



사용자 가이드

AWS Transfer Family



AWS Transfer Family: 사용자 가이드

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

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS Transfer Family란 무엇인가요?	1
AWS Transfer Family 작동 방식	3
Transfer Family와 관련된 블로그 게시물	4
사전 조건	7
리전, 엔드포인트 및 할당량	7
가입 AWS	7
스토리지 구성	8
Amazon S3 버킷 구성	9
Amazon EFS 파일 시스템 구성	12
IAM 역할 및 정책 생성	16
사용자 역할 생성	17
세션 정책의 작동 방식	20
읽기/쓰기 액세스 정책의 예	23
Transfer Family 자습서	26
서버 엔드포인트 시작하기	26
사전 조건	27
콘솔에 로그인	28
SFTP활성화 서버 생성	28
서비스 관리 사용자 추가	29
클라이언트를 사용하여 파일 전송	30
복호화 워크플로 생성	32
1단계: 실행 역할 구성	33
2단계: 관리형 워크플로 생성	34
3단계: 서버에 워크플로 추가 및 사용자 생성	35
4단계: PGP 키 페어 생성	37
5단계: 에 PGP 프라이빗 키 저장 AWS Secrets Manager	37
6단계: 파일 암호화	39
7단계: 워크플로 실행 및 결과 보기	39
SFTP 커넥터 생성 및 사용	40
1단계: 필요한 지원 리소스 생성	41
2단계: SFTP 커넥터 생성 및 테스트	46
3단계: SFTP 커넥터를 사용하여 파일 전송 및 검색	50
원격 서버로 사용할 Transfer Family SFTP 서버를 생성하는 절차	53
사용자 지정 자격 증명 공급자 사용	55

사전 조건	56
1단계: CloudFormation 스택 생성	56
2단계: 서버의 API 게이트웨이 메서드 구성 확인	57
3단계: Transfer Family 서버 세부 정보 보기	58
4단계: 사용자가 서버에 연결할 수 있는지 테스트	60
5단계: SFTP 연결 및 파일 전송 테스트	60
6단계: 버킷에 대한 액세스 제한	61
Amazon을 사용하는 경우 Lambda 업데이트 EFS	63
AS2 구성 설정	64
1단계: 에 대한 인증서 생성 AS2	66
2단계: AS2 프로토콜을 사용하는 Transfer Family 서버 생성	69
3단계: Transfer Family 인증서 리소스로 인증서 가져오기	72
4단계: 사용자와 사용자의 거래 파트너를 위한 프로필 생성	73
5단계: 사용자와 사용자의 파트너 간의 계약서 작성	74
6단계: 사용자와 사용자의 거래 파트너 간의 커넥터를 생성합니다.	75
7단계: Transfer FamilyAS2를 사용하여 파일 교환 테스트	76
SFTP, FTPS,용 Transfer Family FTP	78
자격 증명 공급자 옵션	78
AWS Transfer Family 엔드포인트 유형 매트릭스	80
Transfer Family 서버 엔드포인트 구성	84
SFTP활성화 서버 생성	86
FTPS활성화 서버 생성	97
FTP활성화 서버 생성	109
에서 서버 생성 VPC	119
사용자 지정 호스트 이름으로 작업	139
서버 엔드포인트를 통해 파일 전송	143
사용 가능한 SFTP/FTPS/FTP 명령	145
Amazon VPC 엔드포인트 찾기	146
setstat 오류 방지	148
열기 사용SSH	31
Win 사용SCP	149
Cyberduck 사용하기	31
사용 FileZilla	153
Perl 클라이언트 사용	154
업로드 후 처리	154
사용자 관리	155

서비스 관리형 사용자	157
디렉터리 서비스 사용자	166
사용자 지정 자격 증명 공급자 사용자	183
논리적 디렉터리 사용	210
논리적 디렉터리 사용 규칙	211
논리적 디렉터리 구현 및 chroot	213
논리적 디렉터리 구성 예	215
Amazon용 논리적 디렉터리 구성 EFS	216
사용자 지정 AWS Lambda 응답	217
SFTP 커넥터	218
SFTP 커넥터 구성	218
SFTP 커넥터 생성	219
SFTP 커넥터 알고리즘	226
SFTP 커넥터와 함께 사용할 보안 암호 저장	228
SFTP 커넥터 프라이빗 키 생성 및 형식 지정	229
SFTP 커넥터 테스트	232
SFTP 커넥터를 사용하여 파일 전송	234
SFTP 커넥터 관리	235
SFTP 커넥터 업데이트	236
SFTP 커넥터 세부 정보 보기	236
SFTP 커넥터 할당량	238
에 대한 Transfer Family AS2	240
AS2 사용 사례	241
구성 AS2	245
Transfer Family 콘솔을 사용하여 AS2 서버 생성	246
템플릿을 사용하여 AS2 서버 생성	249
AS2 구성	252
AS2 특징 및 기능	257
AS2 커넥터 구성	259
AS2 커넥터 생성	259
AS2 커넥터 알고리즘	262
AS2 커넥터에 대한 기본 인증	263
AS2 커넥터에 대한 기본 인증 활성화	265
커넥터 세부 정보 보기	269
AS2 파트너 관리	270
AS2 인증서 가져오기	270

AS2 인증서 교체	272
AS2 프로파일 생성	273
AS2 계약 생성	274
AS2 메시지 전송	275
AS2 메시지 전송	275
AS2 메시지 수신	277
HTTPS 에 대한 구성 AS2	278
AS2 커넥터를 사용하여 파일 전송	281
파일 이름 및 위치	282
상태 코드	284
샘플 JSON 파일	285
모니터 AS2	287
AS2 상태 코드	288
AS2 오류 코드	289
파일 처리 워크플로 관리	301
워크플로 만들기	303
워크플로 구성 및 실행	304
워크플로 세부 정보 보기	306
사전 정의된 단계 사용	309
파일 복사	309
파일 복호화	314
파일 태그 지정	319
파일 삭제	320
워크플로에 명명된 변수	321
태그 및 삭제 워크플로 예시	321
사용자 지정 파일 처리 단계 사용	326
여러 Lambda 함수를 연속적으로 사용	327
사용자 정의 처리 후 파일에 액세스	328
파일 업로드 AWS Lambda 시 로 전송된 이벤트 예	329
사용자 지정 워크플로 단계를 위한 Lambda 함수 예	330
IAM 사용자 지정 단계에 대한 권한	331
IAM 워크플로 정책	331
워크플로 신뢰 관계	333
실행 역할 예시: 복호화, 복사, 태그 지정	334
실행 역할 예시: 함수 실행 및 삭제	336
워크플로의 예외 처리	336

워크플로 실행 모니터링	337
CloudWatch 워크플로에 대한 로깅	337
CloudWatch 워크플로 지표	340
템플릿에서 워크플로 생성	340
Transfer Family 서버에서 워크플로 제거	344
제한 및 제약 조건	345
서버 관리	347
서버 목록 보기	347
서버 삭제	347
SFTP 서버 세부 정보 보기	349
AS2 서버 세부 정보 보기	350
서버 세부 정보 편집	352
File Transfer 프로토콜 편집	354
사용자 지정 자격 증명 제공자 파라미터 편집	357
서버 엔드포인트 편집	359
로깅 편집	361
보안 정책 편집	361
관리형 워크플로 변경	363
서버의 디스플레이 배너 변경	364
서버를 온라인이나 오프라인으로 전환	364
서버 호스트 키 관리	365
추가 서버 호스트 키 추가	366
서버 호스트 키 삭제	368
서버 호스트 키 교체	369
추가 서버 호스트 키 정보	370
콘솔 내 사용량 모니터링	370
액세스 통제 관리	374
S3 버킷 액세스 정책 생성	374
세션 정책 생성	376
사용자가 S3 버킷에서 <code>mkdir</code> 를 실행하지 못하도록 방지	379
로깅	381
CloudTrail 로깅	381
CloudTrail 로깅 활성화	383
서버 생성을 위한 로그 항목 예제	383
CloudWatch 로깅	385
서버에 대한 로깅 생성	385

