzerdefinierter Identitäten arbeiten](#) oder [Verwenden des AWS Directory Service für Microsoft Active Directory](#).

Ein Server kann Benutzer nur mit einer Methode authentifizieren (vom Dienst verwaltet, Verzeichnisdienst oder benutzerdefinierter Identitätsanbieter), und diese Methode kann nicht geändert werden, nachdem der Server erstellt wurde.

Themen

- [SSH-Schlüssel auf macOS, Linux oder Unix erstellen](#)
- [SSH-Schlüssel unter Microsoft Windows erstellen](#)
- [Konvertierung eines SSH2-Schlüssels in das Format eines öffentlichen SSH-Schlüssels](#)

SSH-Schlüssel auf macOS, Linux oder Unix erstellen

Auf den Betriebssystemen macOS, Linux oder Unix verwenden Sie den `ssh-keygen` Befehl, um einen öffentlichen SSH-Schlüssel und einen privaten SSH-Schlüssel zu erstellen, die auch als `key pair` bezeichnet werden.

Note

In den folgenden Beispielen geben wir keine Passphrase an: In diesem Fall fordert das Tool Sie auf, Ihre Passphrase einzugeben und sie dann zur Überprüfung zu wiederholen. Die Erstellung einer Passphrase bietet einen besseren Schutz für Ihren privaten Schlüssel und kann auch die allgemeine Systemsicherheit verbessern. Sie können Ihre Passphrase nicht wiederherstellen: Wenn Sie sie vergessen, müssen Sie einen neuen Schlüssel erstellen. Wenn Sie jedoch einen Server-Hostschlüssel generieren, müssen Sie eine leere Passphrase angeben, indem Sie die `-N ""` Option im Befehl angeben (oder indem Sie **Enter** zweimal drücken, wenn Sie dazu aufgefordert werden), da Transfer Family Family-Server beim Start kein Passwort anfordern können.

Um SSH-Schlüssel auf einem macOS-, Linux- oder Unix-Betriebssystem zu erstellen

1. Öffnen Sie auf macOS-, Linux- oder Unix-Betriebssystemen ein Befehlsterminal.
2. AWS Transfer Family akzeptiert RSA-, ECDSA- und Schlüssel. ED25519-formatted Wählen Sie den entsprechenden Befehl basierend auf dem Typ des Schlüsselpaars, das Sie generieren.

Tipp: *key_name* Ersetzen Sie es durch den tatsächlichen Namen Ihrer SSH-Schlüsselpaardatei.

- Um ein RSA 4096-Bit-Schlüsselpaar zu generieren:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Um ein 521-Bit-ECDSA-Schlüsselpaar zu generieren (ECDSA hat Bitgrößen von 256, 384 und 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Um ein ED25519-Schlüsselpaar zu generieren:

```
ssh-keygen -t ed25519 -f key_name
```

Im Folgenden wird ein Beispiel für die `ssh-keygen` Ausgabe gezeigt.

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|      . ....E      |
|      = ...        |
|. . . = ..o        |
|  . o +  oo =      |
|  + =  .S.= *      |
|  . o o ..B + o    |
|      .o.+.* .     |
|      =o*+*.       |
|      ..*o*+.      |
+-----[SHA256]-----+
```

Tipp: Wenn Sie den `ssh-keygen` Befehl wie oben gezeigt ausführen, erstellt er die öffentlichen und privaten Schlüssel als Dateien im aktuellen Verzeichnis.

Ihr SSH-Schlüsselpaar ist jetzt einsatzbereit. Folgen Sie den Schritten 3 und 4, um den öffentlichen SSH-Schlüssel für Ihre vom Service verwalteten Benutzer zu speichern. Diese Benutzer verwenden die Schlüssel, wenn sie Dateien auf Transfer Family Family-Serverendpunkten übertragen.

3. Navigieren Sie zu der `key_name.pub` Datei und öffnen Sie sie.
4. Kopieren Sie den Text und fügen Sie ihn in den öffentlichen SSH-Schlüssel für den vom Service verwalteten Benutzer ein.
 - a. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/> und wählen Sie dann im Navigationsbereich Server aus.
 - b. Wählen Sie auf der Seite Server die Server-ID für den Server aus, der den Benutzer enthält, den Sie aktualisieren möchten.

- c. Wählen Sie den Benutzer aus, für den Sie einen öffentlichen Schlüssel hinzufügen möchten.
- d. Wählen Sie im Bereich Öffentliche SSH-Schlüssel die Option Öffentlichen SSH-Schlüssel hinzufügen aus.

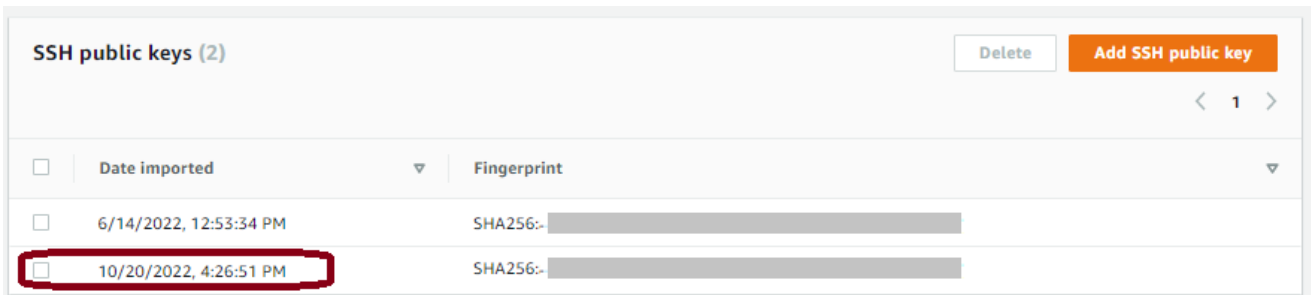
The screenshot shows the 'User: OneUser' configuration page in the AWS Transfer Family console. The breadcrumb navigation is 'Transfer Family > Servers > s-[server icon] > User: OneUser'. At the top right are 'View logs' and 'Delete' buttons. The main section is 'User configuration' with an 'Edit' button. It contains two columns: 'Role' with a 'Role' link, and 'Policy' with a 'View' button. Below these are 'Posix Profile' (User ID: 2001, Group ID: 2001, Secondary Group IDs: -) and 'Home directory' (Path: /fs-[redacted], Permissions: Restricted). At the bottom is the 'SSH public keys (1)' section, which includes a 'Delete' button, an 'Add SSH public key' button, and a table with one key.

☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256-[redacted]

- e. Fügen Sie den Text des öffentlichen Schlüssels, den Sie generiert haben, in das Textfeld für den öffentlichen SSH-Schlüssel ein und wählen Sie dann Schlüssel hinzufügen aus.

The screenshot shows the 'Add key' dialog in the AWS Transfer Family console. The breadcrumb navigation is 'Transfer Family > Servers > s-[server icon] > OneUser > Add key'. The title is 'Add key'. The main section is 'SSH public keys' with an 'Info' link. It contains a text area with the placeholder 'Enter SSH public key'. At the bottom right are 'Cancel' and 'Add key' buttons.

Der neue Schlüssel ist im Bereich mit öffentlichen SSH-Schlüsseln aufgeführt.



SSH public keys (2)		Delete	Add SSH public key
☐	Date imported	Fingerprint	
☐	6/14/2022, 12:53:34 PM	SHA256:-	
☐	10/20/2022, 4:26:51 PM	SHA256:-	

SSH-Schlüssel unter Microsoft Windows erstellen

Windows enthält OpenSSH als integrierte Funktion, mit der Sie SSH-Schlüssel im gleichen Format wie unter Linux oder macOS generieren können. Alternativ können Sie Tools von Drittanbietern wie den Schlüsselgenerator von PuTTY (PuTTYgen) verwenden.

Verwenden des in Windows integrierten OpenSSH

Neuere Versionen von Windows enthalten standardmäßig OpenSSH. Sie können dieselben `ssh-keygen` Befehle wie im Abschnitt beschrieben verwenden: macOS/Linux

1. Öffnen Sie Windows PowerShell oder die Befehlszeile.
2. Führen Sie je nach Schlüsseltyp, den Sie generieren möchten, einen der folgenden Befehle aus:

- Um ein RSA 4096-Bit-Schlüsselpaar zu generieren:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Um ein ECDSA 521-Bit-Schlüsselpaar zu generieren:

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Um ein ED25519-Schlüsselpaar zu generieren:

```
ssh-keygen -t ed25519 -f key_name
```

3. Folgen Sie den gleichen Schritten wie im macOS/Linux Abschnitt, in den Sie Ihren öffentlichen Schlüssel hochladen möchten. AWS Transfer Family

Verwenden von PuTTYgen (Drittanbieter-Tool)

Einige SSH-Clients von Drittanbietern für Windows, wie PuTTY, verwenden unterschiedliche Schlüsselformate. PuTTY verwendet das PPK Format für private Schlüssel. Wenn Sie PuTTY oder verwandte Tools wie WinSCP verwenden, können Sie PuTTYgen verwenden, um Schlüssel in diesem Format zu erstellen.

Note

Wenn Sie WinSCP eine private Schlüsseldatei präsentieren, die nicht im .ppk Format ist, bietet dieser Client an, den Schlüssel für Sie in ein .ppk Format zu konvertieren.

[Ein Tutorial zum Erstellen von SSH-Schlüsseln mithilfe von PuTTYgen finden Sie auf der Website. SSH.com](#)

Konvertierung eines SSH2-Schlüssels in das Format eines öffentlichen SSH-Schlüssels

AWS Transfer Family akzeptiert nur öffentliche Schlüssel. SSH-formatted Wenn Sie einen öffentlichen SSH2-Schlüssel haben, müssen Sie ihn konvertieren. Ein öffentlicher SSH2-Schlüssel hat das folgende Format:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

Ein öffentlicher SSH-Schlüssel hat das folgende Format:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Führen Sie den folgenden Befehl aus, um einen SSH2-formatted öffentlichen Schlüssel in einen SSH-formatted öffentlichen Schlüssel zu konvertieren. *ssh2-key* Ersetzen Sie ihn durch den Namen Ihres SSH2-Schlüssels und *ssh-key* durch den Namen Ihres SSH-Schlüssels.

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

Drehen Sie die SSH-Schlüssel

Aus Sicherheitsgründen empfehlen wir die bewährte Methode, Ihre SSH-Schlüssel zu rotieren. In der Regel wird diese Rotation als Teil einer Sicherheitsrichtlinie festgelegt und automatisiert implementiert. Je nach Sicherheitsstufe kann ein SSH-Schlüsselpaar für eine hochsensible Kommunikation nur einmal verwendet werden. Dadurch werden Risiken vermieden, die aus dem Speichern von Schlüsseln erwachsen. Es ist jedoch viel üblicher, SSH-Anmeldeinformationen für einen bestimmten Zeitraum zu speichern und ein Intervall festzulegen, das die Benutzer nicht übermäßig belastet. Dieser Zeitraum hat typischerweise eine Länge von drei Monaten.

Note

Informationen zur automatisierten SSH-Schlüsselrotation unter Verwendung von Infrastruktur als Code finden Sie unter [Terraform-Module der Transfer Family](#)

Es gibt zwei Methoden zum Durchführen der SSH-Schlüsselrotation:

- Auf der Konsole können Sie einen neuen öffentlichen SSH-Schlüssel hochladen und einen vorhandenen öffentlichen SSH-Schlüssel löschen.
- Mithilfe der API können Sie bestehende Benutzer aktualisieren, indem Sie die [DeleteSshPublicKey](#) API verwenden, um den öffentlichen Secure Shell (SSH) -Schlüssel eines Benutzers zu löschen, und die [ImportSshPublicKey](#) API, um dem Konto des Benutzers einen neuen öffentlichen Secure Shell (SSH) -Schlüssel hinzuzufügen.

Console

Um eine Schlüsselrotation in der Konsole durchzuführen

1. Öffnen Sie die AWS Transfer Family Konsole unter <https://console.aws.amazon.com/transfer/>.
2. Navigieren Sie zur Seite Server.
3. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Seite mit den Serverdetails aufzurufen.
4. Wählen Sie unter Benutzer das Kontrollkästchen des Benutzers aus, dessen öffentlichen SSH-Schlüssel Sie rotieren möchten. Wählen Sie dann Aktionen und anschließend Schlüssel hinzufügen aus, um die Seite Schlüssel hinzufügen aufzurufen.

oder

Wählen Sie den Benutzernamen aus, um die Seite mit den Benutzerdetails aufzurufen, und wählen Sie dann Öffentlichen SSH-Schlüssel hinzufügen aus, um die Seite Schlüssel hinzufügen aufzurufen.

5. Geben Sie den neuen öffentlichen SSH-Schlüssel ein und wählen Sie Schlüssel hinzufügen.

 Important

Das Format des öffentlichen SSH-Schlüssels hängt von der Art des von Ihnen generierten Schlüssels ab.

- Für RSA-Schlüssel lautet das Format. `ssh-rsa string`
- Für ED25519-Schlüssel lautet das Format. `ssh-ed25519 string`
- Bei ECDSA-Schlüsseln beginnt der Schlüssel je nach Größe des von `ecdsa-sha2-nistp384` Ihnen generierten Schlüssels mit `ecdsa-sha2-nistp256` oder `ecdsa-sha2-nistp521`, oder. Auf die Anfangszeichenfolge folgt dann *string*, ähnlich wie bei den anderen Schlüsseltypen.

Sie kehren zur Seite mit den Benutzerdetails zurück, und der neue öffentliche SSH-Schlüssel, den Sie gerade eingegeben haben, wird im Abschnitt Öffentliche SSH-Schlüssel angezeigt.

6. Aktivieren Sie das Kontrollkästchen des alten YOU-Schlüssels, den Sie löschen möchten, und wählen Sie dann Löschen.
7. Bestätigen Sie den Löschvorgang, indem Sie das Wort eingebendelete, und wählen Sie dann Löschen.

API

Um eine Schlüsselrotation mithilfe der API durchzuführen

1. Öffnen Sie auf macOS-, Linux- oder Unix-Betriebssystemen ein Befehlsterminal.
2. Rufen Sie den SSH-Schlüssel ab, den Sie löschen möchten, indem Sie den folgenden Befehl eingeben. Um diesen Befehl zu verwenden, *serverID* ersetzen Sie ihn durch die Server-ID für Ihren Transfer Family Family-Server und *username* durch Ihren Benutzernamen.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

Der Befehl gibt Details über den Benutzer zurück. Kopieren Sie den Inhalt des "SshPublicKeyId": Felds. Sie müssen diesen Wert später in diesem Verfahren eingeben.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. Importieren Sie als Nächstes einen neuen SSH-Schlüssel für Ihren Benutzer. Geben Sie an der -Eingabeaufforderung folgenden Befehl ein. Um diesen Befehl zu verwenden, *serverID* ersetzen Sie ihn durch die Server-ID für Ihren Transfer Family Family-Server, *username* ersetzen Sie ihn durch Ihren Benutzernamen und *public-key* ersetzen Sie ihn durch den Fingerabdruck Ihres neuen öffentlichen Schlüssels.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
--ssh-public-key-body='public-key'
```

Wenn der Befehl erfolgreich ist, wird keine Ausgabe zurückgegeben.

4. Löschen Sie abschließend den alten Schlüssel, indem Sie den folgenden Befehl ausführen. Um diesen Befehl zu verwenden, *serverID* ersetzen Sie ihn durch die Server-ID für Ihren Transfer Family Family-Server, *username* ersetzen Sie ihn durch Ihren Benutzernamen und *keyID-from-step-2* ersetzen Sie ihn durch den Schlüssel-ID-Wert, den Sie in Schritt 2 dieses Verfahrens kopiert haben

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'  
--ssh-public-key-id='keyID-from-step-2'
```

5. (Optional) Um zu bestätigen, dass der alte Schlüssel nicht mehr existiert, wiederholen Sie Schritt 2.

Generieren Sie PGP-Schlüssel

Sie können die PGP-Entschlüsselung (Pretty Good Privacy) für die Dateien verwenden, die Transfer Family mit Workflows verarbeitet. Um die Entschlüsselung in einem Workflow-Schritt zu verwenden, geben Sie einen PGP-Schlüssel an. Ausführliche Informationen zu PGP-Schlüsselalgorithmen,

einschließlich Empfehlungen und FIPS-Konformität, finden Sie unter. [PGP-Schlüsselpaar-Algorithmen](#)

Der AWS Speicher-Blog enthält einen Beitrag, in dem beschrieben wird, wie Dateien mithilfe von Transfer Family Managed Workflows, Verschlüsseln und [Entschlüsseln von Dateien mit PGP und einfach entschlüsselt werden können, ohne Code zu](#) schreiben, beschrieben werden. AWS Transfer Family

Welchen Operator Sie zum Generieren Ihrer PGP-Schlüssel verwenden, hängt von Ihrem Betriebssystem und der Version der Software zur Schlüsselgenerierung ab, die Sie verwenden.

Wenn Sie Linux oder Unix verwenden, verwenden Sie zur Installation Ihr Paketinstallationsprogramm. gpg Abhängig von Ihrer Linux-Distribution sollte einer der folgenden Befehle für Sie funktionieren.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Für Windows oder macOS können Sie herunterladen, was Sie benötigen <https://gnupg.org/download/>.

Nachdem Sie Ihre PGP-Schlüsselgenerator-Software installiert haben, führen Sie den `gpg --gen-key` Befehl `gpg --full-gen-key` oder aus, um ein key pair zu generieren.

Note

Wenn Sie GnuPG Version 2.3.0 oder neuer verwenden, müssen Sie Folgendes ausführen. `gpg --full-gen-key` Wenn Sie nach dem Typ des zu erstellenden Schlüssels gefragt werden, wählen Sie RSA oder ECC. Wenn Sie ECC wählen, können Sie zwischen BrainPool und Curve25519 für die NIST elliptische Kurve wählen.

Nützliche Unterbefehle **gpg**

Im Folgenden finden Sie einige nützliche Unterbefehle für: `gpg`

- `gpg --help`— Dieser Befehl listet die verfügbaren Optionen auf und kann einige Beispiele enthalten.
- `gpg --list-keys`— Dieser Befehl listet die Details für alle Schlüsselpaare auf, die Sie erstellt haben.

- `gpg --fingerprint`— Dieser Befehl listet die Details für alle Ihre Schlüsselpaare auf, einschließlich des Fingerabdrucks der einzelnen Schlüssel.
- `gpg --export -a user-name`— Dieser Befehl exportiert den öffentlichen Schlüsselteil des Schlüssels für den *user-name*, der bei der Generierung des Schlüssels verwendet wurde.

PGP-Schlüssel verwalten

Um Ihre PGP-Schlüssel zu verwalten, verwenden Sie. AWS Secrets Manager

Note

Ihr geheimer Name beinhaltet Ihre Transfer Family Family-Server-ID. Das bedeutet, dass Sie bereits einen Server identifiziert oder erstellt haben sollten, bevor Sie Ihre PGP-Schlüsselinformationen darin AWS Secrets Manager speichern können.

Wenn Sie einen Schlüssel und eine Passphrase für alle Ihre Benutzer verwenden möchten, können Sie die PGP-Schlüsselblockinformationen unter dem geheimen Namen `aws/transfer/server-id/@pgp-default`, wo sich die ID für Ihren Transfer Family Family-Server *server-id* befindet. Transfer Family verwendet diesen Standardschlüssel, wenn es keinen Schlüssel gibt, der dem Benutzer *user-name* entspricht, der den Workflow ausführt.

Sie können einen Schlüssel für einen bestimmten Benutzer erstellen. In diesem Fall lautet das Format für den geheimen Namen `aws/transfer/server-id/user-name`, wobei dem Benutzer *user-name* entspricht, der den Workflow für einen Transfer Family Family-Server ausführt.

Note

Sie können maximal 3 private PGP-Schlüssel pro Transfer Family Family-Server pro Benutzer speichern.

Um PGP-Schlüssel für die Verwendung bei der Entschlüsselung zu konfigurieren

1. Abhängig von der GPG-Version, die Sie verwenden, führen Sie einen der folgenden Befehle aus, um ein PGP-Schlüsselpaar zu generieren.
 - Wenn Sie **GnuPG** Version 2.3.0 oder neuer verwenden, führen Sie den folgenden Befehl aus:

```
gpg --full-gen-key
```

Sie können wählen **RSA**, oder, falls Sie möchten **ECC**, können Sie entweder **NIST BrainPool** oder **Curve25519** für die elliptische Kurve wählen. Wenn Sie `gpg --gen-key` stattdessen ausführen, erstellen Sie ein key pair, das den ECC Curve 25519-Verschlüsselungsalgorithmus verwendet.

- Für Versionen **GnuPG** vor 2.3.0 können Sie den folgenden Befehl verwenden, da RSA der Standardverschlüsselungstyp ist.