워크플로에 대한 로깅 관리	393
에 대한 역할 구성 CloudWatch	396
Transfer Family 로그 스트림 보기	398
Amazon CloudWatch 경보 생성	401
S3 액세스 로그에 S3 API 호출 로깅	401
혼동된 대리자 문제를 제한하는 예	402
CloudWatch Transfer Family의 로그 구조	403
CloudWatch 로그 항목 예	408
CloudWatch 지표 사용	412
사용자 알림	415
를 사용하여 이벤트 관리 EventBridge	416
Transfer Family 이벤트	417
SFTP, FTPS 및 FTP 서버 이벤트	417
SFTP 커넥터 이벤트	418
A2S 이벤트	418
Transfer Family 이벤트 전송	419
이벤트 패턴 생성	419
이벤트에 대한 Transfer Family 이벤트 패턴 테스트	420
권한	421
추가 리소스	421
이벤트 세부 정보 참조	421
서버 이벤트	422
커넥터 이벤트	426
AS2 이벤트	431
보안	437
보안 정책 작업	438
암호화 알고리즘	439
TransferSecurityPolicy-2024년 1월	447
TransferSecurityPolicy-2023년 5월	448
TransferSecurityPolicy-2022년 3월	449
TransferSecurityPolicy-2020년 6월	450
TransferSecurityPolicy-2018년 11월	451
TransferSecurityPolicy-FIPS-2024년 1월	452
TransferSecurityPolicy-FIPS-2023년 5월	454
TransferSecurityPolicy-FIPS-2020년 6월	455
포스트 쿼텀 보안 정책	456

포스트 쿼터 보안 정책	461
의 포스트 쿼터 하이브리드 키 교환 정보 SSH	462
사용 방법	462
테스트 방법	463
데이터 보호	466
데이터 암호화	467
키 관리	469
자격 증명 및 액세스 관리	484
고객	485
ID를 통한 인증	485
정책을 사용한 액세스 관리	488
에서 AWS Transfer Family 를 사용하는 방법 IAM	491
자격 증명 기반 정책 예시	495
태그 기반 정책 예제	497
ID 및 액세스 문제 해결	501
규정 준수 확인	503
복원력	503
인프라 보안	504
웹 애플리케이션 방화벽	505
교차 서비스 혼동된 대리인 방지	506
Transfer Family 사용자 역할 전송	507
Transfer Family 워크플로 역할 전송	509
Transfer Family 로깅/호출 역할 이전	510
AWS 관리형 정책	512
AWSTransferConsoleFullAccess	512
AWSTransferFullAccess	514
AWSTransferLoggingAccess	516
AWSTransferReadOnlyAccess	516
정책 업데이트	517
Transfer Family 문제 해결	519
서비스 관리 사용자 문제 해결	519
Amazon EFS 서비스 관리형 사용자 문제 해결	520
퍼블릭 키 본문이 너무 긴 문제 해결	520
SSH 퍼블릭 키를 추가하지 못한 문제 해결	520
Amazon API Gateway 문제 해결	521
인증 오류가 너무 많음	521

연결 종료	522
암호화된 Amazon S3 버킷에 대한 정책 문제 해결	523
인증 문제 해결	523
인증 실패—SSH/SFTP	524
관리형 AD 불일치 영역 문제	524
기타 인증 문제	525
관리형 워크플로 문제 해결	525
Amazon을 사용하여 워크플로 관련 오류 해결 CloudWatch	525
워크플로 복사 오류 문제 해결	527
워크플로 복호화 문제 해결	528
Amazon EFS 문제 해결	530
누락된 POSIX 프로파일 문제 해결	530
Amazon을 사용한 논리적 디렉터리 문제 해결 EFS	531
ID 제공자 테스트 문제 해결	532
SFTP 커넥터에 대해 신뢰할 수 있는 호스트 키 추가 문제 해결	532
파일 업로드 문제 해결	533
Amazon S3 파일 업로드 오류 문제 해결	533
읽을 수 없는 파일 명칭 문제 해결	533
ResourceNotFound 예외 문제 해결	534
SFTP 커넥터 문제 해결	534
키 협상 실패	535
기타 SFTP 커넥터 문제	535
AS2 문제 해결	536
API 참조	537
환영합니다	537
작업	540
CreateAccess	543
CreateAgreement	550
CreateConnector	556
CreateProfile	563
CreateServer	567
CreateUser	580
CreateWorkflow	588
DeleteAccess	596
DeleteAgreement	599
DeleteCertificate	602

DeleteConnector	604
DeleteHostKey	606
DeleteProfile	609
DeleteServer	611
DeleteSshPublicKey	614
DeleteUser	617
DeleteWorkflow	620
DescribeAccess	622
DescribeAgreement	626
DescribeCertificate	629
DescribeConnector	632
DescribeExecution	635
DescribeHostKey	640
DescribeProfile	643
DescribeSecurityPolicy	646
DescribeServer	650
DescribeUser	655
DescribeWorkflow	660
ImportCertificate	665
ImportHostKey	670
ImportSshPublicKey	674
ListAccesses	679
ListAgreements	683
ListCertificates	687
ListConnectors	691
ListExecutions	694
ListHostKeys	699
ListProfiles	703
ListSecurityPolicies	707
ListServers	711
ListTagsForResource	715
ListUsers	720
ListWorkflows	725
SendWorkflowStepState	728
StartFileTransfer	731
StartServer	737

StopServer	740
TagResource	743
TestConnection	746
TestIdentityProvider	750
UntagResource	757
UpdateAccess	760
UpdateAgreement	767
UpdateCertificate	773
UpdateConnector	777
UpdateHostKey	782
UpdateProfile	786
UpdateServer	789
UpdateUser	801
데이터 유형	808
As2ConnectorConfig	811
CopyStepDetails	815
CustomStepDetails	817
DecryptStepDetails	819
DeleteStepDetails	822
DescribedAccess	824
DescribedAgreement	828
DescribedCertificate	832
DescribedConnector	836
DescribedExecution	840
DescribedHostKey	843
DescribedProfile	846
DescribedSecurityPolicy	848
DescribedServer	850
DescribedUser	858
DescribedWorkflow	862
EfsFileLocation	864
EndpointDetails	866
ExecutionError	870
ExecutionResults	872
ExecutionStepResult	873
FileLocation	875

HomeDirectoryMapEntry	876
IdentityProviderDetails	878
InputFileLocation	880
ListedAccess	881
ListedAgreement	884
ListedCertificate	887
ListedConnector	890
ListedExecution	892
ListedHostKey	894
ListedProfile	896
ListedServer	898
ListedUser	901
ListedWorkflow	904
LoggingConfiguration	906
PosixProfile	907
ProtocolDetails	909
S3FileLocation	912
S3InputFileLocation	914
S3StorageOptions	916
S3Tag	917
ServiceMetadata	918
SftpConnectorConfig	919
SshPublicKey	921
Tag	923
TagStepDetails	924
UserDetails	926
WorkflowDetail	928
WorkflowDetails	930
WorkflowStep	932
API 요청 만들기	934
Transfer Family 필수 요청 헤더	934
Transfer Family 요청 입력 및 서명	936
오류 응답	936
사용 가능한 라이브러리	938
공통 파라미터	939
일반적인 오류	941

문서 기록	943
AWS 용어집	953
.....	cmliv

AWS Transfer Family란 무엇인가요?

AWS Transfer Family 는 AWS 스토리지 서비스로 파일을 전송하거나 전송할 수 있는 보안 전송 서비스입니다. Transfer Family는 AWS 클라우드 플랫폼의 일부입니다. 는 SFTP, AS2, FTPS를 통해 Amazon S3 또는 Amazon 로 FTP 직접 또는 Amazon 에서 파일을 전송할 수 있도록 완전 관리형 지원을 AWS Transfer Family 제공합니다. 인증, 액세스 및 방화벽에 대한 기존 클라이언트 측 구성을 유지하여 파일 전송 워크플로를 원활하게 마이그레이션, 자동화 및 모니터링할 수 있으므로 고객, 파트너 및 내부 팀 또는 해당 애플리케이션에는 변경 사항이 없습니다.

자세한 내용을 알아보고 Amazon Web Services로 클라우드 애플리케이션 구축을 시작하려면 [시작하기 AWS](#)를 참조하세요.

AWS Transfer Family 는 다음 AWS 스토리지 서비스에서 또는 스토리지 서비스로 데이터를 전송할 수 있습니다.

- Amazon Simple Storage Service(S3) 스토리지 Amazon S3에 관한 자세한 내용은 [Amazon Simple Storage Service 시작하기](#)를 참조하세요.
- Amazon Elastic File System(Amazon EFS) Network File System(NFS) 파일 시스템. Amazon 에 대한 자세한 내용은 [Amazon Elastic File System?](#)를 EFS참조하세요.

AWS Transfer Family 는 다음 프로토콜을 통해 데이터 전송을 지원합니다.

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP): 버전 3
- 파일 전송 프로토콜 보안(FTPS)
- 파일 전송 프로토콜(FTP)
- 적용 가능성 설명 2(AS2)

Note

FTP 및 FTPS 데이터 연결의 경우 Transfer Family가 데이터 채널을 설정하는 데 사용하는 포트 범위는 8192~8200입니다.

File Transfer 프로토콜은 금융 서비스, 의료, 광고, 소매를 비롯한 다양한 산업의 데이터 교환 워크플로에서 활용됩니다. Transfer Family는 파일 전송 워크플로를 로 마이그레이션하는 작업을 간소화합니다 AWS.

다음은 Amazon S3에서 Transfer Family를 사용하는 몇 가지 일반적인 사용 사례입니다.

- 공급업체 및 파트너와 같은 타사의 업로드를 AWS 위한 의 데이터 레이크입니다.
- 고객과의 구독 기반 데이터 배포.
- 조직 내의 내부 전송.

다음은 Amazon 에서 Transfer Family를 사용하기 위한 몇 가지 일반적인 사용 사례입니다EFS.

- 데이터 분산
- 공급망
- 콘텐츠 관리
- 웹 서비스 애플리케이션

다음은 에서 Transfer Family를 사용하기 위한 몇 가지 일반적인 사용 사례입니다AS2.

- 프로토콜에 내장된 데이터 보호 및 보안 기능을 필요로 하는 컴플라이언스 요구 사항이 있는 워크플로
- 공급망 물류
- 결제 워크플로
- Business-to-business (B2B) 트랜잭션
- 엔터프라이즈 리소스 계획(ERP) 및 고객 관계 관리(CRM) 시스템과 통합

Transfer Family를 사용하면 서버 인프라를 실행할 필요 AWS 없이 에서 파일 전송 프로토콜 지원 서버에 액세스할 수 있습니다. 이 서비스를 사용하여 최종 사용자의 클라이언트 및 구성을 그대로 AWS 유지하면서 파일 전송 기반 워크플로를 로 마이그레이션할 수 있습니다. 먼저 호스트 이름을 서버 엔드포인트에 연결한 다음, 사용자를 추가하고 적절한 수준의 액세스를 제공해야 합니다. 이 작업이 끝나면, 사용자의 전송 요청은 Transfer Family 서버 엔드포인트에서 바로 처리됩니다.

Transfer Family는 다음과 같은 이점이 있습니다.

- 사용자의 필요에 맞게 실시간으로 확장되는 종합 관리형 서비스입니다.
- 애플리케이션을 수정하거나 File Transfer 프로토콜 인프라를 실행하지 않아도 됩니다.
- 내구성이 뛰어난 Amazon S3 스토리지의 데이터를 사용하면 처리, 분석, 보고, 감사 및 아카이브 할 수 AWS 서비스 에 네이티브를 사용할 수 있습니다.

- Amazon을 데이터 스토어 EFS로 사용하면 AWS 클라우드 서비스 및 온프레미스 리소스와 함께 사용할 수 있는 완전 관리형 탄력적 파일 시스템을 얻을 수 있습니다. AmazonEFS은 애플리케이션을 중단하지 않고 필요에 따라 페타바이트로 확장할 수 있도록 구축되었으며, 파일을 추가하고 제거할 때 자동으로 증가하고 축소됩니다. 따라서 확장을 수용하기 위해 용량을 프로비저닝하고 관리할 필요가 없습니다.
- AWS Transfer Family를 사용하여 업로드한 파일의 처리를 쉽게 설정, 실행, 자동화 및 모니터링할 수 있게 해주는 완전 관리형 서버리스 File Transfer 워크플로 서비스입니다.
- 선결제 비용이 없으며, 서비스를 사용한 만큼만 지불하면 됩니다.

다음 섹션에서는 Transfer Family의 다양한 기능에 대한 설명, 시작하기 자습서, 다양한 프로토콜 지원 서버를 설정하는 방법, 다양한 유형의 자격 증명 공급자를 사용하는 방법 및 서비스 API 참조를 확인할 수 있습니다.

Transfer Family를 시작하려면 다음을 참조하세요.

- [AWS Transfer Family 작동 방식](#)
- [사전 조건](#)
- [AWS Transfer Family 서버 엔드포인트 시작하기](#)

AWS Transfer Family 작동 방식

AWS Transfer Family는 다음 프로토콜을 통해 Amazon Simple Storage Service(Amazon S3) 스토리지 또는 Amazon Elastic File System(AmazonEFS) 파일 시스템으로 파일을 주고 받는 데 사용할 수 있는 완전 관리형 AWS 서비스입니다.

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP): 버전 3
- 파일 전송 프로토콜 보안(FTPS)
- 파일 전송 프로토콜(FTP)
- 적용 가능성 설명 2(AS2)

AWS Transfer Family는 최대 3개의 가용 영역을 지원하며 연결 및 전송 요청을 위한 자동 조정, 중복 플릿을 지원합니다. 지연 시간 기반 라우팅을 사용하여 중복성을 높이고 네트워크 지연 시간을 최소화하는 방법에 대한 예제는 블로그 게시물 [SFTP 서버용 AWS 전송으로 네트워크 지연 시간 최소화를 참조하세요](#).