```
gpg --gen-key
```

 Important

Während der Schlüsselgenerierung müssen Sie eine Passphrase und eine E-Mail-Adresse angeben. Achten Sie darauf, diese Werte zu notieren. Sie müssen die Passphrase angeben, wenn Sie die Schlüsseldetails AWS Secrets Manager später in diesem Verfahren eingeben. Und Sie müssen dieselbe E-Mail-Adresse angeben, um den privaten Schlüssel im nächsten Schritt zu exportieren.

2. Führen Sie den folgenden Befehl aus, um den privaten Schlüssel zu exportieren. Um diesen Befehl zu verwenden, *private.pgp* ersetzen Sie ihn durch den Namen der Datei, in der der private Schlüsselblock gespeichert werden soll, und *marymajor@example.com* durch die E-Mail-Adresse, die Sie bei der Generierung des key pair verwendet haben.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. Dient AWS Secrets Manager zum Speichern Ihres PGP-Schlüssels.
 - a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Secrets Manager Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
 - b. Wählen Sie im linken Navigationsbereich Secrets aus.
 - c. Wählen Sie auf der Seite Secrets die Option Neues Geheimnis speichern aus.
 - d. Wählen Sie auf der Seite Geheimtyp auswählen für Geheimtyp die Option Anderer Geheimtyp aus.
 - e. Wählen Sie im Bereich Key/value Paare die Key/value Registerkarte aus.

- Schlüssel — Enter**PGPPrivateKey**.

 Note

Sie müssen die **PGPPrivateKey** Zeichenfolge exakt eingeben: Fügen Sie vor oder zwischen den Zeichen keine Leerzeichen hinzu.

- Wert — Fügen Sie den Text Ihres privaten Schlüssels in das Wertfeld ein. Sie finden den Text Ihres privaten Schlüssels in der Datei (z. B. `private.pgp`), die Sie beim Exportieren Ihres Schlüssels zu Beginn dieses Verfahrens angegeben haben. Der Schlüssel beginnt mit `-----BEGIN PGP PRIVATE KEY BLOCK-----` und endet mit `-----END PGP PRIVATE KEY BLOCK-----`.

 Note

Stellen Sie sicher, dass der Textblock nur den privaten Schlüssel und nicht auch den öffentlichen Schlüssel enthält.

- f. Wählen Sie Zeile hinzufügen und wählen Sie im Bereich Key/valuePaare die Key/valueRegisterkarte aus.

- Schlüssel — Enter**PGPPassphrase**.

 Note

Sie müssen die **PGPPassphrase** Zeichenfolge exakt eingeben: Fügen Sie vor oder zwischen den Zeichen keine Leerzeichen hinzu.

- Wert — Geben Sie die Passphrase ein, die Sie bei der Generierung Ihres PGP-Schlüsselpaars verwendet haben.

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value	Plaintext	
PGPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	mypassphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

[Add new key](#)

Note

Sie können bis zu 3 Sätze von Schlüsseln und Passphrasen hinzufügen. Um einen zweiten Satz hinzuzufügen, fügen Sie zwei neue Zeilen hinzu, geben Sie und **PGPPassphrase2** für die Schlüssel ein **PGPrivateKey2** und fügen Sie einen weiteren privaten Schlüssel und eine Passphrase ein. Um einen dritten Satz hinzuzufügen, müssen die Schlüsselwerte und sein. **PGPrivateKey3** **PGPPassphrase3**

- g. Wählen Sie Weiter aus.
- h. Geben Sie auf der Seite Geheimen Schlüssel konfigurieren einen Namen und eine Beschreibung für Ihr Geheimnis ein.
 - Wenn Sie einen Standardschlüssel erstellen, d. h. einen Schlüssel, der von jedem Transfer Family Family-Benutzer verwendet werden kann, geben Sie ein **aws/transfer/server-id/@pgp-default**. *server-id* Ersetzen Sie ihn durch die ID des Servers, der den Workflow enthält, der einen Entschlüsselungsschritt enthält.

- Wenn Sie einen Schlüssel erstellen, der von einem bestimmten Transfer Family Family-Benutzer verwendet werden soll, geben Sie ein `aws/transfer/server-id/user-name`. `server-id` Ersetzen Sie ihn durch die ID des Servers, der den Workflow enthält, der einen Entschlüsselungsschritt enthält, und `user-name` ersetzen Sie ihn durch den Namen des Benutzers, der den Workflow ausführt. Das `user-name` wird in dem Identitätsanbieter gespeichert, den der Transfer Family Family-Server verwendet.
- i. Wählen Sie Weiter und akzeptieren Sie die Standardeinstellungen auf der Seite „Rotation konfigurieren“. Klicken Sie anschließend auf Weiter.
- j. Wählen Sie auf der Seite „Überprüfen“ die Option Speichern aus, um das Geheimnis zu erstellen und zu speichern.

Der folgende Screenshot zeigt die Details für den Benutzer **marymajor** für einen bestimmten Transfer Family Family-Server. Dieses Beispiel zeigt drei Schlüssel und die entsprechenden Passphrasen.

The screenshot displays the AWS Secrets Manager console for a secret named `/aws/transfer/s-.../marymajor`. The secret is associated with the encryption key `aws/secretsmanager`. The secret description states: "Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-...".

The secret value is displayed in a table with two columns: **Secret key** and **Secret value**. The table contains three rows of PGP private keys and their corresponding passphrases.

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase3	mypassphrase3

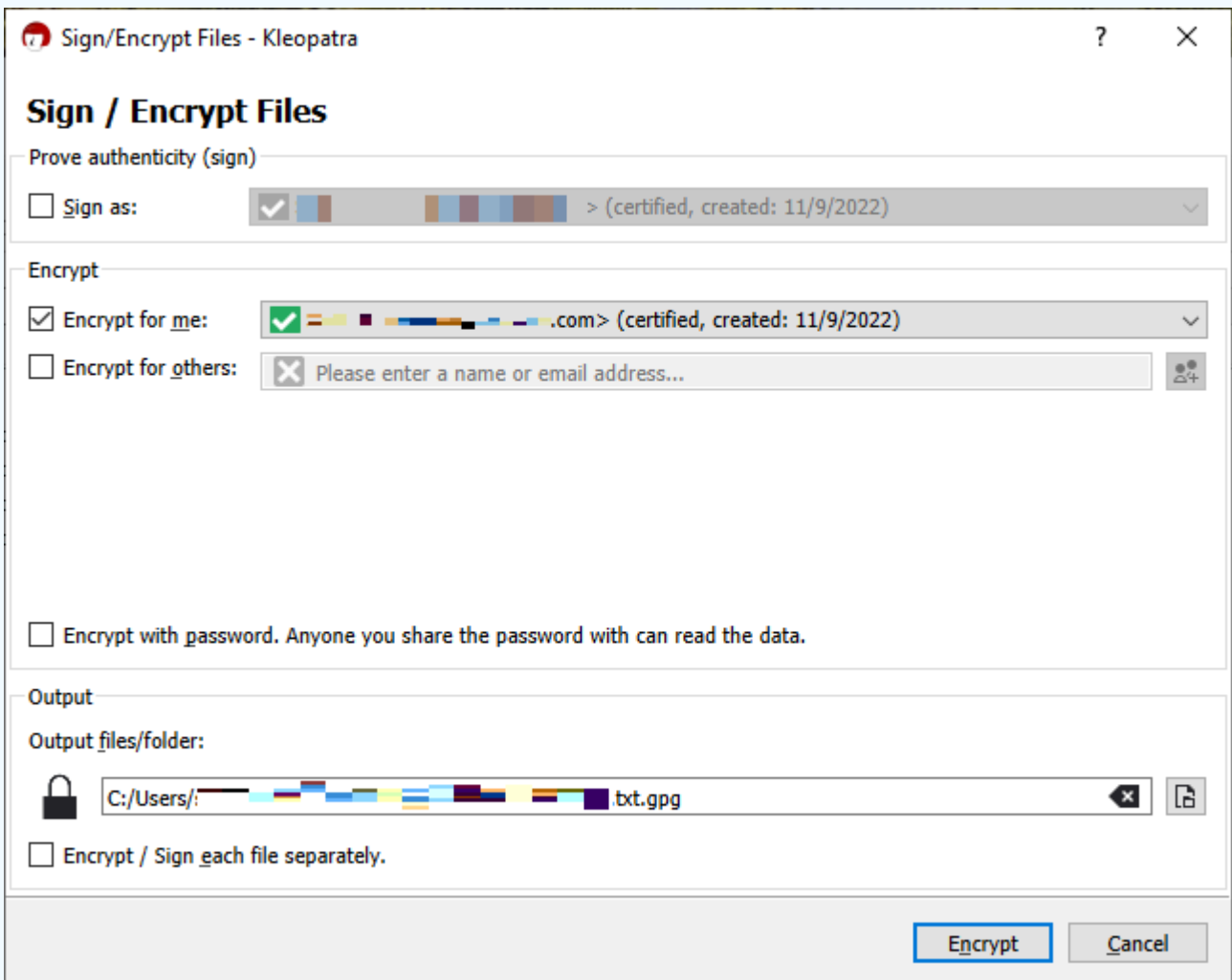
Unterstützte PGP-Clients

Die folgenden Clients wurden mit Transfer Family getestet und können zum Generieren von PGP-Schlüsseln und zum Verschlüsseln von Dateien verwendet werden, die Sie mit einem Workflow entschlüsseln möchten.

- Gpg4win + Kleopatra.

Note

Wenn Sie Dateien signieren/verschlüsseln auswählen, stellen Sie sicher, dass Sie die Auswahl für Signieren als deaktivieren: Derzeit unterstützen wir das Signieren von verschlüsselten Dateien nicht.



Wenn Sie die verschlüsselte Datei signieren und versuchen, sie mit einem Entschlüsselungsworkflow auf einen Transfer Family Family-Server hochzuladen, wird die folgende Fehlermeldung angezeigt:

```
Encrypted file with signed message unsupported
```

- Hauptversionen von GnuPG: 2.4, 2.3, 2.2, 2.0 und 1.4.

Beachten Sie, dass andere PGP-Clients möglicherweise auch funktionieren, aber nur die hier genannten Clients wurden mit Transfer Family getestet.

Identitäts- und Zugriffsmanagement für AWS Transfer Family

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Transfer Family IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Transfer Family funktioniert mit IAM](#)
- [AWS Transfer Family Beispiele für identitätsbasierte Richtlinien](#)
- [AWS Transfer Family Beispiele für tagbasierte Richtlinien](#)
- [Problembehandlung bei AWS Transfer Family Identität und Zugriff](#)
- [IAM-Bedingungsschlüssel für die Unternehmensführung](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe [Problembehandlung bei AWS Transfer Family Identität und Zugriff](#)).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe [Wie AWS Transfer Family funktioniert mit IAM](#)).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe [AWS Transfer Family Beispiele für identitätsbasierte Richtlinien](#)).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto an](#) im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter [AWS Signature Version 4 for API requests](#) im IAM-Benutzerhandbuch.

Root-Benutzer des AWS-Kontos

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem so genannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle Ressourcen hat. AWS-Services Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Tasks that require root user credentials](#) im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen

aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu](#) können.

Eine [IAM-Gruppe](#) spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) wechseln](#) oder indem Sie eine AWS Oder-API-Operation AWS CLI aufrufen. Weitere Informationen finden Sie unter [Methoden, um eine Rolle zu übernehmen](#) im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) 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 definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcen und unter welchen Bedingungen durchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter [Choose between managed policies and inline policies](#) im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#).

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. 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 Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im -IAM-Benutzerhandbuch.
- **Service-Kontrollrichtlinien (SCPs)** – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Ressourcen-Kontrollrichtlinien (RCPs)** – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter [Ressourcen-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter [Bewertungslogik für Richtlinien](#) im IAM-Benutzerhandbuch.

Wie AWS Transfer Family funktioniert mit IAM

Bevor Sie AWS Identity and Access Management (IAM) zur Verwaltung des Zugriffs auf verwenden AWS Transfer Family, sollten Sie wissen, mit welchen IAM-Funktionen Sie arbeiten können. AWS Transfer FamilyEinen allgemeinen Überblick darüber, wie AWS Transfer Family und andere AWS Dienste mit IAM funktionieren, finden Sie im [AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren](#).

Themen

- [AWS Transfer Family identitätsbasierte Richtlinien](#)
- [AWS Transfer Family ressourcenbasierte Richtlinien](#)
- [Autorisierung auf der Grundlage von Tags AWS Transfer Family](#)
- [AWS Transfer Family IAM-Rollen](#)

AWS Transfer Family identitätsbasierte Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen erteilt oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. AWS Transfer Family unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Weitere Informationen zu allen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [Referenz zu den IAM-JSON-Richtlinienelementen im AWS Identity and Access Management Benutzerhandbuch](#).

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Transfer Family verwendet: `transfer:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, einen Server mit dem Transfer Family `CreateServer` API-Vorgang zu erstellen, nehmen Sie die `transfer:CreateServer` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen ein `Action`- oder `NotAction`-Element enthalten. AWS Transfer Family definiert seinen eigenen Satz an Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere -Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen durch Kommas.

```
"Action": [  
    "transfer:action1",  
    "transfer:action2"
```

Sie können auch Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "transfer:Describe"
```

Eine Liste der AWS Transfer Family Aktionen finden Sie unter [Aktionen definiert von AWS Transfer Family](#) in der Service Authorization Reference.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Die Transfer Family Family-Serverressource hat den folgenden ARN.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Um beispielsweise den `s-01234567890abcdef` Transfer Family Family-Server in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Weitere Informationen zum Format von ARNs finden Sie unter [Amazon Resource Names \(ARNs\)](#) in der Service Authorization Reference oder unter [IAM-ARNs](#) im IAM-Benutzerhandbuch.

Um alle Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```


Einige AWS Transfer Family Aktionen werden für mehrere Ressourcen ausgeführt, z. B. für Ressourcen, die in IAM-Richtlinien verwendet werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

In einigen Fällen müssen Sie mehr als einen Ressourcentyp angeben, z. B. wenn Sie eine Richtlinie erstellen, die den Zugriff auf Server und Benutzer von Transfer Family ermöglicht. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Eine Liste der AWS Transfer Family Ressourcen finden Sie unter [Ressourcentypen definiert von AWS Transfer Family](#) in der Service Authorization Reference.

Bedingungsschlüssel

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

AWS Transfer Family definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Eine Liste der AWS Transfer Family Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS Transfer Family](#) in der Service Authorization Reference.

Beispiele

Beispiele für AWS Transfer Family identitätsbasierte Richtlinien finden Sie unter [AWS Transfer Family Beispiele für identitätsbasierte Richtlinien](#) Informationen zu VPC-endpunktspezifischen IAM-

Richtlinien finden Sie unter. [Beschränkung des VPC-Endpunktzugriffs für Transfer Family Family-Server](#)

AWS Transfer Family ressourcenbasierte Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal auf der AWS Transfer Family Ressource ausführen kann und unter welchen Bedingungen. Amazon S3 unterstützt ressourcenbasierte Berechtigungsrichtlinien für Amazon S3. *buckets* Resource-based Mithilfe von Richtlinien können Sie anderen Konten pro Ressource Nutzungsberechtigungen erteilen. Sie können auch eine ressourcenbasierte Richtlinie verwenden, um einem AWS Service den Zugriff auf Ihr Amazon S3 zu ermöglichen. *buckets*

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als [Prinzipal in einer ressourcenbasierten Richtlinie](#) angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Principal und die Ressource in unterschiedlichen AWS Konten befinden, müssen Sie der Prinzipaleinheit auch die Erlaubnis erteilen, auf die Ressource zuzugreifen. Sie erteilen Berechtigungen, indem Sie der Entität eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie im Benutzerhandbuch [unter Unterschiede zwischen IAM-Rollen und ressourcenbasierten Richtlinien](#). AWS Identity and Access Management

Der Amazon S3 S3-Service unterstützt nur eine Art von ressourcenbasierter Richtlinie, die als Richtlinie bezeichnet wird und an eine *bucket* angehängt ist. *bucket* Diese Richtlinie definiert, welche Hauptentitäten (Konten, Benutzer, Rollen und Verbundbenutzer) Aktionen für das Objekt ausführen können.

Beispiele

Beispiele für AWS Transfer Family ressourcenbasierte Richtlinien finden Sie unter. [AWS Transfer Family Beispiele für tagbasierte Richtlinien](#)

Autorisierung auf der Grundlage von Tags AWS Transfer Family

Sie können Tags an AWS Transfer Family Ressourcen anhängen oder Tags in einer Anfrage an übergeben AWS Transfer Family. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `transfer:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung

`aws : TagKeys` verwenden. Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf AWS Transfer Family Ressourcen finden Sie unter [AWS Transfer Family Beispiele für tagbasierte Richtlinien](#).

AWS Transfer Family IAM-Rollen

Eine [IAM-Rolle](#) ist eine Entität in Ihrem AWS Konto, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit AWS Transfer Family

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie [AssumeRole](#) oder aufrufen [GetFederationToken](#).

AWS Transfer Family unterstützt die Verwendung temporärer Anmeldeinformationen.

AWS Transfer Family Beispiele für identitätsbasierte Richtlinien

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von AWS Transfer Family -Ressourcen. Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen zum Erstellen einer identitätsbasierten IAM-Richtlinie mithilfe dieser Beispieldokumente zu JSON-Richtlinien finden Sie im Benutzerhandbuch unter [Erstellen von Richtlinien auf der Registerkarte JSON](#). AWS Identity and Access Management

Themen

- [Best Practices für Richtlinien](#)
- [Verwenden der Konsole AWS Transfer Family](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand AWS Transfer Family Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen

AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf 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 [Von AWS verwaltete Richtlinien](#) oder [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#) 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. 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 [Richtlinienvvalidierung mit 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 [Sicherer API-Zugriff mit MFA](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Best Practices für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Konsole AWS Transfer Family

Um auf die AWS Transfer Family Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den AWS Transfer Family Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie. Weitere Informationen finden Sie im [Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen AWS Identity and Access Management](#) Benutzer.

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 den API-Operation entsprechen, die Sie ausführen möchten.

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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    }
  ]
}
```

```

    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}

```

AWS Transfer Family Beispiele für tagbasierte Richtlinien

Im Folgenden finden Sie Beispiele dafür, wie Sie den Zugriff auf AWS Transfer Family Ressourcen anhand von Tags steuern können.

Verwendung von Tags zur Steuerung des Zugriffs auf AWS Transfer Family Ressourcen

Bedingungen in IAM-Richtlinien sind Teil der Syntax, mit der Sie Berechtigungen für AWS Transfer Family Ressourcen angeben. Sie können den Zugriff auf AWS Transfer Family Ressourcen (wie Benutzer, Server, Rollen und andere Entitäten) anhand von Tags auf diesen Ressourcen steuern. Tags sind Schlüssel-Wert-Paare, Weitere Informationen zum Markieren von Ressourcen finden Sie unter [Taggen von AWS Ressourcen](#) in der. Allgemeine AWS-Referenz

In AWS Transfer Family können Ressourcen Tags haben, und einige Aktionen können Tags enthalten. Wenn Sie eine IAM-Richtlinie erstellen, können Sie Markierungs-Bedingungsschlüssel verwenden, um Folgendes zu kontrollieren:

- Welche Benutzer anhand der Tags, die die AWS Transfer Family Ressource besitzt, Aktionen an einer Ressource ausführen können.
- Welche Tags in der Anforderung einer Aktion übergeben werden können.
- Ob bestimmte Tag-Schlüssel in einer Anforderung verwendet werden können.

Durch die Verwendung der tagbasierten Zugriffskontrolle können Sie eine genauere Kontrolle als auf API-Ebene anwenden. Sie können auch eine dynamischere Steuerung anwenden als mit einer ressourcenbasierten Zugriffskontrolle. Sie können IAM-Richtlinien erstellen, die einen Vorgang auf der Grundlage der in der Anfrage angegebenen Tags (Anforderungs-Tags) zulassen oder verweigern. Sie können IAM-Richtlinien auch auf der Grundlage von Tags auf der Ressource erstellen, auf der gearbeitet wird (Ressourcen-Tags). Im Allgemeinen sind Ressourcen-Tags für Tags vorgesehen, die sich bereits auf Ressourcen befinden. Anforderungs-Tags sind für das Hinzufügen oder Entfernen von Tags zu einer Ressource vorgesehen.

Die vollständige Syntax und Semantik von Tag-Bedingungsschlüsseln finden Sie im IAM-Benutzerhandbuch unter [Steuern des Zugriffs auf AWS Ressourcen mithilfe von Ressourcen-Tags](#). Einzelheiten zur Angabe von IAM-Richtlinien mit API Gateway finden Sie unter [Steuern des Zugriffs auf eine API mit IAM-Berechtigungen](#) im API Gateway Developer Guide.

Beispiel 1: Verweigern Sie Aktionen, die auf Ressourcen-Tags basieren

Sie können die Ausführung einer Aktion an einer Ressource auf der Grundlage von Tags verweigern. Die folgende Beispielrichtlinie verweigert `TagResource`, `UntagResource`, `StartServer`, `DescribeUser`, `StopServer`, `DescribeServer`, wenn die Benutzer- oder Serverressource mit dem Schlüssel `stage` und dem Wert `prod` gekennzeichnet ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}
```

```
    ]
  }
}
```

Beispiel 2: Aktionen auf der Grundlage von Ressourcen-Tags zulassen

Sie können zulassen, dass eine Aktion für eine Ressource ausgeführt wird, die auf Tags basiert. Die folgende Beispielrichtlinie ermöglicht `TagResource`, `UntagResource`, `StartServer`, `StopServer`, und `DescribeUser` Operationen `DescribeServer`, wenn die Benutzer- oder Serverressource mit dem Schlüssel `stage` und dem Wert gekennzeichnet ist `prod`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}
```

Beispiel 3: Verweigern Sie die Erstellung eines Benutzers oder Servers auf der Grundlage von Anforderungs-Tags

Die folgende Beispielrichtlinie enthält zwei Anweisungen. Die erste Anweisung verweigert den `CreateServer` Vorgang für alle Ressourcen, wenn der Kostenstellenschlüssel für das Tag keinen Wert hat.

Die zweite Anweisung lehnt den `CreateServer` Vorgang ab, wenn der Kostenstellenschlüssel für das Tag einen anderen Wert als 1, 2 oder 3 enthält.

 Note

Diese Richtlinie ermöglicht das Erstellen oder Löschen einer Ressource, die einen Schlüssel namens `costcenter` und den Wert 12, oder 3 enthält.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:CreateServer"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/costcenter": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "transfer:CreateServer",
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringNotEquals": {
          "aws:RequestTag/costcenter": [
            "1",
            "2",
            "3"
          ]
        }
      }
    }
  ]
}
```

```
}  
]
```

Problembehandlung bei AWS Transfer Family Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Transfer Family IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Transfer Family](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Transfer Family Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Transfer Family

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer mateojackson versucht, die Konsole zum Anzeigen von Details zu einem *widget* zu verwenden, jedoch nicht über `transfer:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
transfer:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *my-example-widget* auf die Ressource `transfer;:GetWidget` zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Transfer Family übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte 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 AWS Transfer Family 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.