Transfer Family Managed File Transfer Workflows(MFTW)는 완전 관리형 서버리스 파일 전송 워크플로 서비스로, 를 사용하여 업로드된 파일의 처리를 쉽게 설정, 실행, 자동화 및 모니터링할 수 있습니다. AWS Transfer Family. 고객은 MFTW 를 사용하여 Transfer Familycompressing/decompressing, and encrypting/decrypting를 사용하여 전송되는 데이터 복사, 태그 지정, 스캔, 필터링과 같은 다양한 처리 단계를 자동화할 수 있습니다. 이를 통해 추적 및 감사에 대한 엔드 투 엔드 가시성이 제공됩니다. 자세한 내용은 [AWS Transfer Family 관리형 워크플로](#)를 참조하세요.

AWS Transfer Family 는 모든 표준 파일 전송 프로토콜 클라이언트를 지원합니다. 다음은 대표적인 클라이언트입니다.

- [열기SSH](#) - Macintosh 및 Linux 명령줄 유틸리티입니다.
- [WinSCP](#) - Windows 전용 그래픽 클라이언트입니다.
- [Cyberduck](#) - Linux, Macintosh, Microsoft Windows 그래픽 클라이언트.
- [FileZilla](#) - Linux, Macintosh 및 Windows 그래픽 클라이언트입니다.

Transfer Family와 관련된 블로그 게시물

다음 표에는 Transfer Family 고객에게 유용한 정보가 들어 있는 블로그 게시물이 나와 있습니다. 표는 시간 역순으로 정렬되어 있어 가장 최근 게시물이 표의 맨 앞에 표시됩니다.

블로그 게시물 제목 및 링크	날짜
Transfer Family가 안전하고 규정을 준수하는 관리형 파일 전송 솔루션을 구축하는 데 도움이 되는 방법	2024년 1월 3일
를 사용하여 맬웨어 위협 탐지 AWS Transfer Family	2023년 7월 20일
를 사용하여 SAP 워크로드 확장 AWS Transfer Family	2023년 7월 13일
PGP 및 를 사용하여 파일 암호화 및 복호화 AWS Transfer Family	2023년 6월 21일
Azure Active Directory 및 를 AWS Transfer Family 사용하여 에 인증 AWS Lambda	2022년 12월 15일

블로그 게시물 제목 및 링크	날짜
AWS Transfer Family 관리형 워크플로를 사용하여 파일 전송 알림 사용자 지정	2022년 10월 14일
AWS Transfer Family 워크플로를 사용하여 클라우드 네이티브 File Transfer 플랫폼 구축	2022년 1월 5일
A AWS Transfer Family 및 를 사용하여 사용자 셀프 서비스 키 관리를 활성화합니다 AWS Lambda.	2021년 12월 17일
AWS Transfer Family 및 Amazon S3를 사용하여 데이터 액세스 제어 개선	2021년 10월 5일
AWS Global Accelerator 및 AWS Transfer Family 서비스를 사용하여 인터넷 연결 파일 전송 처리량 개선	2021년 6월 7일
AWS 웹 애플리케이션 방화벽 및 Amazon API Gateway AWS Transfer Family 를 사용한 보안	2021년 5월 5일
AWS 웹 애플리케이션 방화벽 및 Amazon API Gateway AWS Transfer Family 를 사용한 보안	2021년 1월 15일
AWS Transfer Family Amazon Elastic File System 지원	2021년 1월 7일
AWS Transfer Family 를 사용하기 위한 암호 인증 활성화 AWS Secrets Manager	2020년 11월 5일
AWS Transfer Family 및 를 사용하여 데이터 액세스 중앙 집중화 AWS Storage Gateway	2020년 6월 22일
AWS Lambda 서버리스 애플리케이션에서 Amazon EFS for 사용	2020년 6월 18일
IP 허용 목록을 사용하여 AWS Transfer Family 서버 보호	2020년 4월 8일

블로그 게시물 제목 및 링크	날짜
SFTP 서버 AWS 전송으로 네트워크 지연 시간 최소화	2020년 2월 19일
로 SFTP 서버 리프트 앤 시프트 마이그레이션 AWS	2020년 2월 12일
chroot 및 논리적 디렉터리로 구조 간소화 AWS SFTP	2019년 9월 26일
에서 Okta를 자격 증명 공급자로 사용 AWS Transfer Family	2019년 5월 30일

사전 조건

다음 섹션에서는 AWS Transfer Family 서비스를 사용하는 데 필요한 사전 조건을 설명합니다. 최소한 Amazon Simple Storage Service(Amazon S3) 버킷을 생성하고 AWS Identity and Access Management (IAM) 역할을 통해 해당 버킷에 대한 액세스를 제공해야 합니다. 또한 사용자는 신뢰 관계도 수립해야 합니다. 이 신뢰 관계를 통해 Transfer Family는 사용자의 파일 전송 요청을 처리할 수 있도록 버킷에 액세스할 IAM 역할을 맡을 수 있습니다.

주제

- [지원되는 AWS 리전, 엔드포인트 및 할당량](#)
- [가입 AWS](#)
- [와 함께 사용할 스토리지 구성 AWS Transfer Family](#)
- [IAM 역할 및 정책 생성](#)

지원되는 AWS 리전, 엔드포인트 및 할당량

AWS 서비스에 프로그래밍 방식으로 연결하려면 엔드포인트를 사용합니다. 예를 들어 미국 동부(오하이오) 리전()에 있는 고객의 엔드포인트us-east-2는 입니다transfer.us-east-2.amazonaws.com. 서비스 할당량은 AWS 계정계정의 최대 서비스 리소스 또는 작업 수입니다. 이 가이드에서는 [AS2 할당량](#) 및 에서 할당량을 찾을 수 있습니다[SFTP 커넥터 할당량](#).

지원되는 AWS 리전, 엔드포인트 및 서비스 할당량에 대한 자세한 내용은 의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요Amazon Web Services 일반 참조.

가입 AWS

Amazon Web Services(AWS)에 가입하면 AWS 를 AWS포함한 의 모든 서비스에 계정이 자동으로 가입됩니다 AWS Transfer Family. 사용자에게는 사용한 서비스에 대해서만 요금이 청구됩니다.

AWS 계정이 이미 있는 경우 다음 작업으로 건너뛰니다. AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성합니다.

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

1. <https://portal.aws.amazon.com/billing/가입> 을 엽니다.

2. 온라인 지시 사항을 따릅니다.

등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

에 가입하면 AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 [관리 사용자에게 관리자 액세스 권한을 할당하고](#), 루트 사용자만 [루트 사용자 액세스 권한이 필요한 태스크](#)를 수행하는 것입니다.

Transfer Family 사용 비용 견적을 AWS Pricing Calculator 얻는 데 사용할 요금 및 에 대한 자세한 내용은 [AWS Transfer Family 요금](#) 섹션을 참조하세요.

AWS 리전 가용성에 대한 자세한 내용은 의 [AWS Transfer Family 엔드포인트 및 할당량을 참조하세요](#) AWS 일반 참조.

와 함께 사용할 스토리지 구성 AWS Transfer Family

이 주제에서는 에서 사용할 수 있는 스토리지 옵션에 대해 설명합니다 AWS Transfer Family. Transfer Family 서버의 스토리지 EFS로 Amazon S3 또는 Amazon을 사용할 수 있습니다.

목차

- [Amazon S3 버킷 구성](#)
 - [Amazon S3 액세스 포인트](#)
 - [Amazon S3 HeadObject 동작](#)
 - [파일을 쓰고 나열할 수 있는 권한만 부여](#)
 - [많은 수의 제로바이트 객체로 인해 지연 시간 문제가 발생합니다.](#)
- [Amazon EFS 파일 시스템 구성](#)
 - [Amazon EFS 파일 소유권](#)
 - [Transfer Family용 Amazon EFS 사용자 설정](#)
 - [Amazon에서 Transfer Family 사용자 구성 EFS](#)
 - [Amazon EFS 루트 사용자 생성](#)
 - [지원되는 Amazon EFS 명령](#)

Amazon S3 버킷 구성

AWS Transfer Family 는 사용자의 전송 요청을 서비스하기 위해 Amazon S3 버킷에 액세스하므로 파일 전송 프로토콜 지원 서버 설정의 일부로 Amazon S3 버킷을 제공해야 합니다. 기존 버킷을 사용할 수도 있고, 새 버킷을 만들어도 됩니다.

Note

동일한 AWS 리전에 있는 SFTP 서버 및 S3 버킷을 사용할 필요는 없지만 모범 사례로 권장됩니다.

사용자를 설정할 때 각 사용자에게 IAM 역할을 할당합니다. 이 역할은 Amazon S3 버킷에 대한 사용자의 액세스 수준을 결정합니다.

새 버킷 생성에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [S3 버킷을 생성하려면 어떻게 해야 하나요?](#)를 참조하세요.

Note

Amazon S3 객체 잠금을 사용하면 일정한 시간 동안 또는 무기한으로 객체를 덮어쓰지 않도록 할 수 있습니다. 이는 다른 서비스와 마찬가지로 Transfer Family에서도 동일한 방식으로 작동합니다. 객체가 존재하고 보호되는 경우 해당 파일에 쓰거나 삭제할 수 없습니다. Amazon S3 객체 잠금에 대한 자세한 내용은 [Amazon Simple Storage Service 사용 설명서](#)의 Amazon S3 객체 잠금 사용을 참조하세요.

Amazon S3 액세스 포인트

AWS Transfer Family 는 공유 데이터 세트에 대한 세분화된 액세스를 쉽게 관리할 수 있는 [Amazon S3의 기능인 Amazon S3 액세스 포인트](#)를 지원합니다. Amazon S3 버킷 이름을 사용하는 모든 곳에서 S3 액세스 포인트 별칭을 사용할 수 있습니다. Amazon S3 버킷의 공유 데이터에 액세스할 수 있는 서로 다른 권한을 가진 사용자를 위해 Amazon S3에 수백 개의 액세스 포인트를 생성할 수 있습니다.

예를 들어 액세스 포인트를 사용하여 서로 다른 세 팀이 동일한 공유 데이터 세트에 액세스하도록 허용할 수 있습니다. 한 팀은 S3에서 데이터를 읽고, 두 번째 팀은 S3에 데이터를 쓰고, 세 번째 팀은 S3에서 데이터를 읽고, 쓰고, 삭제할 수 있습니다. 위에서 언급한 대로 세분화된 액세스 제어를 구현하려면 여러 팀에 비대칭 액세스를 제공하는 정책이 포함된 S3 액세스 포인트를 생성할 수 있습니다. Transfer

Family 서버와 함께 S3 액세스 포인트를 사용하면 수백 개의 사용 사례를 아우르는 복잡한 S3 버킷 정책을 만들지 않고도 세밀한 액세스 제어를 달성할 수 있습니다. Transfer Family 서버에서 S3 액세스 포인트를 사용하는 방법에 대한 자세한 내용은 [AWS Transfer Family 및 Amazon S3 블로그 게시물을 사용하여 데이터 액세스 제어 강화](#)를 참조하세요.

Note

AWS Transfer Family 는 현재 Amazon S3 다중 리전 액세스 포인트를 지원하지 않습니다.

Amazon S3 HeadObject 동작

Note

Transfer Family 서버를 생성하거나 업데이트할 때 Amazon S3 디렉터리의 성능을 최적화하여 HeadObject 호출을 없앨 수 있습니다.

Amazon S3에서 버킷과 객체는 기본 리소스이며 객체는 버킷에 저장됩니다. Amazon S3는 계층적 파일 시스템을 모방할 수 있지만 때로는 일반적인 파일 시스템과 다르게 동작할 수 있습니다. 예를 들어 디렉터리는 Amazon S3의 일류 개념이 아니라 객체 키를 기반으로 합니다. 는 객체의 키를 슬래시 문자(/)로 분할하고, 마지막 요소를 파일 이름으로 처리한 다음, 접두사가 동일한 파일 이름을 동일한 경로 아래에 그룹화하여 디렉터리 경로를 AWS Transfer Family 제공합니다. mkdir를 사용하거나 Amazon S3 콘솔을 사용하여 빈 디렉터리를 생성할 때 폴더 경로를 나타내는 0바이트 객체가 생성됩니다. 이러한 객체의 키는 후행 슬래시로 끝납니다. 이러한 0바이트 객체에 대한 설명은 Amazon S3 사용 설명서의 [폴더를 사용하여 Amazon S3 콘솔에서 객체 구성](#)에 설명되어 있습니다.

ls 명령을 실행하고 일부 결과가 Amazon S3 0바이트 객체(이러한 객체에는 슬래시 문자로 끝나는 키가 있음)인 경우 Transfer Family는 이러한 각 객체에 대한 HeadObject 요청을 발행합니다(자세한 내용은 Amazon Simple Storage Service API 참조[HeadObject](#)의 참조). 이로 인해 Transfer Family를 통해 Amazon S3를 스토리지로 사용할 때 다음과 같은 문제가 발생할 수 있습니다.

파일을 쓰고 나열할 수 있는 권한만 부여

경우에 따라 Amazon S3 객체에 대한 쓰기 액세스 권한만 제공할 수 있습니다. 예를 들어, 버킷에 객체를 쓰기(또는 업로드) 및 나열할 수 있는 액세스 권한을 제공하지만 객체를 읽기(다운로드)할 수 있는 액세스 권한은 제공하지 않을 수 있습니다. 파일 전송 클라이언트를 사용하여 ls 및 mkdir 명령을 수행하려면 Amazon S3 ListObjects 및 PutObject 권한이 있어야 합니다. 그러나 Transfer Family가

파일 쓰기 또는 나열을 HeadObject 직접 호출해야 하는 경우 이 호출에는 GetObject 권한이 필요하기 때문에 액세스 거부 오류로 호출이 실패합니다.

Note

Transfer Family 서버를 생성하거나 업데이트할 때 Amazon S3 디렉터리의 성능을 최적화하여 HeadObject 호출을 없앨 수 있습니다.

이 경우 슬래시 AWS Identity and Access Management (IAM)로 끝나는 객체에 대해서만 GetObject 권한을 추가하는 () 정책 조건을 추가하여 액세스 권한을 부여할 수 있습니다/. 이 조건은 파일에 대한 GetObject 호출을 방지하지만(읽을 수 없도록) 사용자가 폴더를 나열하고 트래버스할 수 있도록 허용합니다. 다음 예제 정책은 Amazon S3 버킷에 대한 쓰기 및 목록 액세스만 제공합니다. 이 정책을 사용하려면 **DOC-EXAMPLE-BUCKET**를 버킷 이름으로 바꿉니다.