Die folgende Beispielrichtlinie enthält die Erlaubnis, eine Rolle an zu übergeben AWS Transfer Family. **123456789012** Ersetzen Sie es durch Ihre AWS-Konto-ID und **MyTransferRole** durch Ihren tatsächlichen IAM-Rollennamen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "Effect": "Allow"
    }
  ]
}
```

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Transfer Family Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien

oder Zugriffskontrolllisten (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 diese Funktionen AWS Transfer Family unterstützt werden, finden Sie unter [Wie AWS Transfer Family funktioniert 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 [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

IAM-Bedingungsschlüssel für die Unternehmensführung

AWS Transfer Family stellt IAM-Bedingungsschlüssel bereit, mit denen Sie Ressourcenkonfigurationen in jeder IAM-Richtlinie einschränken können. Diese Bedingungsschlüssel können in identitätsbasierten Richtlinien verwendet werden, die Benutzern oder Rollen zugewiesen sind, oder in Service Control Policies (SCPs) für die Unternehmensführung.

Service Control-Richtlinien sind IAM-Richtlinien, die für das gesamte AWS Unternehmen gelten und präventive Schutzmaßnahmen für mehrere Konten bieten. Wenn diese Bedingungsschlüssel in SCPs verwendet werden, helfen sie dabei, Sicherheits- und Compliance-Anforderungen unternehmensweit durchzusetzen.

Informationen finden Sie auch unter:

- [Aktionen, Ressourcen und Bedingungsschlüssel für Transfer Family](#)
- [Service-Kontrollrichtlinien \(SCPs\)](#)
- Sehen Sie sich [dieses Video](#) an, in dem beschrieben wird, wie Sie präventive Schutzmaßnahmen mithilfe von Richtlinien zur Servicesteuerung durchsetzen

Verfügbare Zustandsschlüssel

AWS Transfer Family unterstützt die folgenden Bedingungsschlüssel zur Verwendung in IAM-Richtlinien:

`transfer:RequestServerEndpointType`

Schränkt die Servererstellung und Updates basierend auf dem Endpunkttyp (PUBLIC, VPC, VPC_ENDPOINT) ein. Wird häufig verwendet, um öffentlich zugängliche Endgeräte zu verhindern.

`transfer:RequestServerProtocols`

Schränkt die Erstellung und Aktualisierung von Servern auf der Grundlage unterstützter Protokolle (SFTP, FTPS, FTP, AS2) ein.

`transfer:RequestServerDomain`

Schränkt die Servererstellung basierend auf dem Domaintyp (S3, EFS) ein.

`transfer:RequestConnectorProtocol`

Schränkt die Erstellung von Konnektoren auf der Grundlage des Protokolls (AS2, SFTP) ein.

Unterstützte Aktionen

Die Bedingungsschlüssel können auf die folgenden Aktionen angewendet werden: AWS Transfer Family

- `CreateServer`: Unterstützt die Tasten `RequestServerEndpointType`, `RequestServerProtocols`, und `RequestServerDomain` Bedingungstasten
- `UpdateServer`: Unterstützt Tasten `RequestServerEndpointType` und `RequestServerProtocols` Bedingungstasten
- `CreateConnector`: Unterstützt `RequestConnectorProtocol` Bedingungsschlüssel

Beispiel für eine SCP-Richtlinie

Das folgende Beispiel für ein SCP verhindert die Einrichtung von öffentlichen AWS Transfer Family Servern in Ihrer Organisation:

```
{
```

```
"Version": "2012-10-17",
"Statement": [{
  "Sid": "DenyPublicTransferServers",
  "Effect": "Deny",
  "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "transfer:RequestServerEndpointType": "PUBLIC"
    }
  }
}]
}
```

Konformitätsprüfung für AWS Transfer Family

Third-party Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften im AWS Transfer Family Rahmen mehrerer Compliance-Programme. AWS Zu diesen Programmen gehören SOC, PCI, HIPAA und andere. Die vollständige Liste finden Sie unter [AWS Leistungen im Leistungsumfang nach Compliance-Programmen](#).

Eine Liste der AWS Dienstleistungen im Rahmen bestimmter Compliance-Programme finden Sie unter [AWS Dienstleistungen im Umfang der einzelnen Compliance-Programme](#). Allgemeine Informationen finden Sie unter [AWS -Compliance-Programme](#).

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen in AWS Artifact](#).

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS Transfer Family hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS
- Whitepaper „[Architecting for HIPAA](#)“ zu Sicherheit und Compliance — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen entwickeln können. AWS HIPAA-compliant

- [AWS -Compliance-Ressourcen](#) – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort interessant sein.
- [AWS Config](#)— Dieser AWS Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub CSPM](#)— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS, die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche zu überprüfen.

Resilienz in AWS Transfer Family

Die AWS globale Infrastruktur basiert auf AWS Regionen und 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 Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

AWS Transfer Family unterstützt bis zu 3 Availability Zones und wird durch eine automatisch skalierbare, redundante Flotte für Ihre Verbindungs- und Übertragungsanfragen unterstützt.

Für alle Transfer Family Family-Endpunkte:

- Zone-level Verfügbarkeitsredundanz ist in den Service integriert.
- Für jede AZ gibt es redundante Flotten.
- Diese Redundanz wird automatisch bereitgestellt.

Note

Für Endgeräte in einer Virtual Private Cloud (VPC) ist es möglich, ein einzelnes Subnetz bereitzustellen. Wir empfehlen jedoch, Endpoints in mehreren Availability Zones innerhalb Ihrer VPC zu erstellen, um das Risiko von Serviceunterbrechungen bei Ausfällen der Availability Zone zu verringern.

Informationen finden Sie auch unter:

- Einzelheiten zum Erstellen von Transfer Family Family-Servern in einer VPC finden Sie unter [Erstellen Sie einen Server in einer virtuellen privaten Cloud](#).
- Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).
- Ein Beispiel dafür, wie Sie mithilfe von Latency-based Routing eine höhere Redundanz erreichen und die Netzwerklatenz minimieren können, finden Sie im Blogbeitrag [Minimiere die Netzwerklatenz mit Ihren AWS Transfer Family Servern](#).

Erstellen Sie eine private Verbindung zwischen einer VPC und APIs AWS Transfer Family

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Transfer Family APIs herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen, der von betrieben wird. [AWS PrivateLink](#) Sie können auf AWS Transfer Family APIs zugreifen, als ob sie sich in Ihrer VPC befinden würden, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung zu verwenden. Die Instances in Ihrer VPC benötigen für die Kommunikation mit AWS Transfer Family -APIs keine öffentlichen IP-Adressen.

Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Weitere Informationen finden Sie unter [Access AWS services through AWS PrivateLink](#) im AWS PrivateLink Handbuch. Bevor Sie einen VPC-Schnittstellen-Endpunkt für AWS Transfer Family APIs einrichten, lesen Sie die [Überlegungen](#) im AWS PrivateLink Handbuch.

Steuern des Zugriffs mithilfe von VPC-Endpunktrichtlinien

Standardmäßig ist der vollständige Zugriff auf AWS Transfer Family APIs über den Endpunkt zulässig. Sie können den Zugriff auf den Schnittstellenendpunkt mithilfe von VPC-Endpunktrichtlinien steuern. Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf AWS Transfer Family APIs steuert. Die Richtlinie gibt die folgenden Informationen an:

- Der Principal, der Aktionen ausführen kann.
- Die Aktionen, die ausgeführt werden können.
- Die Ressourcen, auf denen Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für AWS Transfer Family APIs. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie Zugriff auf alle AWS Transfer Family API-Aktionen für alle Ressourcen, mit Ausnahme derjenigen, die mit Schlüssel `Environment` und Wert gekennzeichnet sind `Test`.

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    }
  }, {
    "Effect": "Allow",
    "Action": "transfer:*",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

Erstellen Sie einen VPC-Schnittstellen-Endpunkt für APIs AWS Transfer Family

Sie können einen VPC-Endpunkt für AWS Transfer Family APIs entweder mit der Amazon VPC-Konsole oder der AWS Befehlszeilenschnittstelle (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellen eines VPC-Endpunkts](#) im AWS PrivateLink-Leitfaden.

Erstellen Sie einen VPC-Endpunkt für AWS Transfer Family APIs mit einem der folgenden Dienstnamen:

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Um einen VPC-Schnittstellen-Endpunkt zu erstellen, der dem US-Regierungsstandard Federal Information Processing Standard (FIPS) Publication 140-3 entspricht.

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an AWS Transfer Family APIs stellen, indem Sie den Standard-DNS-Namen für die Region verwenden, z. B. `transfer.us-east-1.amazonaws.com`

Sicherheit der Infrastruktur in AWS Transfer Family

AWS Transfer Family ist als verwalteter Dienst 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 für den Zugriff AWS Transfer Family über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Vermeiden Sie es, AWS Transfer Family NLBs und NATs vor Servern zu platzieren

Note

Server, die mit FTP- und FTPS-Protokollen konfiguriert sind, ermöglichen nur eine Konfiguration mit einer VPC: Es ist kein öffentlicher Endpunkt verfügbar für. FTP/FTPS

Viele Kunden konfigurieren einen Network Load Balancer (NLB), um den Datenverkehr an ihren AWS Transfer Family Server weiterzuleiten. In der Regel tun sie dies entweder, weil sie ihren Server erstellt haben, bevor ihnen die Möglichkeit AWS geboten wurde, sowohl innerhalb ihrer VPC als auch über das Internet darauf zuzugreifen, oder weil sie FTP im Internet unterstützen. Diese Konfiguration erhöht nicht nur die Kosten für Kunden, sondern kann auch andere Probleme verursachen, die wir in diesem Abschnitt beschreiben.

NAT-Gateways sind eine obligatorische Komponente, wenn Clients über ein privates Kundennetzwerk hinter einer Unternehmensfirewall eine Verbindung herstellen. Sie sollten sich jedoch bewusst sein, dass, wenn sich viele Clients hinter demselben NAT-Gateway befinden, dies Auswirkungen auf die Leistung und die Verbindungslimits haben kann. Wenn der Kommunikationspfad vom Client zum FTP- oder FTPS-Server ein NLB oder NAT enthält, kann der Server die IP-Adresse des Clients nicht genau erkennen, da AWS Transfer Family nur die IP-Adresse des NLB oder NAT angezeigt wird.

Wenn Sie die Konfiguration eines Transfer Family Family-Servers hinter einem NLB verwenden, empfehlen wir Ihnen, zu einem VPC-Endpunkt zu wechseln und statt einer NLB eine Elastic IP-Adresse zu verwenden. Beachten Sie bei der Verwendung von NAT-Gateways die unten beschriebenen Verbindungsbeschränkungen.

Wenn Sie das FTPS-Protokoll verwenden, schränkt diese Konfiguration nicht nur Ihre Fähigkeit ein, zu überprüfen, wer auf Ihren Server zugreift, sondern kann sich auch auf die Leistung auswirken. AWS Transfer Family verwendet die Quell-IP-Adresse, um Ihre Verbindungen auf unserer Datenebene gemeinsam zu nutzen. Für FTPS bedeutet dies, dass Transfer Family Family-Server mit NLB- oder NAT-Gateways auf der Kommunikationsroute nicht über 10.000 gleichzeitige Verbindungen verfügen, sondern auf nur 300 gleichzeitige Verbindungen beschränkt sind.

Wir empfehlen zwar, Network Load Balancer vor den AWS Transfer Family Servern zu vermeiden, aber wenn Ihre FTP- oder FTPS-Implementierung eine NLB- oder NAT-Verbindung in der Kommunikationsroute vom Client erfordert, sollten Sie die folgenden Empfehlungen beachten:

- Verwenden Sie für einen NLB Port 21 für Integritätsprüfungen anstelle der Ports 8192-8200.
- Aktivieren Sie für den AWS Transfer Family Server die Wiederaufnahme der TLS-Sitzung, indem Sie die Einstellung festlegen. `TlsSessionResumptionMode = ENFORCED`

Note

Dies ist der empfohlene Modus, da er erhöhte Sicherheit bietet:

- Erfordert, dass Clients die TLS-Sitzungswiederaufnahme für nachfolgende Verbindungen verwenden.
- Bietet stärkere Sicherheitsgarantien, indem konsistente Verschlüsselungsparameter gewährleistet werden.
- Hilft, potenzielle Downgrade-Angriffe zu verhindern.
- Sorgt für die Einhaltung der Sicherheitsstandards und optimiert gleichzeitig die Leistung.

- Wenn möglich, sollten Sie auf die Verwendung eines NLB verzichten, um die AWS Transfer Family Leistungs- und Verbindungslimits voll auszunutzen.

Wenn Sie weitere Informationen zu NLB-Alternativen benötigen, wenden Sie sich über den AWS Support an das AWS Transfer Family Produktmanagement-Team. Weitere Informationen zur Verbesserung Ihres Sicherheitsstatus finden Sie im Blogbeitrag [Sechs Tipps zur Verbesserung der Sicherheit Ihres AWS Transfer Family Servers](#).

Sicherheit der VPC-Konnektivität und der Infrastruktur

SFTP-Konnektoren mit VPC-Ausgangstyp bieten verbesserte Infrastruktursicherheit durch Netzwerkisolierung und private Konnektivität:

Vorteile der Netzwerkisolierung

- Privater Netzwerkverkehr: Der gesamte Connector-Traffic zu privaten SFTP-Servern verbleibt innerhalb Ihrer VPC und durchquert niemals das öffentliche Internet.
- Kontrollierter Ausgang: Bei öffentlichen Endpunkten, auf die über VPC zugegriffen wird, wird der Datenverkehr über Ihre NAT-Gateways geleitet, sodass Sie die Kontrolle über ausgehende IP-Adressen und Netzwerkrichtlinien haben.
- VPC-Sicherheitskontrollen: Nutzen Sie bestehende VPC-Sicherheitsgruppen, Netzwerk-ACLs und Routing-Tabellen, um den Connector-Netzwerkzugriff zu kontrollieren.
- Hybride Konnektivität: Greifen Sie über etablierte VPN- oder Direct Connect-Verbindungen ohne zusätzliche Internetverbindung auf lokale SFTP-Server zu.

Überlegungen zur Sicherheit von Resource Gateway

Resource Gateways bieten sichere Zugangspunkte für Cross-VPC Resource Access:

- Multi-AZ Bereitstellung: Resource Gateways benötigen Subnetze in mindestens zwei Availability Zones, um hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten.
- Kontrollen für Sicherheitsgruppen: Konfigurieren Sie Sicherheitsgruppen so, dass der Zugriff auf SFTP-Ports (normalerweise Port 22) nur von autorisierten Quellen aus eingeschränkt wird.
- Platzierung privater Subnetze: Stellen Sie Resource Gateways in privaten Subnetzen bereit, wenn Sie eine Verbindung zu privaten SFTP-Servern herstellen, um die Netzwerkisolierung aufrechtzuerhalten.

- Verbindungslimits: Jedes Resource Gateway unterstützt bis zu 350 gleichzeitige Verbindungen mit einem Leerlaufzeitlimit von 350 Sekunden für TCP-Verbindungen.

Fügen Sie eine Firewall für Webanwendungen hinzu

AWS WAF ist eine Firewall für Webanwendungen, die hilft, Webanwendungen und APIs vor Angriffen zu schützen. Sie können damit eine Reihe von Regeln konfigurieren, die als Web Access Control List (Web ACL) bezeichnet werden und Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Weitere Informationen finden Sie unter [Verwenden AWS WAF zum Schutz Ihrer APIs](#).

Um hinzuzufügen AWS WAF

1. Öffnen Sie die API Gateway Gateway-Konsole unter <https://console.aws.amazon.com/apigateway/>.
2. Wählen Sie im API-Navigationsbereich Ihre benutzerdefinierte Identitätsanbieter-Vorlage aus.
3. Wählen Sie Stages.
4. Wählen Sie im Bereich Stages den Namen der Stufe aus.
5. Wählen Sie im Bereich Stage Editor die Registerkarte Settings.
6. Führen Sie eine der folgenden Aktionen aus:
 - Wählen Sie unter Web Application Firewall (WAF) für Web ACL die Web-ACL aus, die Sie dieser Phase zuordnen möchten.
 - Wenn die von Ihnen benötigte Web-ACL nicht existiert, müssen Sie eine erstellen, indem Sie wie folgt vorgehen:
 1. Wählen Sie Web-ACL erstellen.
 2. Wählen Sie auf der Startseite des AWS WAF-Service die Option Web-ACL erstellen aus.
 3. Geben Sie unter Web-ACL-Details für Name den Namen der Web-ACL ein.
 4. Wählen Sie unter Regeln die Option Regeln hinzufügen und anschließend Meine eigenen Regeln und Regelgruppen hinzufügen aus.
 5. Wählen Sie unter Regeltyp die Option IP-Set aus, um eine bestimmte Liste von IP-Adressen zu identifizieren.
 6. Geben Sie unter Regel den Namen der Regel ein.
 7. Wählen Sie für IP-Set einen vorhandenen IP-Satz aus. Informationen zum Erstellen eines IP-Sets finden Sie unter [Einen IP-Satz erstellen](#).

8. Wenn Sie die IP-Adresse als ursprüngliche Adresse verwenden möchten, wählen Sie im Header die Option IP-Adresse aus.
 9. Geben Sie als Namen des Header-Felds ein `SourceIP`.
 10. Wählen Sie für Position im Header die Option Erste IP-Adresse aus.
 11. Wählen Sie für Fallback bei fehlender IP-Adresse die Option Match oder No Match, je nachdem, wie Sie mit einer ungültigen (oder fehlenden) IP-Adresse im Header umgehen möchten.
 12. Wählen Sie unter Aktion die Aktion des IP-Sets aus.
 13. Wählen Sie für Standard-Web-ACL-Aktion für Anfragen, die keiner Regel entsprechen, die Option Zulassen oder Blockieren aus und klicken Sie dann auf Weiter.
 14. Wählen Sie für die Schritte 4 und 5 die Option Weiter aus.
 15. Überprüfen Sie unter Überprüfen und erstellen Ihre Auswahl und wählen Sie dann Web-ACL erstellen aus.
7. Wählen Sie Save Changes.
 8. Wählen Sie Resources aus.
 9. Wählen Sie für Aktionen die Option Deploy API aus.

Informationen zur Sicherheit von Transfer Family mit AWS Web Application Firewall finden Sie unter [Securing Transfer Family with AWS Application Firewall und Amazon API Gateway](#) im AWS Speicher-Blog.

Cross-service verwirrter Stellvertreter, Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiere Entität zur Durchführung der Aktion zwingen kann. Bei AWS dienststellenübergreifendem Identitätswechsel kann es zu einem Problem mit verwirrtem Stellvertreter kommen. Cross-service Ein Identitätswechsel kann auftreten, wenn ein Dienst (der anrufende Dienst) einen anderen Dienst (den angerufenen Dienst) aufruft. Der anrufende Dienst kann so manipuliert werden, dass er seine Berechtigungen nutzt, um auf die Ressourcen eines anderen Kunden so einzuwirken, dass er sonst keine Zugriffsberechtigung hätte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben. Eine ausführliche Beschreibung dieses Problems finden Sie im IAM-Benutzerhandbuch unter [The Confused Deputy Problem](#).

Wir empfehlen, die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die AWS Transfer Family für die Ressource hat. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des exakten Amazon-Ressourcennamens (ARN) der Ressource, die Sie zulassen möchten. Wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:transfer::region::account-id:server/*`.

AWS Transfer Family verwendet die folgenden Rollentypen:

- **Benutzerrolle** — Ermöglicht dienstverwalteten Benutzern den Zugriff auf die erforderlichen Transfer Family Family-Ressourcen. AWS Transfer Family übernimmt diese Rolle im Kontext eines Transfer Family Family-Benutzer-ARN.
- **Zugriffsrolle** — Ermöglicht den Zugriff nur auf die Amazon S3 S3-Dateien, die übertragen werden. Für eingehende AS2-Übertragungen verwendet die Zugriffsrolle den Amazon-Ressourcennamen (ARN) für die Vereinbarung. Für ausgehende AS2-Übertragungen verwendet die Zugriffsrolle den ARN für den Connector.
- **Aufruflerrolle** — Zur Verwendung mit Amazon API Gateway als benutzerdefiniertem Identitätsanbieter des Servers. Transfer Family übernimmt diese Rolle im Kontext eines Transfer Family Family-Servers ARN.
- **Rolle „Protokollierung“** — Wird verwendet, um Einträge bei Amazon zu protokollieren CloudWatch. Transfer Family verwendet diese Rolle, um Erfolgs- und Fehlschlagsdetails sowie Informationen zu Dateiübertragungen zu protokollieren. Transfer Family übernimmt diese Rolle im Kontext eines Transfer Family Family-Servers ARN. Für ausgehende AS2-Übertragungen verwendet die Protokollierungsrolle den Connector-ARN.
- **Ausführungsrolle** — Ermöglicht es einem Transfer Family Family-Benutzer, Workflows aufzurufen und zu starten. Transfer Family übernimmt diese Rolle im Zusammenhang mit einem Transfer Family Family-Workflow-ARN.

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

Note

Ersetzen Sie in den folgenden Beispielen jedes Beispiel *user input placeholder* durch Ihre eigenen Informationen.

Note

In unseren Beispielen verwenden wir `ArnLike` sowohl als auch `ArnEquals`. Sie sind funktionell identisch, weshalb Sie beide verwenden können, wenn Sie Ihre Richtlinien erstellen. Die Dokumentation Transfer Family verwendet `ArnLike`, wenn die Bedingung ein Platzhalterzeichen enthält, und `ArnEquals` um eine exakte Übereinstimmungsbedingung anzugeben.

AWS Transfer Family Benutzerrolle dienstübergreifend verwirrt stellvertretend Prävention

Die folgende Beispielrichtlinie ermöglicht es jedem Benutzer eines beliebigen Servers im Konto, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/"
        }
      }
    }
  ]
}
```



```

    }
  }
]
}

```

Die folgende Beispielrichtlinie ermöglicht es jedem Benutzer eines bestimmten Servers, die Rolle zu übernehmen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/"
        }
      }
    }
  ]
}

```

Die folgende Beispielrichtlinie ermöglicht es einem bestimmten Benutzer eines bestimmten Servers, die Rolle zu übernehmen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",

```

```

    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:user/server-id/user-name"
      }
    }
  }
]
}

```

AWS Transfer Family Arbeitsablauf Rolle dienstübergreifend verwirrt stellvertretend Prävention

Mit der folgenden Beispielrichtlinie kann jeder Workflow im Konto diese Rolle übernehmen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/*"
        }
      }
    }
  ]
}

```

```
}
```

Die folgende Beispielrichtlinie ermöglicht es einem bestimmten Workflow, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-  
west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}
```

AWS Transfer Family Konnektor Rolle dienstübergreifend verwirrt stellvertretend Prävention

Die folgende Beispielrichtlinie ermöglicht es jedem Connector im Konto, diese Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
```

```

        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
            }
        }
    }
}

```

Die folgende Beispielrichtlinie ermöglicht es einem bestimmten Connector, die Rolle zu übernehmen.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/connector-id"
                }
            }
        }
    ]
}

```

AWS Transfer Family Familienprotokollierung und Anrufrolle dienstübergreifend verwirrte Stellvertreterprävention

Note

Die folgenden Beispiele können sowohl für Protokollierungs- als auch für Aufrufrollen verwendet werden.