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

```

    ],
    "NotResource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/"
    ]
  }
]
}

```

Note

이 정책은 사용자의 파일 추가를 허용하지 않습니다. 즉, 이 정책을 적용받는 사용자는 파일을 열어 콘텐츠에 콘텐츠를 추가하거나 수정할 수 없습니다. 또한 사용 사례에서 파일을 업로드하기 전에 HeadObject을 호출해야 하는 경우에는 이 정책이 적용되지 않습니다.

많은 수의 제로바이트 객체로 인해 지연 시간 문제가 발생합니다.

Amazon S3 버킷에 이러한 0바이트 객체가 많이 포함되어 있는 경우 Transfer Family는 많은 HeadObject 호출을 발생시켜 처리 지연을 초래할 수 있습니다.

이 문제를 해결할 수 있는 한 가지 방법은 모든 0바이트 객체를 삭제하는 것입니다. 유념할 사항:

- 빈 디렉터리가 더 이상 존재하지 않습니다. 디렉터리는 객체 키에 이름이 포함되어 있기 때문에 존재할 수 있습니다.
- 다른 사용자가 mkdir을 호출하여 문제가 생기는 것을 막지는 못합니다. 디렉터리 생성을 방지하는 정책을 만들어 이 문제를 완화할 수 있습니다.
- 일부 시나리오에서는 이러한 0바이트 객체를 사용합니다. 예를 들어 /inboxes/customer1000과 같은 구조를 사용하면 받은 편지함 디렉터리가 매일 정리됩니다.

또 다른 해결 방법은 정책 조건을 통해 표시되는 개체 수를 제한하여 HeadObject 호출 수를 줄이는 것입니다. 실행 가능한 솔루션이 되려면 모든 하위 디렉터리의 제한된 집합만 볼 수 있다는 점을 인정해야 합니다.

Amazon EFS 파일 시스템 구성

AWS Transfer Family 는 Amazon Elastic File System(Amazon EFS)에 액세스하여 사용자의 전송 요청을 서비스합니다. 따라서 EFS 파일 전송 프로토콜 지원 서버 설정의 일환으로 Amazon 파일 시스템을 제공해야 합니다. 기존 파일 시스템을 사용할 수도 있고, 새 버킷을 만들어도 됩니다.

유의할 사항:

- Transfer Family 서버와 Amazon EFS 파일 시스템을 사용하는 경우 서버와 파일 시스템은 동일한 계정에 있어야 합니다 AWS 리전.
- 서버와 파일 시스템이 같은 계정에 속할 필요는 없습니다. 서버와 파일 시스템이 같은 계정에 속하지 않는 경우 파일 시스템 정책에서 사용자 역할에 명시적 권한을 부여해야 합니다.

여러 계정을 설정하는 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [조직 내 AWS 계정 관리를 참조하세요](#).

- 사용자를 설정할 때 각 사용자에게 IAM 역할을 할당합니다. 이 역할은 Amazon EFS 파일 시스템에 대한 액세스 수준을 결정합니다.
- Amazon EFS 파일 시스템 탑재에 대한 자세한 내용은 [Amazon EFS 파일 시스템 탑재를 참조하세요](#).

AWS Transfer Family 및 Amazon이 함께 EFS 작동하는 방법에 대한 자세한 내용은 Amazon Elastic [EFS File System 사용 설명서의 AWS Transfer Family 를 사용하여 Amazon 파일 시스템의 파일에 액세스](#)하기를 참조하세요. Amazon Elastic File System

Amazon EFS 파일 소유권

AmazonEFS은 휴대용 운영 체제 인터페이스(POSIX) 파일 권한 모델을 사용하여 파일 소유권을 나타냅니다.

에서 시스템의 POSIX사용자는 세 가지 고유한 권한 클래스로 분류됩니다. 사용자가 를 사용하여 Amazon EFS 파일 시스템에 저장된 파일에 액세스하도록 허용 AWS Transfer Family하면 해당 사용자에게 “POSIX프로필”을 할당해야 합니다. 이 프로필은 Amazon 파일 시스템의 EFS 파일 및 디렉터리에 대한 액세스를 결정하는 데 사용됩니다.

- 사용자(u): 파일 또는 디렉터리의 소유자. 일반적으로 파일이나 디렉토리를 만든 사람이 소유자이기도 합니다.
- 그룹(g): 공유하는 파일 및 디렉터리에 대해 동일한 액세스 권한이 필요한 사용자 집합입니다.
- 기타(o): 소유자 및 그룹 구성원을 제외하고 시스템에 액세스할 수 있는 다른 모든 사용자. 이 권한 클래스를 “Public”이라고도 합니다.

POSIX 권한 모델에서 모든 파일 시스템 객체(파일, 디렉터리, 심볼 링크, 명명된 파이프 및 소켓)는 이전에 언급한 세 가지 권한 세트와 연결됩니다. Amazon EFS 객체에는 Unix 스타일 모드가 연결되어 있습니다. 이 모드 값은 해당 객체에 대한 작업을 수행할 수 있는 권한을 정의합니다.

또한 Unix 스타일 시스템에서 사용자와 그룹은 Amazon이 파일 소유권을 나타내는 데 EFS 사용하는 숫자 식별자에 매핑됩니다. Amazon의 경우 EFS 객체는 단일 소유자와 단일 그룹이 소유합니다. Amazon EFS는 사용자가 파일 시스템 객체 IDs에 액세스하려고 할 때 매핑된 숫자를 사용하여 권한을 확인합니다.

Transfer Family용 Amazon EFS 사용자 설정

Amazon EFS 사용자를 설정하기 전에 다음 중 하나를 수행할 수 있습니다.

- 사용자를 생성하고 Amazon에서 홈 폴더를 설정할 수 있습니다. EFS 세부 정보는 [Amazon에서 Transfer Family 사용자 구성 EFS](#)를 참조하세요.
- 루트 사용자를 추가하는 것이 편하다면 [Amazon EFS 루트 사용자 생성](#)을 할 수 있습니다.

Note

Transfer Family 서버는 Amazon EFS 액세스 포인트의 POSIX 권한 설정을 지원하지 않습니다. Transfer Family 사용자의 POSIX 프로필(이전 섹션에 설명됨)은 POSIX 권한을 설정할 수 있는 기능을 제공합니다. 이러한 권한은, UID GID 및 보조를 기반으로 세분화된 액세스를 위해 사용자 수준에서 설정됩니다. GIDs.

Amazon에서 Transfer Family 사용자 구성 EFS

Transfer Family는 사용자를 에 아직 존재하지 UID/GID and directories you specify. If the UID/GID/directories 않는 에 매핑한 EFS 다음 사용자에게 전송에서 할당하기 전에 사용자를 생성해야 합니다. Amazon EFS 사용자 생성에 대한 세부 정보는 Amazon Elastic File System [File System 사용 설명서의 Network File System\(NFS\) 수준에서 사용자, 그룹 및 권한 작업에](#) 설명되어 있습니다.

Transfer Family에서 Amazon EFS 사용자를 설정하는 단계

1. [PosixProfile](#) 필드를 사용하여 Transfer Family에서 사용자의 EFS UID 및 를 매핑 GID 합니다.
2. 로그인 시 사용자가 특정 폴더에서 시작하도록 하려면 [HomeDirectory](#) 필드 아래에 EFS 디렉터리를 지정할 수 있습니다.

CloudWatch 규칙 및 Lambda 함수를 사용하여 프로세스를 자동화할 수 있습니다. 와 상호 작용하는 Lambda 함수의 예는 서버리스 애플리케이션에서 Amazon for 사용을 EFS 참조하세요. [EFS AWS Lambda](#)

또한 Transfer Family 사용자를 위한 논리적 디렉터리를 구성할 수 있습니다. 자세한 내용은 [논리적 디렉터리를 사용하여 Transfer Family 디렉터리 구조를 단순화합니다](#). 항목의 [Amazon용 논리적 디렉터리 구성 EFS](#)를 참조하세요.

Amazon EFS 루트 사용자 생성

조직에서 사용자 구성을 위해 SFTP/FTPS를 통해 루트 사용자 액세스를 활성화하는 것이 편한 경우, UID 이고 0GID인 사용자(루트 사용자)를 생성한 다음 해당 루트 사용자를 사용하여 폴더를 생성하고 나머지 사용자의 POSIX ID 소유자를 할당할 수 있습니다. 이 옵션의 장점은 Amazon EFS 파일 시스템을 탑재할 필요가 없다는 것입니다.

[Amazon EFS 서비스 관리형 사용자 추가](#)에 설명된 단계를 수행하고, 사용자 ID와 그룹 ID 모두에 0을 입력합니다.

지원되는 Amazon EFS 명령

다음 명령은 Amazon EFS for 에서 지원됩니다 AWS Transfer Family.

- cd
- ls/dir
- pwd
- put
- get
- rename
- chown: 루트(즉, uid=0인 사용자)만 파일 및 디렉터리의 소유권과 권한을 변경할 수 있습니다.
- chmod: 루트(즉, uid=0인 사용자)만 파일 및 디렉터리의 소유권과 권한을 변경할 수 있습니다.
- chgrp: 루트 또는 파일 소유자만 파일 그룹을 보조 그룹 중 하나로 변경할 수 있는 파일 소유자만 지원됩니다.
- ln -s/symlink
- mkdir
- rm/delete
- rmdir
- chmtime

IAM 역할 및 정책 생성

이 주제에서는 와 함께 사용할 수 있는 정책 및 역할의 유형을 설명하고 사용자 역할을 생성하는 프로세스를 AWS Transfer Family 안내합니다. 또한 세션 정책의 작동 방식을 설명하고 사용자 역할 예를 제공합니다.

AWS Transfer Family 는 다음 유형의 역할을 사용합니다.

- 사용자 역할 - 서비스 관리형 사용자가 필요한 Transfer Family 리소스에 액세스할 수 있도록 허용합니다. Transfer Family 사용자 의 컨텍스트에서 이 역할을 AWS Transfer Family 가정합니다ARN.
- 액세스 역할 - 전송 중인 Amazon S3 파일에만 액세스할 수 있습니다. 인바운드 AS2 전송의 경우 액세스 역할은 계약에 Amazon 리소스 이름(ARN)을 사용합니다. 아웃바운드 AS2 전송의 경우 액세스 역할은 커넥터에 ARN 를 사용합니다.
- 호출 역할 - 서버의 사용자 지정 자격 증명 공급자로 Amazon API Gateway와 함께 사용됩니다. Transfer Family는 Transfer Family 서버 의 컨텍스트에서 이 역할을 맡습니다ARN.
- 로깅 역할 - Amazon 에 항목을 로깅하는 데 사용됩니다 CloudWatch. Transfer Family는 이 역할을 사용하여 File Transfer에 대한 정보와 함께 성공 및 실패 세부 정보를 기록합니다. Transfer Family는 Transfer Family 서버 의 컨텍스트에서 이 역할을 맡습니다ARN. 아웃바운드 AS2 전송의 경우 로깅 역할은 커넥터 를 사용합니다ARN.
- 실행 역할 - Transfer Family 사용자가 전화를 걸어 워크플로를 시작할 수 있습니다. Transfer Family 는 Transfer Family 워크플로의 맥락에서 이 역할을 맡습니다ARN.

이러한 역할 외에도 세션 정책을 사용할 수 있습니다. 세션 정책은 필요한 경우 액세스를 제한하는 데 사용됩니다. 이러한 정책은 독립형이라는 점에 유의하세요. 즉, 이러한 정책은 역할에 추가할 수 없습니다. 대신 Transfer Family 사용자에게 직접 세션 정책을 추가할 수 있습니다.

Note

서비스 관리 Transfer Family 사용자를 생성하는 경우 홈 폴더를 기반으로 정책 자동 생성을 선택할 수 있습니다. 사용자 액세스를 자신의 폴더에 제한하려는 경우 유용한 단축키입니다. 또한 [세션 정책의 작동 방식](#)에서 세션 정책 및 예에 대한 세부 정보를 볼 수 있습니다. 세션 정책에 대한 자세한 내용은 IAM 사용 설명서의 [세션 정책](#)에서 확인할 수도 있습니다.

주제

- [사용자 역할 생성](#)

- [세션 정책의 작동 방식](#)
- [읽기/쓰기 액세스 정책의 예](#)

사용자 역할 생성

사용자를 만들 때, 사용자 액세스에 관한 결정을 여러 번 해야 합니다. 이러한 결정에는 사용자가 액세스할 수 있는 Amazon S3 버킷 또는 Amazon EFS 파일 시스템, 각 Amazon S3 버킷의 일부 및 파일 시스템의 파일에 액세스할 수 있는 권한, 사용자가 보유한 권한(예: PUT 또는 GET)이 포함됩니다.

액세스를 설정하려면 해당 액세스 정보를 제공하는 자격 증명 기반 AWS Identity and Access Management (IAM) 정책 및 역할을 생성합니다. 이 프로세스의 일환으로 사용자에게 EFS 파일 작업의 대상 또는 소스인 Amazon S3 버킷 또는 Amazon 파일 시스템에 대한 액세스 권한을 제공합니다. 이렇게 하려면 나중에 자세하게 설명하는, 다음과 같은 상위 수준 단계를 거쳐야 합니다.

사용자 역할 생성

1. [에 대한 IAM 정책을 생성합니다 AWS Transfer Family](#). 이에 대한 설명은 [에 대한 IAM 정책을 생성하려면 AWS Transfer Family](#)에 나와 있습니다.
2. IAM 역할을 생성하고 새 IAM 정책을 연결합니다. 예시는 [읽기/쓰기 액세스 정책의 예](#)에서 확인하십시오.
3. AWS Transfer Family 및 IAM 역할 간에 신뢰 관계를 설정합니다. 이에 대한 설명은 [신뢰 관계를 구축하기 위해](#)에 나와 있습니다.

다음 절차에서는 IAM 정책 및 역할을 생성하는 방법을 설명합니다.

에 대한 IAM 정책을 생성하려면 AWS Transfer Family

1. [에서 IAM 콘솔을 엽니다](https://console.aws.amazon.com/iam/) <https://console.aws.amazon.com/iam/>.
2. 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
3. 정책 생성 페이지에서 JSON 탭을 선택합니다.
4. 나타나는 편집기에서 편집기의 내용을 IAM 역할에 연결할 IAM 정책으로 바꿉니다.