In diesen Beispielen können Sie die ARN-Details für einen Workflow entfernen, wenn an Ihren Server keine Workflows angehängt sind.

Die folgende logging/invoke Beispielrichtlinie ermöglicht es jedem Server (und Workflow) im Konto, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

Die folgende logging/invoke Beispielrichtlinie ermöglicht es einem bestimmten Server (und Workflow), die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/server-id",
            "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}
```

AWS verwaltete Richtlinien für AWS Transfer Family

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, [kundenverwaltete AWS Identity and Access Management \(IAM\) Richtlinien zu erstellen](#), die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS -Richtlinien finden Sie unter [Verwaltete AWS -Richtlinien](#) im IAM-Leitfaden. Eine detaillierte Liste aller AWS verwalteten Richtlinien finden Sie im [Referenzhandbuch für AWS verwaltete Richtlinien](#).

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in [Verwaltete AWS -Richtlinien für Auftragsfunktionen](#) im IAM-Leitfaden.

AWS verwaltete Richtlinie: `AWSTransferConsoleFullAccess`

Die `AWSTransferConsoleFullAccess` Richtlinie bietet vollen Zugriff auf Transfer Family über die AWS Management Console. Weitere Informationen finden Sie unter [Service-linked Rolle für AWS Transfer Family](#).

AWS verwaltete Richtlinie: `AWSTransferFullAccess`

Die `AWSTransferFullAccess` Richtlinie bietet vollen Zugriff auf die Dienste von Transfer Family. Weitere Informationen finden Sie unter [Service-linked Rolle für AWS Transfer Family](#).

AWS verwaltete Richtlinie: `AWSTransferLoggingAccess`

Die `AWSTransferLoggingAccess` Richtlinie gewährt AWS Transfer Family vollen Zugriff, um Protokollstreams und Gruppen zu erstellen und Protokollereignisse in Ihrem Konto zu speichern. Weitere Informationen finden Sie unter [Service-linked Rolle für AWS Transfer Family](#).

AWS verwaltete Richtlinie: `AWSTransferReadOnlyAccess`

Die `AWSTransferReadOnlyAccess` Richtlinie bietet Lesezugriff auf die Transfer Family Family-Dienste. Weitere Informationen finden Sie unter [Service-linked Rolle für AWS Transfer Family](#).

AWS Familienupdates auf AWS verwaltete Richtlinien übertragen

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Transfer Family an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der [Dokumenthistorie für AWS Transfer Family](#)-Seite.

Änderungen	Beschreibung	Date
Aktualisierung der Dokumentation	Es wurden Abschnitte für jede der von Transfer Family verwalteten Richtlinien hinzugefügt.	27. Januar 2022
AWSTransferReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Transfer Family hat neue Berechtigungen hinzugefügt, damit die Richtlinie gelesen werden kann AWS Managed Microsoft AD.	30. September 2021
AWS Transfer Family hat begonnen, Änderungen zu verfolgen	AWS Transfer Family begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	15. Juni 2021

Terraform-Module der Transfer Family

[HashiCorp Terraform](#) ist eine Open-Source-Engine für Infrastructure as Code (IaC), die mit der HashiCorp Configuration Language (HCL) entwickelt wurde. Terraform bietet einen konsistenten CLI- (Command Line Interface) -Workflow, der in Verbindung mit AWS Transfer Family für die Back-End-Infrastruktur Hunderte von Cloud-Diensten verwalten und Cloud-APIs in deklarativen Konfigurationsdateien kodifizieren kann.

Sie können Terraform verwenden, um SFTP-Server und SFTP-Konnektoren der AWS Transfer Family zusammen mit den zugehörigen Abhängigkeiten und Anpassungen sicher bereitzustellen. Das Repository, das Terraform-Code enthält, um die Ressourcen zu erstellen, die für die Ausführung von AWS Transfer Family erforderlich sind, finden Sie im Quellcode des [Terraform Transfer Family Family-Moduls](#) unter. GitHub

Note

Die AWS Transfer Family Family-Module für Terraform sind ein von der Community unterstütztes Projekt. Sie sind nicht Teil eines AWS Dienstes. Best-effort Der Support wird von der AWS Storage-Community bereitgestellt.

SFTP-Server

Diese Automatisierung bietet Ihnen ein anpassbares Terraform-Modul und umfassende Beispiele zur Erstellung eines SFTP-Endpunkts (PUBLICoder VPC von Endpunkttypen), zur Integration mit Amazon CloudWatch für die Protokollierung und Überwachung, zur Verwaltung von Benutzeridentitäten für den Endpunktzugriff und zur Konfiguration von IAM-Rollen für den Zugriff auf Amazon S3 S3-Buckets, in denen Dateien gespeichert sind. Das Modul unterstützt mehrere öffentliche SSH-Schlüssel pro Benutzer (bis zu 50 Schlüssel) für verbesserte Sicherheit und Funktionen zur Schlüsselrotation.

SFTP-Anschlüsse

AWS Das Terraform-Modul Transfer Family unterstützt jetzt den Einsatz von SFTP-Konnektoren für die Übertragung von Dateien zwischen Amazon S3 und Remote-SFTP-Servern. SFTP-Konnektoren bieten vollständig verwaltete Low-Code-Funktionen zum Kopieren von Dateien zwischen Amazon S3 und Remote-SFTP-Servern.

Sie können Terraform jetzt verwenden, um Ihre SFTP-Konnektoren, die zugehörigen Abhängigkeiten und Anpassungen programmgesteuert in einer einzigen Bereitstellung bereitzustellen. Das Modul bietet auch umfassende Beispiele zur Automatisierung von Dateiübertragungsworkflows auf der Grundlage eines Zeitplans oder von Ereignisauslösern. Die Verwendung von Terraform für die Bereitstellung macht zeitaufwändige und fehleranfällige manuelle Konfigurationen überflüssig und bietet Ihnen eine schnelle, wiederholbare und sichere Bereitstellungsoption, die skalierbar ist.

AS2

Um die Unterstützung für AS2-Terraform-Vorlagen anzuzeigen, fügen Sie der Funktionsanfrage für [Terraform-Vorlagen der Transfer Family](#) eine Reaktion mit dem Daumen hoch (#) hinzu. Sie können auch einen Kommentar hinzufügen, der Ihren Anwendungsfall beschreibt.

B2B-Datenaustausch

AWS B2B Data Interchange automatisiert die Transformation, Validierung und Generierung von EDI-Dokumenten (Electronic Data Interchange) in und aus JSON- und XML-Datenformaten. [Um zu zeigen, dass Terraform-Vorlagen für den B2B-Datenaustausch unterstützt werden, fügen Sie der Funktionsanfrage eine Reaktion mit dem Daumen hoch \(#\) hinzu.](#) Sie können auch einen Kommentar hinzufügen, der Ihren Anwendungsfall beschreibt.

Problembehebung AWS Transfer Family

Dieses Kapitel enthält Informationen zur Fehlerbehebung für häufig auftretende Probleme, die bei der Verwendung auftreten können AWS Transfer Family. Jeder Abschnitt konzentriert sich auf einen bestimmten Funktionsbereich, damit Sie schnell Lösungen für Ihre Probleme finden können.

- Informationen zu Problemen mit IAM in Transfer Family finden Sie unter [Problembehandlung bei AWS Transfer Family Identität und Zugriff](#).
- Informationen zu Problemen mit Ihren Transfer Family Family-Web-Apps finden Sie unter [Fehlerbehebung bei Ihren Web-Apps](#).

Themen

- [Behebung von Authentifizierungsproblemen](#)
- [Behebung von Problemen mit dem SFTP-Connector](#)
- [Behebung von SFTP-Konnektivitäts- und Übertragungsproblemen](#)
- [Probleme mit benutzerdefinierten Identitätsanbietern beheben](#)
- [Workflow-Probleme beheben](#)
- [Behebung von EFS-Problemen](#)
- [Behebung von Speicher- und Verschlüsselungsproblemen](#)
- [Behebung von Überwachungs- und Warnproblemen](#)
- [Behebung von Problemen bei der Übertragung zwischen Regionen](#)
- [Behebung von Problemen bei der Terraform-Bereitstellung](#)
- [Behebung von Integrationsproblemen mit der Web Application Firewall](#)
- [Behebung von Problemen mit serviceverwalteten Benutzern](#)
- [AS2-Probleme beheben](#)

Behebung von Authentifizierungsproblemen

In diesem Abschnitt werden mögliche Lösungen für die folgenden Authentifizierungsprobleme beschrieben.

Themen

- [Authentifizierungsfehler— SSH/SFTP](#)
- [Problem mit nicht übereinstimmenden verwalteten AD-Bereichen](#)
- [Die Active Directory-Gruppenlimits wurden überschritten](#)
- [Verschiedene Probleme bei der Authentifizierung](#)
- [Probleme mit Amazon API Gateway beheben](#)
- [Beheben Sie Fehler beim Testen Ihres Identitätsanbieters](#)
- [Doppelte Amazon S3 S3-Buckets in der Web-App](#)

Authentifizierungsfehler— SSH/SFTP

Beschreibung

Wenn Sie versuchen, mithilfe des Secure Shell (SSH) File Transfer Protocol (SFTP) eine Verbindung zu Ihrem Server herzustellen, erhalten Sie eine Meldung, die der folgenden ähnelt:

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

Wenn Sie ein API Gateway verwenden und dieser Fehler angezeigt wird, finden Sie weitere Informationen unter [Zu viele Authentifizierungsfehler](#).

Ursache

Sie haben kein RSA-Schlüsselpaar für Ihren Benutzer hinzugefügt, daher müssen Sie sich stattdessen mit einem Passwort authentifizieren.

Lösung

Wenn Sie den `sftp` Befehl ausführen, geben Sie die `-o PubkeyAuthentication=no` Option an. Diese Option zwingt das System, Ihr Passwort anzufordern. Beispiel:

```
sftp -o PubkeyAuthentication=no sftp-user@server-id.server.transfer.region-id.amazonaws.com
```

Problem mit nicht übereinstimmenden verwalteten AD-Bereichen

Beschreibung

Der Bereich eines Benutzers und sein Gruppenbereich müssen übereinstimmen. Sie müssen sich beide im Standardbereich oder beide im vertrauenswürdigen Bereich befinden.

Ursache

Wenn ein Benutzer und seine Gruppe nicht übereinstimmen, kann der Benutzer nicht von Transfer Family authentifiziert werden. Wenn Sie den Identitätsanbieter für den Benutzer testen, erhalten Sie die Fehlermeldung Kein zugeordneter Zugriff für Benutzergruppen gefunden.

Lösung

Verweisen Sie auf eine Gruppe im Bereich des Benutzers, die dem Gruppenbereich entspricht (entweder Standard oder vertrauenswürdig).

Die Active Directory-Gruppenlimits wurden überschritten

Beschreibung

Wenn Sie versuchen, Ihrem AWS Transfer Family Server weitere Active Directory-Gruppen hinzuzufügen, erhalten Sie eine Fehlermeldung, die besagt, dass Sie die maximal zulässige Anzahl von Gruppen erreicht haben.

Ursache

AWS Transfer Family hat ein Standardlimit von 100 Active Directory-Gruppen pro Server.

Lösung

Dies sind zwei mögliche Lösungen:

- Konsolidieren Sie Ihre Active Directory-Gruppen, um die benötigte Gesamtzahl zu reduzieren.
- Wenn Ihr Anwendungsfall mehr als 100 Gruppen erfordert, sollten Sie die Verwendung einer benutzerdefinierten Identitätsanbieterlösung in Betracht ziehen, wie unter [Vereinfachen der Active Directory-Authentifizierung mit einem benutzerdefinierten Identitätsanbieter für](#) beschrieben AWS Transfer Family.

Verschiedene Probleme bei der Authentifizierung

Beschreibung

Sie erhalten einen Authentifizierungsfehler und keine der anderen Problembehebungsmaßnahmen funktioniert

Ursache

Möglicherweise haben Sie ein Ziel für ein logisches Verzeichnis angegeben, das einen führenden oder abschließenden Schrägstrich (/) enthält.

Lösung

Aktualisieren Sie Ihr logisches Verzeichnisziel, um sicherzustellen, dass es mit einem Schrägstrich beginnt und keinen abschließenden Schrägstrich enthält. `/amzn-s3-demo-bucket/images` Das ist zum Beispiel akzeptabel, aber auch nicht `amzn-s3-demo-bucket/images`. `/amzn-s3-demo-bucket/images/`

Probleme mit Amazon API Gateway beheben

In diesem Abschnitt werden mögliche Lösungen für die folgenden API-Gateway-Probleme beschrieben.

Themen

- [Zu viele Authentifizierungsfehler](#)
- [Die Verbindung wurde geschlossen](#)

Zu viele Authentifizierungsfehler

Beschreibung

Wenn Sie versuchen, mithilfe des Secure Shell (SSH) File Transfer Protocol (SFTP) eine Verbindung zu Ihrem Server herzustellen, wird die folgende Fehlermeldung angezeigt:

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

Ursache

Möglicherweise haben Sie ein falsches Passwort für Ihren Benutzer eingegeben. Versuchen Sie erneut, das richtige Passwort einzugeben.

Wenn das Passwort korrekt ist, kann das Problem durch eine ungültige Rolle mit dem Amazon Resource Name (ARN) verursacht werden. Um zu bestätigen, dass dies das Problem ist, testen Sie den Identitätsanbieter für Ihren Server. Wenn Sie eine Antwort ähnlich der folgenden sehen, ist der Rollen-ARN nur ein Platzhalter, wie durch den Rollen-ID-Wert aller Nullen angezeigt wird:

```
{
  "Response": "{\\"Role\\": \\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\",
  \\"HomeDirectory\\": \\"/\\"}",
  "StatusCode": 200,
  "Message": "",
  "Url": "https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/
servers/transfer-server-ID/users/myuser/config"
}
```

Lösung

Ersetzen Sie die Platzhalterrolle ARN durch eine tatsächliche Rolle, die berechtigt ist, auf den Server zuzugreifen.

So aktualisieren Sie die Rolle

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>
2. Wählen Sie im linken Navigationsbereich Stack aus.
3. Wählen Sie in der Liste „Stacks“ Ihren Stack und anschließend den Tab „Parameter“ aus.
4. Wählen Sie Aktualisieren aus. Wählen Sie auf der Seite Stack aktualisieren die Option Aktuelle Vorlage verwenden und dann Weiter aus.
5. UserRoleArn Ersetzen Sie es durch einen Rollen-ARN, der über ausreichende Berechtigungen für den Zugriff auf Ihren Transfer Family Family-Server verfügt.

Note

Um die erforderlichen Berechtigungen zu gewähren, können Sie die AmazonAPIGatewayAdministrator und die AmazonS3FullAccess verwalteten Richtlinien zu Ihrer Rolle hinzufügen.

6. Wählen Sie Weiter und dann erneut Weiter. Wählen Sie auf der *stack* Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden, und wählen Sie dann Stack aktualisieren aus.

Die Verbindung wurde geschlossen

Beschreibung

Wenn Sie versuchen, mithilfe des Secure Shell (SSH) File Transfer Protocol (SFTP) eine Verbindung zu Ihrem Server herzustellen, wird die folgende Fehlermeldung angezeigt:

```
Connection closed
```

Ursache

Eine mögliche Ursache für dieses Problem ist, dass Ihre CloudWatch Amazon-Logging-Rolle kein Vertrauensverhältnis zu Transfer Family hat.

Lösung

Stellen Sie sicher, dass die Protokollierungsrolle für den Server eine Vertrauensbeziehung mit Transfer Family hat. Weitere Informationen finden Sie unter [So stellen Sie eine Vertrauensbeziehung her](#).

Beheben Sie Fehler beim Testen Ihres Identitätsanbieters

Beschreibung

Wenn Sie Ihren Identitätsanbieter mithilfe der Konsole oder der TestIdentityProvider API-Operation testen, ist das Response Feld leer. Beispiel:

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

Ursache

Die wahrscheinlichste Ursache ist, dass die Authentifizierung aufgrund eines falschen Benutzernamens oder Passworts fehlgeschlagen ist.

Lösung

Stellen Sie sicher, dass Sie die richtigen Anmeldeinformationen für Ihren Benutzer verwenden, und aktualisieren Sie gegebenenfalls den Benutzernamen oder das Passwort.

Doppelte Amazon S3 S3-Buckets in der Web-App

Beschreibung

Derselbe Amazon S3 S3-Bucket wird mehrmals in der Oberfläche der Transfer Family Family-Web-App angezeigt.

Ursache

Dies ist der Fall, wenn ein Benutzer mehreren Active Directory-Gruppen angehört, die Berechtigungen für denselben Amazon S3 S3-Bucket haben. Die Web-App listet alle Zuschüsse auf oberster Ebene auf, die mit der UID oder GID des Benutzers verknüpft sind, einschließlich doppelter Zuschüsse für denselben Bucket-Standort.

Lösung

Um doppelte Angebote zu vermeiden, sollten Sie Zuschüsse so konsolidieren, dass jedem Benutzer nur ein Zuschuss pro Amazon S3 S3-Standort zur Verfügung steht. Überprüfen Sie Ihre Amazon S3 Access Grants-Konfiguration und entfernen Sie redundante Zuweisungen für denselben Bucket in verschiedenen Active Directory-Gruppen.

Behebung von Problemen mit dem SFTP-Connector

In diesem Abschnitt werden mögliche Lösungen für Probleme mit SFTP-Anschlüssen beschrieben.

Themen

- [Beheben Sie Probleme beim Hinzufügen vertrauenswürdiger Hostschlüssel für Ihren SFTP-Connector](#)
- [Die Schlüsselerhandlung schlägt fehl](#)
- [Drosselung des SFTP-Anschlusses](#)

- [Optimierung der Leistung des SFTP-Connectors](#)
- [Behebung von VPC-Verbindungsproblemen](#)
- [Verschiedene Probleme mit dem SFTP-Connector](#)

Beheben Sie Probleme beim Hinzufügen vertrauenswürdiger Hostschlüssel für Ihren SFTP-Connector

Beschreibung

Wenn Sie einen SFTP-Connector erstellen oder bearbeiten und einen vertrauenswürdigen Hostschlüssel hinzufügen, wird die folgende Fehlermeldung angezeigt: `Failed to edit connector details (Invalid host key format.)`

Ursache

Wenn Sie einen korrekten öffentlichen Schlüssel einfügen, liegt das Problem möglicherweise darin, dass Sie den `comment` Teil des Schlüssels eingefügt haben. AWS Transfer Family akzeptiert derzeit den Kommentarteil des Schlüssels nicht.

Lösung

Löscht den Kommentarteil des Schlüssels, wenn Sie ihn in das Textfeld einfügen. Gehen Sie beispielsweise davon aus, dass Ihr Schlüssel wie folgt aussieht:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Entfernen Sie den Text, der auf die `==` Zeichen folgt, und fügen Sie nur den Teil des Schlüssels ein, der `==` bis einschließlich

```
ssh-rsa AAAA...==
```

Die Schlüsselerhandlung schlägt fehl

Beschreibung

Sie erhalten eine Fehlermeldung, wenn die Schlüsselaustauschverhandlung fehlschlägt. Beispiel:

```
Key exchange negotiation failed due to incompatible host key algorithms.
```

```
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

Ursache

Dieser Fehler ist darauf zurückzuführen, dass es keine Überschneidung zwischen den vom Server unterstützten Host-Schlüsselalgorithmen und den vom Connector unterstützten Algorithmen gibt.

Lösung

Stellen Sie sicher, dass der Remoteserver mindestens einen der in der Fehlermeldung aufgeführten Client-Host-Schlüsselalgorithmen unterstützt. Eine Liste der unterstützten Algorithmen finden Sie unter [Sicherheitsrichtlinien für SFTP-Konnektoren AWS Transfer Family](#).

Drosselung des SFTP-Anschlusses

Beschreibung

Bei der Verwendung von SFTP-Konnektoren für Dateiübertragungen treten Fehler auf wie:

```
{"type":"ExecutionThrottled","details":{},"connectorId":"c-1234567890abcdef0"}
```

Oder Sie stellen fest, dass Dateiübertragungen bei Vorgängen mit hohem Volumen verzögert werden oder zeitweise fehlschlagen.

Ursache

SFTP-Konnektoren verfügen über Dienstkontingente, die die Anzahl gleichzeitiger Dateiübertragungen und API-Operationen begrenzen. Wenn diese Grenzwerte überschritten werden, erfolgt eine Drosselung, um den Service zu schützen und eine faire Nutzung durch alle Kunden sicherzustellen.

Lösung

Probieren Sie die folgenden Lösungen aus, um Probleme mit dem SFTP-Connector zu beheben:

1. Implementieren Sie exponentielle Backoff- und Wiederholungslogik in Ihren Anwendungen. Erstellen Sie beispielsweise eine Funktion, die fehlgeschlagene Operationen automatisch wiederholt, wobei die Wartezeiten zwischen den Versuchen zunehmen.
2. Implementieren Sie die Ratenbegrenzung in Ihrer Anwendung:

- Beschränken Sie die Anzahl gleichzeitiger Übertragungen.
 - Fügen Sie Verzögerungen zwischen Übertragungstapeln hinzu.
3. Überwachen Sie Ihre Nutzung anhand der Servicekontingente:
- Verwenden Sie CloudWatch Metriken, um die API-Nutzung zu verfolgen.
 - Richten Sie Alarme ein, um Sie zu benachrichtigen, wenn sich die Kontingentgrenzen nähern.
4. Optionen zur Skalierung Ihrer SFTP-Anschlüsse finden Sie unter [Skalierung Ihrer SFTP-Konnektoren](#).
5. Wenn die Drosselung weiterhin besteht und sich auf Ihren Geschäftsbetrieb auswirkt, fordern Sie über die Service-Kontingents-Konsole eine Erhöhung des Kontingents an.

Optimierung der Leistung des SFTP-Connectors

Beschreibung

Ihre SFTP-Connector-Übertragungen sind langsamer als erwartet, oder es kommt zu einer inkonsistenten Leistung.

Ursache

Die Leistung des SFTP-Connectors kann durch verschiedene Faktoren beeinflusst werden, darunter Netzwerkbedingungen, Dateigrößen, Remoteserverkonfiguration und Beschränkungen für gleichzeitige Übertragungen.

Lösung

So optimieren Sie die Leistung des SFTP-Connectors:

- Konfigurieren Sie Ihren Remote-SFTP-Server für eine optimale Leistung:
 - Erhöhen Sie die maximale Anzahl an Sitzungen und Übertragungen pro Sitzung
 - Optimieren Sie die TCP-Fenstergrößen für Verbindungen mit hoher Latenz
 - Verwenden Sie die Komprimierung, wenn sie von beiden Seiten unterstützt wird
- Erwägen Sie die Netzwerkoptimierung, indem Sie Ihren Transfer Family Family-Connector in einer Region in der Nähe Ihres Remote-SFTP-Servers platzieren.
- Implementieren Sie eine Überwachungsstrategie, um Leistungsengpässe zu identifizieren:
 - Überwachen Sie den Netzwerkdurchsatz und die Latenz
 - Analysieren Sie Protokolle auf Muster bei langsamen Übertragungen

Behebung von VPC-Verbindungsproblemen

In diesem Abschnitt werden Lösungen für häufig auftretende Probleme mit LATTICE-enabled VPC_-SFTP-Konnektoren beschrieben.

Der Connector blieb im Status AUSSTEHEND hängen

Beschreibung

Ihr VPC_ LATTICE-enabled SFTP-Connector bleibt für einen längeren Zeitraum (mehr als 10 Minuten) im PENDING Status.

Ursache

Dies kann auf Verzögerungen bei der DNS-Auflösung, Probleme mit der Konfiguration von Resource Gateway oder Netzwerkzuordnungsproblemen mit VPC VPC-Lattice-Dienst zurückzuführen sein.

Lösung

Wenden Sie [sich AWS Support an AWS Contact](#)., um die Ursache des Problems zu analysieren. Sie können auch die folgende Problemumgehung ausprobieren.

1. Stellen Sie sicher, dass Ihr Resource Gateway den ACTIVE Status hat:

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifizier rgw-1234567890abcdef0
```

2. Stellen Sie sicher, dass Ihre Ressourcenkonfiguration richtig konfiguriert und aktiv ist:

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifizier rcfg-1234567890abcdef0
```

3. Stellen Sie sicher, dass Ihr Resource Gateway über Subnetze in mindestens zwei Availability Zones verfügt, die VPC Lattice unterstützen.
4. Wenn das Problem weiterhin besteht, löschen Sie den Connector und erstellen Sie ihn mit derselben Konfiguration neu.

Der Konnektor hat den Status FEHLER

Beschreibung

Ihr VPC_ LATTICE-enabled SFTP-Connector zeigt ERRORRED den Status mit Fehlerdetails an.

Ursache

Zu den häufigsten Ursachen gehören ein ungültiger ARN für die Ressourcenkonfiguration, unzureichende IP-Adressen in VPC-Subnetzen oder regionsübergreifende Versuche zur gemeinsamen Nutzung von Ressourcen.

Lösung

1. Überprüfen Sie die Fehlerdetails mithilfe von: `describe-connector`

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Stellen Sie sicher, dass der ARN für die Ressourcenkonfiguration korrekt ist und sich in derselben Region wie Ihr Connector befindet.
3. Stellen Sie sicher, dass Ihre VPC-Subnetze über ausreichend verfügbare IP-Adressen für das Resource Gateway verfügen.
4. Stellen Sie sicher, dass Ihr Ressourcenkonfigurationsziel (IP-Adresse oder DNS-Name) von Ihrer VPC aus erreichbar ist.

Fehler „Öffentliche IP-Adresse wird nicht unterstützt“

Beschreibung

Sie erhalten eine Fehlermeldung, wenn Sie versuchen, eine Ressourcenkonfiguration mit einer öffentlichen IP-Adresse zu erstellen: `ValidationException: IP address x.x.x.x is not in allowed ranges.`

Ursache

Ressourcenkonfigurationen für öffentliche Endpunkte müssen DNS-Namen verwenden, keine IP-Adressen.

Lösung

Verwenden Sie bei der Erstellung der Ressourcenkonfiguration den öffentlichen DNS-Namen Ihres SFTP-Servers anstelle seiner IP-Adresse:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \
```

```
--resource-gateway-identifier rgw-1234567890abcdef0 \  
--resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \  
--port-ranges 22
```

Fehler: Availability Zone wird nicht unterstützt

Beschreibung

Beim Erstellen eines Resource Gateways wird eine Fehlermeldung angezeigt: Subnet `subnet-xxx` is not valid because it is not in a supported Availability Zone.

Ursache

Nicht alle Availability Zones unterstützen VPC Lattice Cross-VPC Resource Access. In der Fehlermeldung sind die unterstützten AZs für Ihre Region aufgeführt.

Lösung

1. Erstellen Sie Subnetze in den unterstützten Availability Zones, die in der Fehlermeldung aufgeführt sind.
2. Aktualisieren Sie Ihr Resource Gateway so, dass es nur Subnetze von unterstützten AZs verwendet.
3. Stellen Sie sicher, dass Sie mindestens zwei Subnetze in verschiedenen unterstützten AZs haben.

Verbindungs-Timeouts mit VPC_LATTICE-Anschlüssen

Beschreibung

Bei Dateiübertragungen über VPC-Konnektoren kommt es zu Zeitüberschreitungen oder sie schlagen zeitweise fehl.

Ursache

VPC Lattice hat Verbindungslimits (350 Verbindungen pro Ressource) und Leerlauf-Timeouts (350 Sekunden für TCP).

Lösung

1. Überwachen Sie gleichzeitige Verbindungen, um das Limit von 350 Verbindungen pro Ressource einzuhalten.
2. Implementieren Sie Verbindungspooling und Wiederverwendung in Ihren Anwendungen.

3. Konfigurieren Sie entsprechende Timeout-Werte in Ihren SFTP-Clientanwendungen (weniger als 350 Sekunden).
4. Erwägen Sie, mehrere Ressourcenkonfigurationen für dasselbe Ziel zu erstellen, um die Last zu verteilen.

Verschiedene Probleme mit dem SFTP-Connector

Beschreibung

Sie erhalten nach der Ausführung eine Fehlermeldung `StartFileTransfer`, kennen aber die Ursache des Problems nicht, und nach dem API-Aufruf wird nur die Connector-ID zurückgegeben.

Ursache

Dieser Fehler kann mehrere Ursachen haben. Zur Fehlerbehebung empfehlen wir Ihnen, Ihren Connector zu testen und Ihre CloudWatch Logs zu durchsuchen.

Lösung

- Testen Sie Ihren Connector: Siehe [Testen Sie einen SFTP-Connector](#). Wenn der Test fehlschlägt, gibt das System eine Fehlermeldung aus, die auf dem Grund basiert, warum der Test fehlgeschlagen ist. In diesem Abschnitt wird beschrieben, wie Sie Ihren Connector entweder von der Konsole aus oder mithilfe des [TestConnection](#) API-Befehls testen.
- CloudWatch Logs für Ihren Connector anzeigen: Siehe [Beispielprotokolleinträge für SFTP-Konnektoren](#). Dieses Thema enthält Beispiele für Protokolleinträge für SFTP-Konnektoren und die Benennungskonvention, die Ihnen bei der Suche nach den entsprechenden Protokollen helfen soll.

Behebung von SFTP-Konnektivitäts- und Übertragungsproblemen

In diesem Abschnitt werden mögliche Lösungen für Probleme mit der SFTP-Konnektivität und der Dateiübertragung beschrieben.

Themen

- [Beheben Sie Probleme mit der SFTP-Konnektivität](#)
- [Beheben Sie Probleme mit dem SFTP-Client](#)
- [Beheben Sie Probleme beim Hochladen von Dateien](#)
- [Behebung von Problemen mit dem SFTP-Connector vom VPC-Ausgangstyp](#)

Beheben Sie Probleme mit der SFTP-Konnektivität

Beschreibung

Ihr SFTP-Client kann die Verbindung nicht initiieren. Dieses Problem kann kontinuierlich oder zeitweise auftreten. In den Debug-Protokollen Ihres SFTP-Clients könnten Sie beispielsweise die folgende Abfolge von Ereignissen sehen:

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Ursache

Es gibt einen Grenzfall, in dem das Null-Byte-TCP-ACK (ACK ohne Daten), auch bekannt als Drei-Wege-Handshake, entweder verworfen oder verzögert wird.

Lösung

Um dieses Problem zu umgehen, bietet Transfer Family eine Lösung, die eine andere Konfiguration verwendet, um dieses Problem zu lösen, aber zu Kompatibilitätsproblemen mit älteren Clients führen kann. Aus diesem Grund ist diese Lösung nur auf Port 2223 verfügbar.

Wenn Sie im Verfahren zum Erstellen eines Transfer Family Family-Servers in einer VPC ([Erstellen Sie einen Server in einer virtuellen privaten Cloud](#)) eine Sicherheitsgruppe angeben, konfigurieren Sie den SSH-Verkehr so, dass er Port 2223 verwendet.

Beheben Sie Probleme mit dem SFTP-Client

Clientseitige SFTP-Meldungen werden unter beschrieben. [SFTP-Nachrichten](#) Die beste Methode zur Behebung von Problemen mit dem SFTP-Client besteht darin, die Protokolle des SFTP-Clients zu überprüfen und sich gegebenenfalls an Ihren Netzwerkadministrator zu wenden.

Beheben Sie Probleme beim Hochladen von Dateien

In diesem Abschnitt werden mögliche Lösungen für die folgenden Probleme beim Hochladen von Dateien beschrieben.

Themen

- [Fehler beim Hochladen von Amazon S3 S3-Dateien beheben](#)
- [Beheben Sie Probleme mit unlesbaren Dateinamen](#)

Fehler beim Hochladen von Amazon S3 S3-Dateien beheben

Beschreibung

Wenn Sie versuchen, eine Datei mit Transfer Family in den Amazon S3 S3-Speicher hochzuladen, erhalten Sie die folgende Fehlermeldung: AWS Transfer unterstützt keine Direktzugriffsschreibvorgänge auf S3-Objekte.

Ursache

Wenn Sie Amazon S3 für den Speicher Ihres Servers verwenden, unterstützt Transfer Family nicht mehrere Verbindungen für eine einzelne Übertragung.

Lösung

Wenn Ihr Transfer Family Family-Server Amazon S3 als Speicher verwendet, deaktivieren Sie alle Optionen für Ihre Client-Software, die die Verwendung mehrerer Verbindungen für eine einzelne Übertragung erwähnen.

Beheben Sie Probleme mit unlesbaren Dateinamen

Beschreibung

In einigen Ihrer hochgeladenen Dateien werden beschädigte Dateinamen angezeigt. Benutzer stoßen manchmal auf Probleme mit FTP- und SFTP-Übertragungen, bei denen bestimmte Zeichen in Dateinamen unleserlich dargestellt werden, z. B. Umlaute, Buchstaben mit Akzenten oder bestimmte Schriften wie Chinesisch oder Arabisch.

Ursache

Die FTP- und SFTP-Protokolle ermöglichen zwar, dass die Zeichenkodierung von Dateinamen von Clients ausgehandelt wird, Amazon S3 und Amazon EFS jedoch nicht. Stattdessen benötigen sie eine UTF-8 Zeichenkodierung. Das hat zur Folge, dass bestimmte Zeichen nicht korrekt wiedergegeben werden.

Lösung

Um dieses Problem zu lösen, überprüfen Sie Ihre Client-Anwendung auf die Zeichenkodierung von Dateinamen und stellen Sie sicher, dass sie auf eingestellt ist UTF-8.

Behebung von Problemen mit dem SFTP-Connector vom VPC-Ausgangstyp

Wenn Sie Probleme mit SFTP-Anschlüssen vom Typ VPC-Ausgang haben, überprüfen Sie Folgendes:

Der Status des Connectors ist AUSSTEHEND

Beschreibung

Ihr VPC-Egress-Connector bleibt nach der Erstellung mehrere Minuten lang im Status AUSSTEHEND und TestConnection gibt „Connector nicht verfügbar“ zurück.

Ursache

Es kann mehrere Minuten dauern, bis die DNS-Auflösung für VPC-Connectoren nach der Erstellung abgeschlossen ist.

Lösung

Warten Sie, bis der Connector-Status AKTIV wird, bevor Sie versuchen, Dateien zu übertragen. Dies ist ein normales Verhalten für VPC-Ausgangsanschlüsse.

Verbindungs-Timeouts

Beschreibung

Beim Versuch, eine Verbindung zum SFTP-Server herzustellen, tritt bei VPC VPC-Connector ein Timeout auf.

Ursache

Sicherheitsgruppen lassen möglicherweise keinen Verkehr auf Port 22 zwischen Ihren Resource Gateway-Subnetzen und dem Ziel-SFTP-Server zu.

Lösung

Stellen Sie sicher, dass Sicherheitsgruppen Datenverkehr auf Port 22 zwischen Ihren Resource Gateway-Subnetzen und dem Ziel-SFTP-Server zulassen.

Fehler bei der Ressourcenkonfiguration

Beschreibung

Ihr VPC-Ausgangsconnector kann aufgrund von Problemen mit der Ressourcenkonfiguration keine Verbindung herstellen.

Ursache

Die Ressourcenkonfiguration verweist möglicherweise auf eine falsche IP-Adresse oder einen falschen DNS-Namen, oder das Resource Gateway befindet sich möglicherweise nicht in derselben VPC wie Ihr SFTP-Server (für private Endpunkte).

Lösung

Stellen Sie sicher, dass Ihre Ressourcenkonfiguration auf die richtige IP-Adresse oder den richtigen DNS-Namen verweist und dass sich das Resource Gateway in derselben VPC wie Ihr SFTP-Server befindet (für private Endpunkte). Weitere Informationen finden Sie unter [Ressourcenkonfigurationen](#) im Benutzerhandbuch für Amazon VPC Lattice.

Probleme mit öffentlichen Endpunkten

Beschreibung

Ihr VPC-Ausgangsconnector kann keine Verbindung zu öffentlichen SFTP-Endpunkten herstellen.

Ursache

Für öffentliche Endpunkte müssen Sie in Ihrer Ressourcenkonfiguration einen DNS-Namen (keine IP-Adresse) verwenden, und Ihre VPC muss über ein NAT-Gateway für den ausgehenden Internetzugang verfügen.

Lösung

Stellen Sie sicher, dass Sie in Ihrer Ressourcenkonfiguration einen DNS-Namen und keine IP-Adresse verwenden. Stellen Sie sicher, dass Ihre VPC über ein NAT-Gateway für ausgehenden Internetzugang verfügt.

Probleme mit der Availability Zone

Beschreibung

Aufgrund von Einschränkungen der Availability Zone können Sie kein Resource Gateway erstellen.

Ursache

Resource Gateways benötigen Subnetze in mindestens 2 Availability Zones, und nicht alle AZs unterstützen VPC Lattice.

Lösung

Überprüfen Sie die unterstützten Availability Zones für VPC Lattice in Ihrer Region und stellen Sie sicher, dass Sie Subnetze in mindestens 2 unterstützten AZs haben.

Probleme mit benutzerdefinierten Identitätsanbietern beheben

In diesem Abschnitt werden mögliche Lösungen für Probleme im Zusammenhang mit benutzerdefinierten Identitätsanbietern mit Transfer Family beschrieben.

Themen

- [Beheben Sie Fehler bei der API Gateway Gateway-Integration](#)
- [Behebung von Timeouts bei Lambda-Funktionen](#)
- [Behebung konsistenter Lambda-Timeout-Probleme](#)
- [Beheben Sie Ausnahmen KeyError](#)

Beheben Sie Fehler bei der API Gateway Gateway-Integration

Beschreibung

Benutzer können sich nicht bei Ihrem Transfer Family Family-Server authentifizieren, und beim Testen Ihres Identitätsanbieters werden Fehler wie die folgenden angezeigt:

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Ursache

Fehler bei der API Gateway Gateway-Integration können aus folgenden Gründen auftreten:

- Falsche API-Gateway-Konfiguration
- Lambda-Funktionsfehler werden nicht richtig behandelt
- Berechtigungsprobleme zwischen API Gateway und Lambda
- Fehlerhafte Antworten der Lambda-Funktion

Lösung

Um Fehler bei der API Gateway Gateway-Integration zu beheben:

1. Detaillierte Fehlerinformationen finden Sie in Ihren Lambda-Funktionsprotokollen:
 - Navigieren Sie in der CloudWatch Konsole zu Protokollgruppen `>/aws/lambda/your-function-name`
 - Suchen Sie nach Fehlermeldungen oder Stack-Traces, die auf die Ursache hinweisen
2. Stellen Sie sicher, dass Ihre Lambda-Funktion korrekt formatierte Antworten zurückgibt:

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
  "HomeDirectory": "/mybucket/home/username"
}
```

3. Aktivieren Sie die detaillierte CloudWatch Protokollierung für API Gateway:
 - Wählen Sie in der API Gateway Gateway-Konsole Ihre API aus und wählen Sie Stages
 - Wählen Sie Ihre Phase aus und aktivieren Sie unter Logs/TracingCloudWatch Logs
 - Stellen Sie die Protokollebene auf FEHLER oder INFO ein
4. Testen Sie Ihren API-Gateway-Endpoint direkt:

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-server-id/users/username/config \
-H "Content-Type: application/json" \
-d '{"Password": "password"}'
```

5. Überprüfen Sie die Berechtigungen zwischen API Gateway und Lambda:
 - Stellen Sie sicher, dass API Gateway berechtigt ist, Ihre Lambda-Funktion aufzurufen
 - Überprüfen Sie, ob die Ausführungsrolle für Ihre Lambda-Funktion über die erforderlichen Berechtigungen verfügt

Behebung von Timeouts bei Lambda-Funktionen

Beschreibung

Wenn Benutzer versuchen, sich mit einem benutzerdefinierten Identitätsanbieter bei Ihrem Transfer Family Family-Server zu authentifizieren, kommt es zu langen Verzögerungen, gefolgt von Authentifizierungsfehlern. In Ihren Lambda-Protokollen werden Timeout-Fehler angezeigt.

Ursache

Lambda-Funktionen, die für benutzerdefinierte Identitätsanbieter verwendet werden, haben ein Standard-Timeout von 3 Sekunden. Wenn Ihre Authentifizierungslogik länger als dieses Timeout dauert (z. B. beim Abfragen externer Datenbanken oder bei API-Aufrufen an Identitätsanbieter von Drittanbietern), wird die Funktion unterbrochen und die Authentifizierung schlägt fehl.

Lösung

So lösen Sie Probleme mit Lambda-Timeout:

1. Erhöhen Sie das Timeout der Lambda-Funktion:
 - Navigieren Sie in der Lambda-Konsole zu Ihrer Funktion und wählen Sie die Registerkarte Konfiguration
 - Klicken Sie unter Allgemeine Konfiguration auf Bearbeiten
 - Erhöhen Sie den Timeout-Wert (bis zu 15 Sekunden werden für Authentifizierungsfunktionen empfohlen)
2. Optimieren Sie Ihren Lambda-Funktionscode:
 - Verwenden Sie Verbindungspooling für Datenbankabfragen
 - Implementieren Sie das Zwischenspeichern von Daten, auf die häufig zugegriffen wird
 - Minimiere externe API-Aufrufe während der Authentifizierung
3. Erwägen Sie die Verwendung von Lambda Provisioned Concurrency, um Kaltstarts zu vermeiden:

```
aws lambda put-provisioned-concurrency-config \
  --function-name my-authentication-function \
  --qualifier prod \
  --provisioned-concurrent-executions 5
```

4. Überwachen Sie die Lambda-Leistung mithilfe von CloudWatch Metriken und richten Sie Alarmer für Dauerschwellenwerte ein

Behebung konsistenter Lambda-Timeout-Probleme

Beschreibung

Benutzer erleben konsistente Timeouts, wenn sie eine Lambda-Funktion zur Authentifizierung verwenden.

Ursache

Lambda kann den entsprechenden AWS Dienst, der für die Authentifizierung verwendet wird, nicht erreichen (z. B. DynamoDB, Secrets Manager oder ein anderer Identitätsanbieter).

Lösung

Stellen Sie sicher, dass Subnetze Dienste erreichen können. AWS Oder, wenn Sie eine Verbindung zu einem Internet Identity Provider (wie Okta) herstellen, stellen Sie sicher, dass das Subnetz der Lambda-Funktion das Internet über ein NAT-Gateway erreichen kann

Beheben Sie Ausnahmen **KeyError**

Beschreibung

In Ihren Transfer Family Family-Protokolleinträgen finden Sie 'KeyError' Ausnahmen.

Ursache

Die wahrscheinlichste Ursache ist, dass der Benutzer oder der `identity_provider` Datensatz falsch formatiert ist oder dass Pflichtfelder fehlen.

Lösung

Suchen ERRORS Sie im Protokoll in der `/aws/transfer/your-server-id` Protokollgruppe nach Hinweisen.

Workflow-Probleme beheben

In diesem Abschnitt werden mögliche Lösungen für Probleme mit verwalteten Workflows beschrieben.

Themen

- [Beheben Sie Probleme mit verwalteten Workflows](#)
- [Beheben Sie Probleme mit der Workflow-Entschlüsselung](#)

Beheben Sie Probleme mit verwalteten Workflows

In diesem Abschnitt werden mögliche Lösungen für die folgenden Workflow-Probleme beschrieben.

Themen

- [Workflow-bezogene Fehler mithilfe von Amazon beheben CloudWatch](#)
- [Beheben Sie Fehler beim Kopieren von Workflows](#)

Workflow-bezogene Fehler mithilfe von Amazon beheben CloudWatch

Beschreibung

Wenn Sie Probleme mit Ihren Workflows haben, können Sie Amazon verwenden, CloudWatch um die Ursache zu untersuchen.

Ursache

Es kann mehrere Ursachen geben. Verwenden Sie Amazon CloudWatch Logs, um Nachforschungen anzustellen.

Lösung

Transfer Family gibt den Workflow-Ausführungsstatus in CloudWatch Logs aus. Die folgenden Arten von Workflow-Fehlern können in CloudWatch Protokollen auftreten:

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

Sie können die Ausführungsprotokolle Ihres Workflows mithilfe einer anderen Filter- und Mustersyntax filtern. Sie können beispielsweise einen Protokollfilter in Ihren CloudWatch Protokollen erstellen, um Workflow-Ausführungsprotokolle zu erfassen, die die ExecutionErroredNachricht enthalten. Einzelheiten finden Sie unter [Real-time Verarbeitung von Protokolldaten mit Abonnements](#) und [Filter- und Mustersyntax](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

StepErrored

```
2021-10-29T12:57:26.272-05:00
```

```

{"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
"workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
"transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}

```

StepErrored zeigt an, dass ein Schritt innerhalb des Workflows einen Fehler generiert hat. In einem einzigen Workflow können Sie mehrere Schritte konfigurieren. Dieser Fehler teilt Ihnen mit, in welchem Schritt der Fehler aufgetreten ist, und gibt eine Fehlermeldung aus. In diesem speziellen Beispiel wurde der Schritt so konfiguriert, dass er eine Datei kennzeichnet. Das Taggen einer Datei in einem Amazon EFS-Dateisystem wird jedoch nicht unterstützt, sodass der Schritt einen Fehler generierte.

ExecutionErrored

```

2021-10-29T12:57:26.618-05:00
{"type":"ExecutionErrored","details":{}, "workflowId":"w-w-
abcdef01234567890",
"executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
"username":"lhr","sessionId":"1234567890abcdef0"}}

```

Wenn ein Workflow keinen Schritt ausführen kann, generiert er eine **ExecutionErrored** Meldung. Wenn Sie beispielsweise einen einzelnen Schritt in einem bestimmten Workflow konfiguriert haben und der Schritt nicht ausgeführt werden kann, schlägt der gesamte Workflow fehl.

Die Ausführung wurde gedrosselt

Die Ausführung wird gedrosselt, wenn ein Workflow mit einer Geschwindigkeit ausgelöst wird, die schneller ist, als das System unterstützen kann. Diese Protokollmeldung weist darauf hin, dass Sie die Ausführungsrate für Workflows verlangsamen müssen. [Wenn Sie Ihre Workflow-Ausführungsrate nicht reduzieren können, wenden Sie sich AWS Support an Kontakt. AWS](#)

Dienstfehler beim Starten des Workflows

Jedes Mal, wenn Sie einen Workflow von einem Server entfernen und ihn durch einen neuen ersetzen oder die Serverkonfiguration aktualisieren (was sich auf die Ausführungsrolle eines Workflows auswirkt), müssen Sie ungefähr 10 Minuten warten, bevor Sie den neuen Workflow

ausführen. Der Transfer Family Family-Server speichert die Workflow-Details im Cache, und es dauert 10 Minuten, bis der Server seinen Cache aktualisiert hat.

Darüber hinaus müssen Sie sich von allen aktiven SFTP-Sitzungen abmelden und sich nach Ablauf der 10-minütigen Wartezeit wieder anmelden, um die Änderungen zu sehen.

Beheben Sie Fehler beim Kopieren von Workflows

Beschreibung

Wenn Sie einen Workflow ausführen, der einen Schritt zum Kopieren der hochgeladenen Datei enthält, kann der folgende Fehler auftreten:

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
    Status Code: 400; Error Code: 400 Bad Request;
    Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
    "stepType": "COPY", "stepName": "copy-step-name" },
    "workflowId": "workflow-ID",
    "executionId": "execution-ID",
    "transferDetails": {
      "serverId": "server-ID",
      "username": "user-name",
      "sessionId": "session-ID"
    }
  }
}
```

Ursache

Die Quelldatei befindet sich in einem Amazon S3 S3-Bucket, der sich in einem anderen AWS-Region als dem Ziel-Bucket befindet.

Lösung

Wenn Sie einen Workflow ausführen, der einen Kopierschritt beinhaltet, stellen Sie sicher, dass sich der Quell- und der Ziel-Bucket in demselben AWS-Region befinden.

Beheben Sie Probleme mit der Workflow-Entschlüsselung

In diesem Abschnitt werden mögliche Lösungen für die folgenden Probleme mit verschlüsselten Workflows beschrieben.

Themen

- [Beheben Sie Probleme mit der Verschlüsselung anonymer Empfänger](#)
- [Beheben Sie den Fehler für die signierte Verschlüsselungsdatei](#)
- [Beheben Sie einen Fehler für einen FIPS-Algorithmus](#)

Beheben Sie Probleme mit der Verschlüsselung anonymer Empfänger

Beschreibung

Ihr Entschlüsselungsworkflow schlägt fehl, wenn Sie bestimmte verschlüsselte Dateien verarbeiten, funktioniert aber mit anderen.

Ursache

Dateien wurden möglicherweise verschlüsselt, ohne dass ein Empfänger angegeben wurde (anonyme Verschlüsselung), sodass es für den Workflow schwierig ist, zu bestimmen, welcher Schlüssel für die Entschlüsselung verwendet werden soll.

Lösung

Verschlüsseln Sie Dateien mit einem nicht anonymen Empfänger immer mithilfe des Parameters. `-r`
Beispiel:

```
gpg -e -r user@example.com --openpgp file.txt
```

Um zu überprüfen, ob eine Datei mit einem bestimmten Empfänger oder anonym verschlüsselt wurde, verwenden Sie den folgenden Befehl: `--list-packets`

```
gpg --list-packets file.txt.gpg
```

Dieser Befehl zeigt die Paketstruktur der GPG-encrypted Datei an, ohne ihren Inhalt zu entschlüsseln. Suchen Sie nach einer Ausgabe, die Empfängerinformationen enthält, z. B.:

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Wenn Sie Schlüssel-ID-Informationen sehen, wurde die Datei für einen bestimmten Empfänger verschlüsselt. Wenn diese Informationen fehlen, wurde die Datei möglicherweise anonym verschlüsselt, was zu Entschlüsselungsfehlern in Transfer Family Family-Workflows führen kann.

Sie können diesen Befehl auch verwenden, um Folgendes zu überprüfen:

- Welche Verschlüsselungsalgorithmen wurden verwendet
- Komprimierungsmethoden (falls vorhanden)
- Zeitstempel der Erstellung

Um die Liste der unterstützten Verschlüsselungsalgorithmen für Ihre GPG-Installation einzusehen, verwenden Sie:

```
gpg --version
```

Mithilfe dieser Informationen können Sie sicherstellen, dass Sie Verschlüsselungsalgorithmen verwenden, die mit Transfer Family Family-Workflows kompatibel sind, insbesondere wenn FIPS-Konformität erforderlich ist.

Beheben Sie den Fehler für die signierte Verschlüsselungsdatei

Beschreibung

Ihr Entschlüsselungsworkflow schlägt fehl und Sie erhalten die folgende Fehlermeldung:

```
"Encrypted file with signed message unsupported"
```

Ursache

Transfer Family unterstützt derzeit nicht das Signieren von verschlüsselten Dateien.

Lösung

Wenn es in Ihrem PGP-Client eine Option zum Signieren der verschlüsselten Datei gibt, stellen Sie sicher, dass Sie die Auswahl deaktivieren, da Transfer Family derzeit das Signieren verschlüsselter Dateien nicht unterstützt.

Beheben Sie einen Fehler für einen FIPS-Algorithmus

Beschreibung

Ihr Entschlüsselungsworkflow schlägt fehl und die Protokollnachricht sieht wie folgt aus:

```
{  
  "type": "StepErrored",
```

```

"details": {
  "errorType": "BAD_REQUEST",
  "errorMessage": "File encryption algorithm not supported with FIPS mode
enabled.",
  "stepType": "DECRYPT",
  "stepName": "step-name"
},
"workflowId": "workflow-ID",
"executionId": "execution-ID",
"transferDetails": {
  "serverId": "server-ID",
  "username": "user-name",
  "sessionId": "session-ID"
}
}

```

Ursache

Auf Ihrem Transfer Family Family-Server ist der FIPS-Modus aktiviert und es gibt einen zugehörigen Workflow-Schritt „Entschlüsseln“. Beim Verschlüsseln der Dateien vor dem Hochladen auf Ihren Transfer Family Family-Server generiert der Verschlüsselungsclient möglicherweise verschlüsselte Dateien, die nicht von FIPS zugelassene symmetrische Verschlüsselungsalgorithmen verwenden. In einem solchen Szenario kann der Workflow keine Dateien entschlüsseln. Im folgenden Beispiel verwendet GnuPG Version 2.4.0 OCB (einen Nicht-FIPS-Blockchiffriermodus), um Dateien zu verschlüsseln: Dadurch schlägt der Workflow fehl.

Lösung

Sie müssen den GPG-Schlüssel, mit dem Sie Ihre Dateien verschlüsselt haben, bearbeiten und sie dann erneut verschlüsseln. Das folgende Verfahren beschreibt die Schritte, die Sie ausführen müssen.

Um Ihre PGP-Schlüssel zu bearbeiten

1. Identifizieren Sie den Schlüssel, den Sie bearbeiten müssen, indem Sie folgenden Befehl ausführen `gpg --list-keys`

Dies gibt eine Liste von Schlüsseln zurück. Jeder Schlüssel hat Details, die den folgenden ähneln:

```

pub   ed25519 2022-07-07 [SC]
      wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

```

```
uid          [ultimate] Mary Major <marymajor@example.com>
sub    cv25519 2022-07-07 [E]
```

2. Identifizieren Sie den Schlüssel, den Sie bearbeiten möchten. In dem im vorherigen Schritt gezeigten Beispiel lautet die IDwJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.
3. Führen Sie `gpg --edit-key wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Das System antwortet mit Details über das GnuPG-Programm und den angegebenen Schlüssel.

4. Geben Sie an der `gpg>` Eingabeaufforderung ein. `showpref` Die folgenden Details werden zurückgegeben:

```
[ultimate] (1). Mary Major <marymajor@example.com>
  Cipher: AES256, AES192, AES, 3DES
  AEAD: OCB
  Digest: SHA512, SHA384, SHA256, SHA224, SHA1
  Compression: ZLIB, BZIP2, ZIP, Uncompressed
  Features: MDC, AEAD, Keyserver no-modify
```

Beachten Sie, dass die bevorzugten Algorithmen, die auf dem Schlüssel gespeichert sind, aufgeführt sind.

5. Wir möchten den Schlüssel bearbeiten, um alle Algorithmen außer OCB beizubehalten. Führen Sie den `setpref` Befehl aus und geben Sie alle Algorithmen an, die beibehalten werden sollen:

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
  BZIP2, ZIP, Uncompressed
```

Dadurch werden die folgenden Details zurückgegeben:

```
Set preference list to:
  Cipher: AES256, AES192, AES, 3DES
  AEAD:
  Digest: SHA512, SHA384, SHA256, SHA224, SHA1
  Compression: ZLIB, BZIP2, ZIP, Uncompressed
  Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

6. Geben Sie ein, `y` um zu aktualisieren, und geben Sie dann Ihr Passwort ein, wenn Sie aufgefordert werden, die Änderung zu bestätigen.
7. Speichern Sie die Änderungen.

```
gpg> save
```

Bevor Sie Ihren Entschlüsselungsworkflow erneut ausführen, müssen Sie Ihre Dateien mit dem bearbeiteten Schlüssel erneut verschlüsseln.

Behebung von EFS-Problemen

In diesem Abschnitt werden mögliche Lösungen für Probleme mit Amazon EFS-Speicher beschrieben.

Themen

- [Probleme mit Amazon EFS beheben](#)

Probleme mit Amazon EFS beheben

In diesem Abschnitt werden mögliche Lösungen für die folgenden Amazon EFS-Probleme beschrieben.

Themen

- [Problembehandlung für vom Service verwaltete Amazon EFS-Benutzer](#)
- [Beheben Sie das fehlende POSIX-Profil](#)
- [Problembehandlung bei logischen Verzeichnissen mit Amazon EFS](#)

Problembehandlung für vom Service verwaltete Amazon EFS-Benutzer

Beschreibung

Sie führen den `sftp` Befehl aus und die Eingabeaufforderung wird nicht angezeigt. Stattdessen wird die folgende Meldung angezeigt:

```
Couldn't canonicalize: Permission denied
Need cwd
```

Ursache

Die Rolle Ihres AWS Identity and Access Management (IAM-) Benutzers ist nicht berechtigt, auf Amazon Elastic File System (Amazon EFS) zuzugreifen.

Lösung

Erhöhen Sie die Richtlinienberechtigungen für die Rolle Ihres Benutzers. Sie können eine AWS verwaltete Richtlinie hinzufügen, z. `AmazonElasticFileSystemClientFullAccess` B.

Beheben Sie das fehlende POSIX-Profil

Beschreibung

Wenn Sie Amazon EFS-Speicher für Ihren Server und einen benutzerdefinierten Identitätsanbieter verwenden, müssen Sie für Ihre AWS Lambda Funktion ein POSIX-Profil bereitstellen.

Ursache

Eine mögliche Ursache ist, dass die Vorlagen, die wir für die Erstellung einer Amazon API Gateway AWS Lambda Gateway-Methode bereitstellen, derzeit keine POSIX-Informationen enthalten.

Wenn Sie POSIX-Informationen angegeben haben, wird das Format, das Sie für die Bereitstellung der POSIX-Informationen verwendet haben, von Transfer Family möglicherweise nicht korrekt analysiert.

Lösung

Stellen Sie sicher, dass Sie Transfer Family ein JSON-Element für den `PosixProfile` Parameter bereitstellen.

Wenn Sie beispielsweise Python verwenden, könnten Sie die folgende Zeile hinzufügen, in der Sie den `PosixProfile` Parameter analysieren:

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

Oder Sie könnten die folgende Zeile hinzufügen, wobei die *uid-value* und Ganzzahlen 0 oder größer *gid-value* sind, die jeweils die Benutzer-ID (UID) und die Gruppen-ID (GID) darstellen: JavaScript

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

In diesen Codebeispielen `PosixProfile` wird der Parameter als JSON-Objekt und nicht als Zeichenfolge an Transfer Family gesendet.

Außerdem müssen Sie den `PosixProfile` Parameter darin AWS Secrets Manager wie folgt speichern. Ersetzen Sie *your-uid* und *your-gid* durch Ihre tatsächlichen Werte für GID und UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Problembehandlung bei logischen Verzeichnissen mit Amazon EFS

Beschreibung

Wenn das Home-Verzeichnis des Benutzers nicht existiert und er einen `ls` Befehl ausführt, reagiert das System wie folgt:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Ursache

Wenn Ihr Transfer Family Family-Server Amazon EFS verwendet, muss das Home-Verzeichnis für den Benutzer mit Lese- und Schreibzugriff erstellt werden, bevor der Benutzer in seinem logischen Home-Verzeichnis arbeiten kann. Der Benutzer kann dieses Verzeichnis nicht selbst erstellen, da ihm die entsprechenden Berechtigungen für `mkdir` sein logisches Home-Verzeichnis fehlen würden.

Lösung

Ein Benutzer mit Administratorzugriff auf das übergeordnete Verzeichnis muss das logische Basisverzeichnis des Benutzers erstellen.

Behebung von Speicher- und Verschlüsselungsproblemen

In diesem Abschnitt werden mögliche Lösungen für Probleme mit Speicher und Verschlüsselung beschrieben.

Themen

- [Richtlinien zur Fehlerbehebung für verschlüsselte Amazon S3 S3-Buckets](#)
- [Beheben Sie die ResourceNotFound Ausnahme](#)

Richtlinien zur Fehlerbehebung für verschlüsselte Amazon S3 S3-Buckets

Beschreibung

Sie haben einen verschlüsselten Amazon S3 S3-Bucket, den Sie als Speicher für Ihren Transfer Family Family-Server verwenden. Wenn Sie versuchen, eine Datei auf den Server hochzuladen, erhalten Sie die Fehlermeldung `Couldn't close file: Permission denied`.

Und wenn Sie sich die Serverprotokolle ansehen, werden Ihnen die folgenden Fehler angezeigt:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

Ursache

Die Richtlinie für Ihren IAM-Benutzer ist nicht berechtigt, auf den verschlüsselten Bucket zuzugreifen.

Lösung

Sie müssen in Ihrer Richtlinie zusätzliche Berechtigungen angeben, um die erforderlichen AWS Key Management Service (AWS KMS) Berechtigungen zu gewähren. Details hierzu finden Sie unter [Datenschutz und Verschlüsselung](#).

Beheben Sie die **ResourceNotFound** Ausnahme

Beschreibung

Sie erhalten eine Fehlermeldung, dass die Ressource nicht gefunden werden kann. Wenn Sie beispielsweise ausführen `UpdateServer`, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:
Unknown server
```

Ursache

Es gibt mehrere Gründe für den Empfang einer `ResourceNotFoundException` Nachricht. In den meisten Fällen ist die Ressource, die Sie in Ihrem API-Befehl angegeben haben, nicht vorhanden. Wenn Sie eine vorhandene Ressource angegeben haben, ist die wahrscheinlichste Ursache, dass sich Ihre Standardregion von der Region für Ihre Ressource unterscheidet. Wenn Ihre Standardregion

beispielsweise us-east-1 ist und sich Ihr Transfer Family Family-Server in us-east-2 befindet, erhalten Sie eine Unbekannte Ressourcenausnahme.

[Einzelheiten zum Festlegen einer Standardregion finden Sie unter Schnellkonfiguration mit. `aws configure`](#)

Lösung

Fügen Sie Ihrem API-Befehl einen Regionsparameter hinzu, um explizit anzugeben, wo sich eine bestimmte Ressource befindet.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Behebung von Überwachungs- und Warnproblemen

Dieser Abschnitt enthält Informationen zur Behebung von Überwachungs- und Warnproblemen AWS Transfer Family, einschließlich fehlender oder unvollständiger CloudWatch Metriken und fehlender EventBridge Ereignisse.

Themen

- [Beheben Sie Fehler bei fehlenden oder unvollständigen Metriken CloudWatch](#)
- [Beheben Sie fehlende EventBridge Ereignisse](#)

Beheben Sie Fehler bei fehlenden oder unvollständigen Metriken CloudWatch

Beschreibung

CloudWatch Die Messwerte für Ihre Transfer Family Family-Server fehlen, sind unvollständig oder werden nicht wie erwartet aktualisiert.

Ursache

Fehlende oder unvollständige Messwerte können verschiedene Ursachen haben:

- Protokollierung von Konfigurationsproblemen
- Niedriges Aktivitätsniveau, das keine Messwerte innerhalb des erwarteten Zeitrahmens generiert
- Anzeige von Metriken mit falschen Dimensionen oder Zeiträumen

Lösung

So lösen Sie Probleme mit fehlenden oder unvollständigen CloudWatch Metriken:

1. Stellen Sie sicher, dass die Protokollierung für Ihren Transfer Familyserver richtig konfiguriert ist:
 - Vergewissern Sie sich in der Transfer Family Family-Konsole, dass die Protokollierung unter Serverdetails > Zusätzliche Details > Logging-Rolle aktiviert ist.
 - Achten Sie darauf, dass die Logging-Rolle über die erforderlichen Berechtigungen und Vertrauensbeziehungen verfügt.
2. Gehen Sie beim Anzeigen von Metriken in der CloudWatch Konsole wie folgt vor:
 - Verwenden Sie die richtigen Dimensionen, z. B. ServerId für Metriken auf Serverebene
 - Passen Sie den Zeitraum an, um sicherzustellen, dass er Aktivitätsperioden abdeckt
 - Vergewissere dich, dass du im richtigen Bereich bist AWS-Region
3. Generieren Sie Testaktivitäten auf Ihrem Transfer Family Family-Server, um sicherzustellen, dass Metriken erstellt werden.

Beheben Sie fehlende EventBridge Ereignisse

Beschreibung

Sie haben EventBridge Amazon-Regeln so konfiguriert, dass sie Transfer Family Family-Ereignisse erfassen, aber Ereignisse werden nicht an Ihre Zielorte gesendet oder lösen keine erwarteten Aktionen aus.

Ursache

Fehlende EventBridge Ereignisse können folgende Ursachen haben:

- Falsch konfigurierte Ereignismuster
- Probleme mit Berechtigungen bei Ereigniszielen
- Dienstbeschränkungen oder Drosselung
- Ereignisse werden aufgrund der Serverkonfiguration nicht generiert

Lösung

So beheben Sie fehlende EventBridge Ereignisse:

1. Stellen Sie sicher, dass Ihr Event-Muster korrekt formatiert ist, um den Ereignissen von Transfer Family zu entsprechen:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. Vergewissere dich, dass dein Eventziel über die erforderlichen Berechtigungen verfügt:
 - Stellen Sie für Lambda-Ziele sicher, dass die Ressourcenrichtlinie der Lambda-Funktion EventBridge den Aufruf zulässt
 - Stellen Sie bei SQS-Zielen sicher, dass die Warteschlangenrichtlinie das Senden von Nachrichten zulässt EventBridge
 - Vergewissern Sie sich bei SNS-Zielen, dass die Themenrichtlinie das Veröffentlichen EventBridge auf diesen Zielen zulässt
3. Testen Sie Ihre Regel, indem Sie Beispielergebnisse generieren:
 - Verwenden Sie die EventBridge Konsole, um ein Testereignis zu erstellen, das Ihrem Muster entspricht
 - Führen Sie Aktionen auf Ihrem Transfer Family Family-Server aus, die Ereignisse generieren sollen
4. Aktivieren Sie EventBridge Regelmetriken, um Regelaufrufe und -fehler zu überwachen:

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. Suchen Sie in den CloudWatch Protokollen nach Fehlermeldungen im Zusammenhang mit Fehlern bei der Zustellung von Ereignissen

Behebung von Problemen bei der Übertragung zwischen Regionen

In diesem Abschnitt werden mögliche Lösungen für Probleme im Zusammenhang mit der Übertragung von Dateien beschrieben AWS-Regionen.

Themen

- [Beheben Sie Probleme mit regionsübergreifenden Übertragungsberechtigungen](#)
- [Beheben Sie Leistungsprobleme bei regionsübergreifenden Übertragungen](#)

Beheben Sie Probleme mit regionsübergreifenden Übertragungsberechtigungen

Beschreibung

Wenn Sie versuchen, Dateien mithilfe von Transfer Family-Workflows zwischen Amazon S3 S3-Buckets in verschiedenen Regionen zu übertragen, treten Fehler auf wie:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

Ursache

Cross-region Übertragungen erfordern spezielle IAM-Berechtigungen sowohl für den Quell- als auch für den Ziel-Bucket. Die von Ihrem Transfer Family Family-Server oder -Workflow verwendete IAM-Rolle verfügt möglicherweise nicht über ausreichende Berechtigungen, um auf Buckets in anderen Regionen zuzugreifen.

Lösung

So lösen Sie Probleme mit regionsübergreifenden Übertragungsberechtigungen:

1. Stellen Sie sicher, dass Ihre IAM-Rolle über Berechtigungen sowohl für Quell- als auch für Ziel-Buckets verfügt:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::source-bucket-name/*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource": "arn:aws:s3:::destination-bucket-name/*"
}
]
}

```

2. Wenn Sie die KMS-Verschlüsselung verwenden, fügen Sie Berechtigungen sowohl für den Quell- als auch für den Ziel-KMS-Schlüssel hinzu:

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}

```

3. Stellen Sie sicher, dass die Bucket-Richtlinien in beiden Regionen den Zugriff von der IAM-Rolle Ihres Transfer Family Family-Servers aus zulassen
4. Stellen Sie bei kontoübergreifenden Übertragungen sicher, dass die richtigen kontoübergreifenden Berechtigungen konfiguriert sind

Beheben Sie Leistungsprobleme bei regionsübergreifenden Übertragungen

Beschreibung

Cross-region Übertragungen sind deutlich langsamer als erwartet oder es kommt zu Zeitüberschreitungen bei Übertragungen großer Dateien.

Ursache

Cross-region Übertragungen sind naturgemäß mit einer höheren Latenz verbunden und können durch Netzwerkbedingungen, Dateigrößen und Dienstbeschränkungen beeinflusst werden. Bei großen Dateien oder großen Mengen kleiner Dateien kann es zu Leistungseinbußen kommen.

Lösung

So verbessern Sie die Übertragungsleistung zwischen Regionen:

- Für große Dateien sollten Sie die Verwendung von Amazon S3 Transfer Acceleration in Betracht ziehen:

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Bei mehreren kleinen Dateien sollten Sie diese vor der Übertragung in einem Batch zusammenfügen:
 - Verwenden Sie die Komprimierung, um mehrere Dateien zu kombinieren
 - Verwenden Sie Amazon S3 S3-Batch-Operationen für umfangreiche Übertragungen
- Erwägen Sie die Verwendung von SFTP-Konnektoren der Transfer Family mit entsprechenden Timeout-Einstellungen für große Übertragungen
- Bei wiederkehrenden Übertragungen sollten Sie erwägen, Daten mithilfe von Amazon S3 Cross-Region Replication (CRR) anstelle von Ad-hoc-Übertragungen zu replizieren
- Überwachen Sie die Übertragungsleistung mithilfe von CloudWatch Amazon-Metriken, um Engpässe zu identifizieren

Behebung von Problemen bei der Terraform-Bereitstellung

In diesem Abschnitt werden mögliche Lösungen für Probleme im Zusammenhang mit der Bereitstellung von Transfer Family Family-Ressourcen mithilfe von Terraform beschrieben.

Allgemeine Informationen zu Terraform-Modulen für Transfer Family finden Sie unter [Terraform-Module der Transfer Family](#)

Themen

- [Beheben Sie Fehler bei der Erstellung von Terraform-Ressourcen](#)
- [Beheben Sie Probleme mit der Terraform-Statusverwaltung](#)

Beheben Sie Fehler bei der Erstellung von Terraform-Ressourcen

Beschreibung

Beim Versuch, Transfer Family Family-Ressourcen mit Terraform zu erstellen, treten Fehler auf wie:

```
Error: error creating Transfer Server: InvalidRequestException: The request is not valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user because the server endpoint type is incompatible with the home directory type.
```

Ursache

Diese Fehler treten normalerweise aufgrund inkompatibler Konfigurationsparameter oder fehlender Abhängigkeiten in Ihrer Terraform-Konfiguration auf. Zu den häufigsten Ursachen gehören:

- Inkompatible Endpunkttypen und Speicherkonfigurationen
- Fehlende erforderliche IAM-Rollen oder -Richtlinien
- Falsche Spezifikationen für Sicherheitsrichtlinien
- Probleme mit der Konfiguration von VPC-Endpunkten

Lösung

So lösen Sie Probleme mit der Terraform-Bereitstellung:

- Stellen Sie sicher, dass Ihre Terraform-Konfiguration kompatible Parameterkombinationen verwendet:
 - Stellen Sie bei öffentlichen Endpunkten sicher, dass Sie Amazon S3 als Speicher verwenden.
 - Überprüfen Sie für VPC-Endpoints die richtige VPC- und Sicherheitsgruppenkonfiguration.
- Verwenden Sie explizite Abhängigkeiten mit dem `depends_on` Attribut, um sicherzustellen, dass Ressourcen in der richtigen Reihenfolge erstellt werden.
- Stellen Sie sicher, dass alle IAM-Rollen über die erforderlichen Vertrauensbeziehungen und Berechtigungen verfügen.

- Verwenden Sie die neueste Version des AWS Anbieters für Terraform, um die Kompatibilität mit allen Funktionen der Transfer Family sicherzustellen.
- Für komplexe Bereitstellungen und einfache Anwendungsfälle sollten Sie die Verwendung der offiziellen Terraform-Module der Transfer Family in Betracht ziehen, die unter verfügbar sind. GitHub <https://github.com/aws-ia/terraform-aws-transfer-family> Diese Module bieten umfangreiche Beispiele für einfache und komplexe Kundenanwendungsfälle, folgen AWS bewährten Methoden und können die Bereitstellung für Kunden vereinfachen, die Hilfe bei der Konfiguration von Infrastructure as Code (IaC) benötigen.

Beheben Sie Probleme mit der Terraform-Statusverwaltung

Beschreibung

Nachdem Sie außerhalb von Terraform (über die Konsole oder AWS CLI) Änderungen an Ihren Transfer Family Family-Ressourcen vorgenommen haben, treten beim Ausführen `terraform plan` von oder Statusabweichungen oder Fehler auf. `terraform apply`

Ursache

Terraform verwaltet eine Statusdatei, in der die von Terraform verwalteten Ressourcen nachverfolgt werden. Wenn Änderungen außerhalb von Terraform vorgenommen werden, ist die Statusdatei nicht mehr mit den tatsächlichen Ressourcen synchron, was zu Fehlern oder unerwartetem Verhalten bei nachfolgenden Terraform-Vorgängen führt.

Lösung

So lösen Sie Probleme mit der Terraform-Statusverwaltung mit Ressourcen von Transfer Family:

1. Wird verwendet `terraform import`, um vorhandene Ressourcen unter die Terraform-Verwaltung zu bringen:

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. Wird verwendet `terraform refresh`, um die Statusdatei mit der aktuellen realen Infrastruktur zu aktualisieren
3. Bei Ressourcen, die nicht importiert werden können oder komplexe Statusprobleme aufweisen, sollten Sie erwägen, sie aus der Statusdatei `terraform state rm` zu entfernen und sie dann mit Terraform neu zu erstellen

4. Implementieren Sie eine Richtlinie zur ausschließlichen Verwaltung der Ressourcen von Transfer Family über Terraform, um zukünftige Zustandsverschiebungen zu verhindern
5. Verwenden Sie Remote-State-Speicher mit Sperre, um gleichzeitige Änderungen bei der Arbeit in Teams zu verhindern

Behebung von Integrationsproblemen mit der Web Application Firewall

In diesem Abschnitt werden mögliche Lösungen für Probleme im Zusammenhang mit der Integration AWS WAF mit Transfer Family beschrieben.

Themen

- [Beheben Sie Fehler beim Blockieren von legitimem Datenverkehr durch WAF](#)
- [Beheben Sie Probleme bei der WAF-Integration mit benutzerdefinierten Identitätsanbietern](#)

Beheben Sie Fehler beim Blockieren von legitimem Datenverkehr durch WAF

Beschreibung

Nach der Konfiguration AWS WAF mit Ihrem Transfer Family Family-Endpunkt können legitime Benutzer keine Verbindung herstellen oder es kommt zu zeitweiligen Verbindungsausfällen. Möglicherweise werden in Ihren Protokollen Antworten vom Typ HTTP 403 (Verboten) angezeigt.

Ursache

Ihre AWS WAF Regeln sind möglicherweise zu restriktiv oder falsch konfiguriert, was zu Fehlalarmen führt, die legitimen Datenverkehr blockieren. Zu den häufigsten Ursachen gehören:

- IP-based Regeln, die versehentlich Unternehmensnetzwerke oder VPNs blockieren
- Rate-based Regeln mit Schwellenwerten, die für Ihre normalen Verkehrsmuster zu niedrig sind
- Verwaltete Regelgruppen, die für Ihren Anwendungsfall zu aggressiv sind

Lösung

So beheben Sie Probleme mit falsch positiven Ergebnissen:

1. Aktivieren AWS WAF Sie die Protokollierung, um festzustellen, welche Regeln die Blöcke auslösen. Anweisungen finden Sie unter [AWS WAF Web-ACL-Verkehr protokollieren](#).
2. Überprüfen Sie Ihre Protokolle, um Muster in den blockierten Anfragen zu identifizieren.
3. Passen Sie Ihre Regeln an, indem Sie:
 - Hinzufügen von IP-Adressen oder Bereichen zu einer Zulassungsliste
 - Erhöhung der Ratenlimits für ratenbasierte Regeln
 - Einstellung bestimmter Regeln auf den Zählmodus statt auf den Blockmodus, um sie zu überwachen, ohne zu blockieren
 - Erstellen von Ausnahmen für bestimmte Regeln mithilfe von Regelgruppenausschlüssen
4. Testen Sie die aktualisierte Konfiguration mit einer repräsentativen Stichprobe legitimen Datenverkehrs, bevor Sie sie vollständig bereitstellen.

Beheben Sie Probleme bei der WAF-Integration mit benutzerdefinierten Identitätsanbietern

Beschreibung

Nach der Konfiguration AWS WAF mit Ihrem Transfer Family Family-Server, der einen benutzerdefinierten Identitätsanbieter verwendet, schlägt die Authentifizierung fehl oder es treten bei Benutzern zeitweise Authentifizierungsprobleme auf.

Ursache

Wenn Sie einen benutzerdefinierten Identitätsanbieter mit API Gateway verwenden, können AWS WAF Regeln die API-Aufrufe zwischen Transfer Family und Ihrem Identitätsanbieter stören. Dies kann passieren, weil AWS WAF der API-Verkehr anhand seiner Regelsätze überprüft und möglicherweise blockiert wird.

Lösung

So lösen Sie Probleme mit AWS WAF und benutzerdefinierten Identitätsanbietern:

- Stellen Sie sicher, dass Ihre AWS WAF Konfiguration Ausnahmen für die API Gateway Gateway-Endpunkte enthält, die von Ihrem benutzerdefinierten Identitätsanbieter verwendet werden.
- Fügen Sie den Service Principal von Transfer Family (transfer.amazonaws.com) zu einer Zulassungsliste in Ihren Regeln hinzu. AWS WAF

- Wenn Sie verwaltete Regelgruppen verwenden, überprüfen Sie diese auf Regeln, die sich auf API-Authentifizierungsabläufe auswirken könnten, und erwägen Sie, diese spezifischen Regeln zu deaktivieren.
- Testen Sie Ihren Identitätsanbieter direkt mithilfe des `TestIdentityProvider` API-Vorgangs, um sicherzustellen, dass er ordnungsgemäß und ohne AWS WAF Störungen funktioniert.

Behebung von Problemen mit serviceverwalteten Benutzern

In diesem Abschnitt werden mögliche Lösungen für Probleme mit dienstverwalteten Benutzern beschrieben.

Themen

- [Beheben Sie Probleme mit Benutzern, die vom Service](#)

Beheben Sie Probleme mit Benutzern, die vom Service

In diesem Abschnitt werden mögliche Lösungen für die folgenden Probleme beschrieben.

Themen

- [Die Problembehandlung für den öffentlichen Schlüsseltext dauert zu lange](#)
- [Bei der Fehlerbehebung konnte der öffentliche SSH-Schlüssel nicht hinzugefügt werden](#)

Die Problembehandlung für den öffentlichen Schlüsseltext dauert zu lange

Beschreibung

Wenn Sie versuchen, einen vom Dienst verwalteten Benutzer zu erstellen, wird die folgende Fehlermeldung angezeigt:

```
Failed to create user (1 validation error detected:  
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or  
equal to 2048)
```

Ursache

Möglicherweise geben Sie einen PGP-Schlüssel für den öffentlichen Schlüssel ein. PGP-Schlüssel für vom Dienst verwaltete Benutzer werden AWS Transfer Family nicht unterstützt.

Lösung

Wenn der PGP-Schlüssel vorhanden ist RSA-based, können Sie ihn in das PEM-Format konvertieren. Zum Beispiel bietet Ubuntu hier ein Konvertierungstool: <https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

Bei der Fehlerbehebung konnte der öffentliche SSH-Schlüssel nicht hinzugefügt werden

Beschreibung

Wenn Sie versuchen, einen öffentlichen Schlüssel für einen vom Service verwalteten Benutzer hinzuzufügen, wird die folgende Fehlermeldung angezeigt:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Ursache

Möglicherweise versuchen Sie, einen SSH2-formatted öffentlichen Schlüssel zu importieren. SSH2-formatted Öffentliche Schlüssel für vom Dienst verwaltete Benutzer werden AWS Transfer Family nicht unterstützt.

Lösung

Sie müssen den Schlüssel in das OpenSSH-Format konvertieren. Dieser Vorgang wird unter beschrieben. [Konvertierung eines SSH2-Schlüssels in das Format eines öffentlichen SSH-Schlüssels](#)

AS2-Probleme beheben

In diesem Abschnitt werden mögliche Lösungen für Probleme mit AS2-Übertragungen beschrieben.

Themen

- [Beheben Sie AS2-Probleme](#)
- [Probleme mit dem AS2-Zertifikat](#)
- [Probleme mit dem AS2 MDN-Empfang](#)
- [Probleme bei der Überwachung des Ablaufs von Zertifik](#)

Beheben Sie AS2-Probleme

[AS2-Fehlercodes](#), Meldungen und Tipps zur Fehlerbehebung für Applicability Statement 2 (AS2) - fähige Server werden im Abschnitt AS2-Fehlercodes in diesem Handbuch beschrieben.

Probleme mit dem AS2-Zertifikat

Beschreibung

Bei AS2-Übertragungen treten zertifikatsbezogene Fehler auf.

Ursache

Zu den häufigsten Ursachen gehören abgelaufene Zertifikate, falsche Zertifikatsformate oder nicht übereinstimmende Zertifikatsketten.

Lösung

Probieren Sie die folgenden Lösungen aus:

- Stellen Sie sicher, dass Ihre Zertifikate nicht abgelaufen sind
- Stellen Sie sicher, dass die Zertifikate das richtige Format haben (PEM für AWS Transfer Family)
- Stellen Sie sicher, dass die Zertifikatskette vollständig und gültig ist
- Vergewissern Sie sich, dass die Signatur- und Verschlüsselungszertifikate der Handelspartner übereinstimmen
- Wechseln Sie die Zertifikate lange vor Ablauf, um Unterbrechungen zu vermeiden

Probleme mit dem AS2 MDN-Empfang

Beschreibung

Sie erhalten keine erwarteten Message Disposition Notifications (MDNs) für AS2-Übertragungen.

Ursache

MDN-Probleme können aufgrund von Netzwerkverbindungsproblemen, falschen Endpunktconfigurationen oder nicht übereinstimmenden MDN-Formaten auftreten.

Lösung

Ziehen Sie diese Lösungen in Betracht:

- Stellen Sie sicher, dass die MDN-URL korrekt konfiguriert und zugänglich ist
- Überprüfen Sie die Netzwerkkonnektivität zwischen dem AS2-Server und dem MDN-Endpunkt
- Stellen Sie sicher, dass beide Handelspartner für denselben MDN-Typ (synchron oder asynchron) konfiguriert sind
- Überprüfen Sie die AS2-Protokolle auf Fehler im Zusammenhang mit der MDN-Verarbeitung
- Wenn Sie synchrones mDNS verwenden, stellen Sie sicher, dass die Timeouts ordnungsgemäß festgelegt sind

Probleme bei der Überwachung des Ablaufs von Zertifik

In diesem Abschnitt finden Sie Lösungen für häufig auftretende Probleme im Zusammenhang mit der Überwachung des Ablaufs von Zertifikaten und der DaysUntilExpiry Metrik.

DaysUntilExpiry Die Metrik wird nicht angezeigt

Problem: Die DaysUntilExpiry Metrik ist CloudWatch nach dem Import eines Zertifikats in Amazon nicht sichtbar.

Lösung:

- Warten Sie nach dem Import des Zertifikats bis zu 24 Stunden. Es kann bis zu einem ganzen Tag dauern, bis Transfer Family die Metrik auf Ihr Konto übermittelt.
- Stellen Sie sicher, dass Sie in der richtigen AWS Region und unter dem AWS/Transfer Namespace in CloudWatch suchen.

Alarmer zum Ablauf des Zertifikats werden nicht ausgelöst

Problem: CloudWatch Alarmer für den Ablauf von Zertifikaten werden nicht wie erwartet ausgelöst.

Lösung:

- Stellen Sie sicher, dass der Alarm mit der Maximum Statistik und einem Zeitraum von 1 Tag konfiguriert ist.
- Vergewissern Sie sich, dass der Schwellenwertvergleich auf `Less than or equal to` die gewünschte Anzahl von Tagen eingestellt ist.

- Stellen Sie sicher, `Treat missing data as good (not breaching)` dass dies in der Alarmkonfiguration ausgewählt ist.
- Stellen Sie sicher, dass die Abmessungen des Alarms mit denen Ihres Zertifikats `CertificateId` und der Beschreibung (falls angegeben) übereinstimmen.
- Vergewissern Sie sich, dass die Alarmaktionen (SNS-Themen, E-Mail-Benachrichtigungen) ordnungsgemäß konfiguriert und aktiv sind.

AWS Transfer Family API-Referenz

Das vollständige API-Referenzhandbuch für Transfer Family ist unter [AWS Transfer Family API Reference](#) verfügbar.

AWS Transfer Family ist ein sicherer Übertragungsservice, mit dem Sie Dateien über die folgenden Protokolle in den und aus dem Amazon Simple Storage Service (Amazon S3) -Speicher übertragen können:

- Secure Shell (SSH) File Transfer Protocol (SFTP)
- Sicheres Dateiübertragungsprotokoll (FTPS)
- Dateiübertragungsprotokoll (FTP)
- Erklärung zur Anwendbarkeit 2 (AS2)

Server, Benutzer und Rollen werden alle anhand ihres Amazon-Ressourcennamens (ARN) identifiziert. Sie können Entitäten mit einem ARN Tags zuweisen, bei denen es sich um Schlüssel-Wert-Paare handelt. Tags sind Metadaten, die verwendet werden können, um diese Entitäten zu gruppieren oder nach ihnen zu suchen. Tags sind beispielsweise für die Buchhaltung nützlich.

Die folgenden Konventionen werden bei AWS Transfer Family ID-Formaten eingehalten:

- ServerId-Werte haben das Format `s-01234567890abcdef`.
- SshPublicKeyId-Werte haben das Format `key-01234567890abcdef`.

Die Formate von Amazon Resource Name (ARN) haben die folgende Form:

- Für Server haben ARNs die folgende Form: `arn:aws:transfer:region:account-id:server/server-id`.

Ein Beispiel für einen Server-ARN lautet `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- Für Benutzer haben ARNs das Format `arn:aws:transfer:region:account-id:user/server-id/username`.

Ein Beispiel ist `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Folgende DNS-Einträge (Endpunkte) werden verwendet:

- API-Endpunkte haben das Format `transfer.region.amazonaws.com`.
- Server-Endpunkte haben das Format `server.transfer.region.amazonaws.com`.

Diese API-Schnittstellenreferenz für AWS Transfer Family enthält Dokumentation für eine Programmierschnittstelle, die Sie zur Verwaltung AWS Transfer Family verwenden können. Die Referenzstruktur:

- Eine alphabetische Liste der API-Aktionen finden Sie unter [Actions](#).
- Eine alphabetische Liste der Datentypen finden Sie unter [Types](#).
- Eine Liste der häufigen Abfrageparameter finden Sie unter [Häufige Parameter](#).
- Beschreibungen der Fehlercodes finden Sie unter [Häufige Fehler](#).

 Tip

Anstatt einen Befehl tatsächlich auszuführen, können Sie den `--generate-cli-skeleton` Parameter mit jedem API-Aufruf verwenden, um eine Parametervorlage zu generieren und anzuzeigen. Anschließend können Sie die generierte Vorlage anpassen und als Eingabe für einen späteren Befehl verwenden. Einzelheiten finden Sie unter [Generieren und Verwenden einer Parameter-Skelettdatei](#).

Dokumenthistorie für AWS Transfer Family

In der folgenden Tabelle wird die Dokumentation für diese Version von beschrieben AWS Transfer Family.

- API-Version: transfer-2018-11-05
- Letzte Aktualisierung der Dokumentation: 19. November 2025

Änderungen	Beschreibung	Date
VPC-Endpunktunterstützung für Transfer Family Family-Web-Apps	AWS Transfer Family Web-Apps unterstützen jetzt VPC-gehostete Endpunkte, sodass Sie Ihren Web-App-Endpunkt in einer virtuellen privaten Cloud für private Datenübertragungen zu und von Amazon S3 hosten können, ohne das öffentliche Internet zu durchqueren. Details hierzu finden Sie unter Eine Transfer Family Family-Web-App in einer VPC erstellen .	19. November 2025
IPv6-Support	AWS Transfer Family unterstützt jetzt Dual-Stack-Endpunkte (IPv4 und IPv6) für öffentliche SFTP-Endpunkte, Endpunkte für, SFTP- und AS2-Konnektoren sowie VPC-internal SFTP/FTPS/FTP/AS2 API-Endpunkte. Details hierzu finden Sie unter IPv6-Unterstützung für Transfer Family Family-Server .	30. Juni 2025

Änderungen	Beschreibung	Date
Verbesserungen der Benutzererfahrung mit SFTP-Konnektoren	• Möglichkeit, die Einstellungen für gleichzeitige Verbindungen für Ihre Konnektoren selbst zu verwalten • Möglichkeit, einen privaten SSH-Schlüssel im OpenSSH-Format bereitzustellen, der für die Authentifizierung von Verbindungen verwendet wird • Möglichkeit, den öffentlichen Hostschlüssel von Remoteservern mithilfe ihrer SFTP-Konnektoren zu ermitteln Details hierzu finden Sie unter Erstellen Sie einen SFTP-Connector mit serviceverwaltungstem Ausgang.	9. April 2025

Änderungen	Beschreibung	Date
Möglichkeit für SFTP-Konnektoren, Dateien auf dem Remote-SFTP-Server zu löschen, umzubenennen und zu verschieben	Sie können jetzt Ihre auf Remote-SFTP-Servern gespeicherten Dateien organisieren, indem Sie Quelldateien löschen, umbenennen oder in Archivverzeichnisse verschieben, nachdem sie vom Remote-Server kopiert wurden. Details hierzu finden Sie unter Dateien oder Verzeichnisse auf dem Remote-SFTP-Server verschieben oder umbenennen.	7. April 2025
Support für AWS Transfer Family Web-Apps	AWS Transfer Family Web-Apps sind eine neue Ressource, mit der Kunden eine einfache Oberfläche für den Zugriff auf ihre Daten in Amazon S3 über einen Webbrowser erstellen können. Details hierzu finden Sie unter Familien-Web-Apps übertragen.	01. Dezember 2024
Die API-Referenz wurde in ein separates Handbuch verschoben	Um das Kundenerlebnis zu verbessern, wird die API-Referenz jetzt separat vom Benutzerhandbuch veröffentlicht. Die separate API-Referenz finden Sie unter Willkommen bei der AWS Transfer Family API.	31. Juli 2024

Änderungen	Beschreibung	Date
Möglichkeit für SFTP-Konnektoren, entfernte Dateien und Verzeichnisse aufzulisten	Transfer Family bietet unseren Kunden die Möglichkeit, SFTP-Konnektoren zu verwenden, um Dateien aufzulisten, die auf Remote-SFTP-Servern gespeichert sind. Details hierzu finden Sie unter Inhalt eines Remote-Verzeichnisses auflisten	23. April 2024
Möglichkeit, das selbstsignierte TLS-Zertifikat eines Handelspartners für den AS2-Nachrichtenaustausch zu verwenden	AWS Transfer Family hat die Option hinzugefügt, das öffentliche, selbstsignierte TLS-Zertifikat eines Handelspartners zu importieren und zu verwenden, um Applicability Statement 2-Nachrichten (AS2) über HTTPS an seinen Server zu senden.	12. April 2024
Hinzufügung von Sicherheitsrichtlinien für SFTP-Konnektoren	AWS Transfer Family hat Sicherheitsrichtlinien für die Verwendung mit SFTP-Konnektoren hinzugefügt. Details hierzu finden Sie unter Sicherheitsrichtlinien für SFTP-Konnektoren AWS Transfer Family .	5. April 2024

Änderungen	Beschreibung	Date
Integrieren Sie mit Amazon EventBridge	AWS Transfer Family veröffentlicht jetzt automatisch Ereignisse EventBridge für alle Dateiübertragungsvorgänge auf Amazon. Details hierzu finden Sie unter Transfer Family Ereignisse verwalten mit Amazon EventBridge .	8. Februar 2024
Hinzufügung neuer Sicherheitsrichtlinien	AWS Transfer Family hat neue FIPS- und Nicht-FIPS-Sicherheitsrichtlinien hinzugefügt. Außerdem ist die Standardsicherheitsrichtlinie, die Servern zugewiesen ist, immer die neueste Sicherheitsrichtlinie. Details hierzu finden Sie unter Sicherheitsrichtlinien für Server AWS Transfer Family .	5. Februar 2024
Support für statische IP-Adressen für SFTP-Anschlüsse und AS2	Transfer Family bietet jetzt statische IP-Adressen für SFTP-Anschlüsse und AS2. Dies ermöglicht die Verbindung mit Remote-SFTP-Servern, die durch IP-Allowlisting-Kontrollen gesichert sind. Für AS2 führen wir statische IP-Adressen für asynchrone MDN-Antworten von AS2-Servern ein.	16. Januar 2024

Änderungen	Beschreibung	Date
Das Benutzerhandbuch wurde neu organisiert, um es besser an die neueste Version von anzupassen. AWS Transfer Family	Transfer Family hat seit der Entstehung des Leitfadens mehrere Funktionen hinzugefügt, was eine Umstrukturierung des Leitfadens erforderlich machte.	3. Januar 2024
Verbesserungen bei den logischen Verzeichniszuordnungen Leistungsoptimierung der Amazon S3 S3-Liste	Transfer Family unterstützt jetzt logische Verzeichniszuordnungen bis zu 2,1 MB. Sie können jetzt auch angeben, ob eine Benutzerzuordnung zu einer Datei erfolgt. Weitere Informationen finden Sie unter Regeln für die Verwendung logischer Verzeichnisse. Wenn Sie einen Server erstellen oder aktualisieren, der Amazon S3 als Speicher verwendet, können Sie jetzt die Leistung beim Auflisten Ihrer S3-Verzeichnisse (oder Ordner) optimieren. Weitere Informationen finden Sie unter Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts.	17. November 2023

Änderungen	Beschreibung	Date
Alternativer Port für SFTP-Server mit Virtual Private Cloud (VPC) -Endpunkten	Sie können jetzt einen alternativen, nicht standardmäßigen Port für Ihre SFTP Transfer Family Family-Server mit VPC-Endpunkten aktivieren. Weitere Informationen finden Sie unter Erstellen Sie einen Server in einer virtuellen privaten Cloud .	17. November 2023
Support für SFTP-Anschlüsse	SFTP-Konnektoren erweitern die Möglichkeiten AWS Transfer Family zur Kommunikation mit Remoteservern sowohl in der Cloud als auch vor Ort. Weitere Informationen finden Sie unter Verwenden von SFTP-Anschlüssen .	25. Juli 2023
Support für AS2 Basic-Authentifizierung	Transfer Family unterstützt jetzt die Verwendung der Standardauthentifizierung für Server, die das Applicability Statement 2 (AS2)-Protokoll verwenden. Weitere Informationen finden Sie unter Standardauthentifizierung für AS2-Konnektoren .	30. Juni 2023

Änderungen	Beschreibung	Date
Support für strukturiertes JSON-Logging	Transfer Family unterstützt jetzt die Bereitstellung strukturierter JSON-Protokolle an Amazon CloudWatch, die Gruppierung von Protokollströmen in benutzerdefinierte Protokollgruppen und die Ausführung gängiger Protokollabfragen über Protokolle hinweg. Weitere Informationen finden Sie unter CloudWatch Amazon-Protokollierung für AWS Transfer Family Server .	24. Juni 2023
Support für mehrere Authentifizierungsmethoden	Transfer Family unterstützt die Authentifizierung mit einem Passwort, einem public/private key pair oder beidem. Dies ist für Server verfügbar, die das SFTP-Protokoll und einen benutzerdefinierten Identitätsanbieter verwenden. Weitere Informationen finden Sie unter Erstellen Sie einen SFTP-enabled Server .	17. Mai 2023

Änderungen	Beschreibung	Date
Support für die Pretty Good Privacy (PGP) -Entschlüsselung mit Dateien, die Transfer Family mit Workflows verarbeitet	Transfer Family bietet integrierte Unterstützung für die Pretty Good Privacy (PGP) -Entschlüsselung. Sie können die PGP-Entschlüsselung für Dateien verwenden, die über SFTP, FTPS oder FTP auf Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) hochgeladen werden. Weitere Informationen erhalten Sie unter Generieren Sie PGP-Schlüssel und Verwenden Sie die PGP-Entschlüsselung in Ihrem Workflow .	21. Dezember 2022
Vollständig verwaltete Unterstützung für das AS2-Dateiübertragungsprotokoll Applicability Statement 2 (Applicability Statement 2) mit Transfer Family Family-Servern	Sie können Server einrichten, die das AS2-Protokoll zum Senden und Empfangen von Informationen an und von Handelspartnern innerhalb oder außerhalb der Umgebung verwenden. AWS Weitere Informationen finden Sie unter AS2 konfigurieren .	25. Juli 2022

Änderungen	Beschreibung	Date
Support für Display-Banner beim Erstellen eines Servers	Sie können benutzerdefinierte Nachrichten hinzufügen, wenn Sie Server erstellen. Sie können eine Nachricht vor der Authentifizierung (alle Protokolle) und eine Nachricht nach der Authentifizierung (für FTP- und FTPS-Server) anzeigen. Weitere Informationen finden Sie unter, Erstellen Sie einen SFTP-enabled Server , Einen FTPS-enabled Server erstellen oder Erstellen Sie einen FTP-enabled Server .	17. Februar 2022
Support für AWS Lambda als Identitätsanbieter	Sie können jetzt eine Verbindung zu einem benutzerdefinierten Identitätsanbieter herstellen, indem Sie AWS Lambda dessen Transfer Family Family-Server verwenden. Bisher mussten Sie eine Amazon API Gateway URL angeben, um einen benutzerdefinierten Identitätsanbieter zu integrieren. Weitere Informationen finden Sie unter Wird AWS Lambda zur Integration Ihres Identitätsanbieters verwendet .	16. November 2021

Änderungen	Beschreibung	Date
Support für Workflows zur verwalteten Dateiübertragung	Workflows für verwaltete Dateiübertragungen bieten Ihnen nach dem Upload Abstraktionen für die allgemeinen Aufgaben, die Sie derzeit manuell ausführen. Weitere Informationen finden Sie unter AWS Transfer Family verwaltete Workflows .	2. September 2021
Support für AWS Directory Service for Microsoft Active Directory	Zusätzlich zu dienstverwalteten und benutzerdefinierten Identitätsanbietern können Sie jetzt auch AWS Directory Service for Microsoft Active Directory den Benutzerzugriff für die Authentifizierung und Autorisierung verwalten. Weitere Informationen finden Sie unter Verwenden des AWS Directory Service für Microsoft Active Directory .	24. Mai 2021
Neu AWS-Regionen	AWS Transfer Family ist jetzt in der Region Afrika (Kapstadt) verfügbar. Weitere Informationen zu Transfer Family Family-Endpunkten finden Sie unter AWS Transfer Family Endpunkte und Kontingente in der. Allgemeine AWS-Referenz	24. Februar 2021

Änderungen	Beschreibung	Date
Neu AWS-Regionen	AWS Transfer Family ist jetzt in den Regionen Asien-Pazifik (Hongkong) und Naher Osten (Bahrain) verfügbar. Weitere Informationen zu Transfer Family Family-Endpunkten finden Sie unter AWS Transfer Family Endpunkte und Kontingente in der. Allgemeine AWS-Referenz	17. Februar 2021
Support für Amazon EFS als Datenspeicher	Transfer Family unterstützt jetzt Dateiübertragungen in und aus dem Amazon Elastic File System (Amazon EFS). Amazon EFS ist ein einfaches , skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem. Weitere Informationen finden Sie unter Ein Amazon EFS-Dateisystem konfigurieren.	06. Januar 2021
Support für AWS WAF	Transfer Family unterstützt AWS WAF jetzt eine Firewall für Webanwendungen, die Webanwendungen und API-Operationen vor Angriffen schützt. Weitere Informationen finden Sie unter Fügen Sie eine Firewall für Webanwendungen hinzu.	24. November 2020

Änderungen	Beschreibung	Date
Support für mehrere Sicherheitsgruppen in einer Virtual Private Cloud (VPC)	Sie können jetzt mehrere Sicherheitsgruppen an einen Server in einer VPC anhängen. Weitere Informationen finden Sie unter Erstellen Sie einen Server in einer virtuellen privaten Cloud .	15. Oktober 2020
Neu AWS-Regionen	Transfer Family ist jetzt in den AWS GovCloud (US) Regionen verfügbar. Weitere Informationen zu Transfer Family Family-Endpunkten für AWS GovCloud (US) Regionen finden Sie unter AWS Transfer Family Endpunkte und Kontingente in der Allgemeinen AWS-Referenz Informationen zur Verwendung von Transfer Family in den AWS GovCloud (US) Regionen finden Sie AWS Transfer Family im AWS GovCloud (US) Benutzerhandbuch.	30. September 2020
Eine Sicherheitsrichtlinie mit unterstützten kryptografischen Algorithmen kann jetzt an Ihren Server angehängt werden	Sie können Ihrem Server jetzt eine Sicherheitsrichtlinie hinzufügen, die eine Reihe unterstützter kryptografischer Algorithmen enthält. Weitere Informationen finden Sie unter Sicherheitsrichtlinien für Server AWS Transfer Family .	12. August 2020

Änderungen	Beschreibung	Date
Unterstützung von Endpunkten für den Federal Information Processing Standard (FIPS)	FIPS-enabled Endpunkte sind jetzt in Nordamerika verfügbar. AWS-Regionen Informationen zu den verfügbaren Regionen finden Sie unter AWS Transfer Family Endpunkte und Kontingente in der. Allgemeine AWS-Referenz Informationen zur Aktivierung von FIPS für einen SFTP-enabled Serverendpunkt finden Sie unter. Erstellen Sie einen SFTP-enabled Server Informationen zum Aktivieren von FIPS für einen FTPS-enabled Serverendpunkt finden Sie unter. Einen FTPS-enabled Server erstellen Informationen zum Aktivieren von FIPS für einen FTP-enabled Serverendpunkt finden Sie unter. Erstellen Sie einen FTP-enabled Server	12. August 2020
Erhöhung der Zeichenlänge des Benutzernamens und zusätzliche zulässige Zeichen	Benutzernamen können jetzt At-Zeichen (@) und Punkte (.) enthalten und dürfen eine maximale Länge von 100 Zeichen haben. Informationen zum Hinzufügen eines Benutzers finden Sie unter Benutzer für Serverendpunkte verwalten .	12. August 2020

Änderungen	Beschreibung	Date
Support für die automatische Erstellung von Amazon CloudWatch Logging AWS Identity and Access Management (IAM) -Rollen	Transfer Family unterstützt jetzt die automatische Erstellung einer CloudWatch Protokollierungs-IAM-Rolle zur Anzeige der Endbenutzeraktivitäten. Weitere Informationen finden Sie unter, Erstellen Sie einen SFTP-enabled Server , Einen FTPS-enabled Server erstellen oder Erstellen Sie einen FTP-enabled Server .	30. Juli 2020
AWS Transfer Family unterstützt jetzt Quell-IP als Autorisierungsfaktor.	Transfer Family bietet Unterstützung für die Verwendung der Quell-IP-Adressen von Endbenutzern als Autorisierungsfaktor, sodass Sie bei der Autorisierung des Zugriffs über Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS) oder File Transfer Protocol (FTP) eine zusätzliche Sicherheitsebene einrichten können. Weitere Informationen finden Sie unter Mit Anbietern benutzerdefinierter Identitäten arbeiten .	9. Juni 2020

Änderungen	Beschreibung	Date
AWS Transfer for SFTP ist jetzt verfügbar AWS Transfer Family und bietet Unterstützung für FTP und FTPS.	Sie können jetzt zwei zusätzliche Protokolle für die Dateiübertragungen Ihrer Benutzer verwenden: File Transfer Protocol Secure (FTPS) und File Transfer Protocol (FTP). Benutzer können zusätzlich zur bestehenden Unterstützung des Secure File Transfer Protocol (SFTP) auch FTP über SSL (FTPS) und FTP-basierte Klartext-Workflows verschieben AWS, ausführen, sichern und integrieren.	23. April 2020
Support für Virtual Private Cloud (VPC) -Sicherheitsgruppen und Elastic IP-Adressen	Sie können jetzt mithilfe von Sicherheitsgruppen eine Zulassungsliste für eingehende IP-Adressen erstellen und so eine zusätzliche Sicherheitsebene für Server bereitstellen. Sie können Elastic IP-Adressen auch dem Endpunkt Ihres Servers zuordnen. Auf diese Weise können Sie Benutzern hinter Firewalls den Zugriff auf diesen Endpunkt ermöglichen. Weitere Informationen finden Sie unter Erstellen Sie einen Server in einer virtuellen privaten Cloud .	10. Januar 2020

Änderungen	Beschreibung	Date
Support für die Arbeit in einer VPC	Sie können jetzt einen Server in einer VPC erstellen. Sie können Ihren Server verwenden, um Daten über Ihren Client zu und von einem Amazon S3 S3-Bucket zu übertragen, ohne das öffentliche Internet nutzen zu müssen. Weitere Informationen finden Sie unter Erstellen Sie einen Server in einer virtuellen privaten Cloud .	27. März 2019
Erste Version von AWS Transfer Family veröffentlicht.	Diese Erstversion umfasst das Einrichten von Verzeichnissen, beschreibt die ersten Schritte und stellt Informationen zur Client-Konfiguration, zur Benutzerkonfiguration und zur Überwachung bereit.	25. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.