읽기/쓰기 액세스 권한을 부여하거나 사용자를 홈 디렉터리로 제한할 수 있습니다. 자세한 내용은 [읽기/쓰기 액세스 정책의 예](#)를 참조하세요.

5. 정책 검토를 선택하고 정책의 이름과 설명을 입력한 다음 정책 생성을 선택합니다.

다음으로 IAM 역할을 생성하고 새 IAM 정책을 연결합니다.

에 대한 IAM 역할을 생성하려면 AWS Transfer Family

1. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.

역할 생성 페이지에서 AWS 서비스가 선택되어 있는지 확인합니다.

2. 서비스 목록에서 전송을 선택하고, 다음: 권한을 선택합니다. 이렇게 하면 AWS Transfer Family 및 간에 신뢰 관계가 설정됩니다 AWS.
3. 권한 정책 연결 섹션에서, 방금 생성한 정책을 찾아 선택한 다음 다음: 태그를 선택합니다.
4. (옵션) 태그의 키와 값을 입력하고 다음: 검토를 선택합니다.
5. 검토 페이지에 새 역할의 명칭과 설명을 입력한 다음 역할 생성을 선택합니다.

다음으로 AWS Transfer Family 및 간에 신뢰 관계를 설정합니다 AWS.

신뢰 관계를 구축하기 위해

Note

이 예에서는 ArnLike 및 ArnEquals 모두를 사용합니다. 기능적으로 동일하므로 정책을 구성할 때 둘 중 하나를 사용할 수 있습니다. Transfer Family 설명서에서는 조건에 와일드 카드 문자가 포함된 경우에는 ArnLike를 사용하고, 정확한 일치 조건을 나타내기 위해서는 ArnEquals를 사용합니다.

1. IAM 콘솔에서 방금 생성한 역할을 선택합니다.
2. 요약 페이지에서 신뢰 관계를 선택한 다음 신뢰 관계 편집을 선택합니다.
3. 신뢰 관계 편집 편집기에서 서비스가 "transfer.amazonaws.com"인지 확인합니다. 액세스 정책은 다음과 같습니다.

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

```

    "Action": "sts:AssumeRole"
  }
]
}

```

대리인 혼동 문제로부터 스스로를 보호하려면 `aws:SourceAccount` 및 `aws:SourceArn` 조건 키를 사용할 것을 권장합니다. 소스 계정은 서버의 소유자이고 소스ARN는 사용자의 ARN입니다. 예:

```

"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"
  }
}

```

사용자 계정의 서버 대신 특정 서버로 제한하려는 경우에도 ArnLike 조건을 사용할 수 있습니다. 예:

```

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

```

Note

위 예제에서 각각을 바꿉니다. *user input placeholder* 자신의 정보를 사용합니다.

햇갈리는 대리인 문제에 대한 자세한 내용 및 기타 예는 [교차 서비스 혼동된 대리인 방지](#) 단원을 참조하세요.

4. 신뢰 정책 업데이트를 선택하여 액세스 정책을 업데이트합니다.

이제 가 사용자를 대신하여 AWS 서비스를 호출 AWS Transfer Family 할 수 있는 IAM 역할을 생성했습니다. 사용자에게 액세스 권한을 부여하기 위해 생성한 IAM 정책을 역할에 연결했습니다. [AWS](#)

[Transfer Family 서버 엔드포인트 시작하기](#) 섹션에서, 이 역할과 정책은 사용자 또는 일반 사용자에게 할당됩니다.

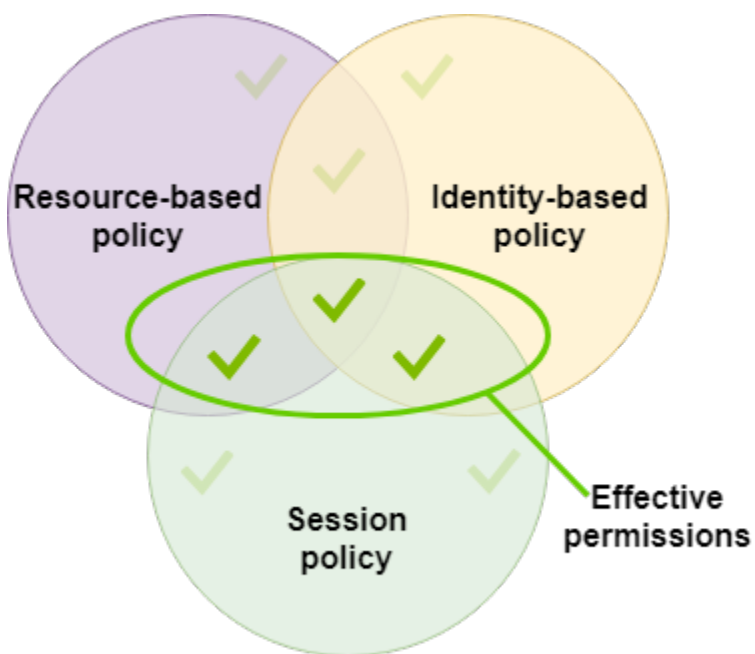
참고 항목

- IAM 역할에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 서비스에 권한을 위임할 역할 생성을 참조하세요](#).
- Amazon S3 리소스의 자격 증명 기반 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Amazon S3의 자격 증명 및 액세스 관리](#)를 참조하세요.
- Amazon EFS 리소스의 자격 증명 기반 정책에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 파일 [시스템 데이터 액세스를 제어하는 IAM 데 사용](#)을 참조하세요.

세션 정책의 작동 방식

관리자가 역할을 생성하면 역할에 여러 사용 사례 또는 팀 구성원을 포괄할 수 있는 광범위한 권한이 포함되는 경우가 많습니다. 관리자가 [콘솔 URL](#)를 구성하는 경우 세션 정책을 사용하여 결과 세션에 대한 권한을 줄일 수 있습니다. 예를 들어 [읽기/쓰기 액세스](#) 권한이 있는 역할을 생성하는 경우 홈 디렉터리에만 대한 사용자의 액세스를 제한URL하는 를 설정할 수 있습니다.

세션 정책은 역할 또는 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 세션 정책은 객체 접두사에 사용자 이름이 포함된 버킷의 일부에만 액세스할 수 있도록 사용자를 잡그는 데 유용합니다. 다음 다이어그램은 세션 정책의 권한이 세션 정책과 리소스 기반 정책의 교집합과 세션 정책 및 자격 증명 기반 정책의 교집합임을 보여줍니다.



자세한 내용은 IAM 사용 설명서의 [세션 정책을](#) 참조하세요.

에서 AWS Transfer Family 세션 정책은 Amazon S3로 또는 Amazon S3에서 전송할 때만 지원됩니다. 다음 예 정책은 사용자가 자신의 home 디렉터리에만 액세스하게 하는 세션 정책입니다. 유의할 사항:

- GetObjectACL 및 PutObjectACL 명령문은 크로스 계정 액세스를 활성화할 필요가 있는 경우에만 요구됩니다. 예컨대, Transfer Family 서버가 다른 계정의 버킷에 액세스할 필요가 있는 경우입니다.
- 세션 정책의 최대 길이는 2,048자입니다. 자세한 내용은 API 참조의 CreateUser 작업에 대한 [정책 요청 파라미터](#)를 참조하세요.
- Amazon S3 버킷이 AWS Key Management Service (AWS KMS)를 사용하여 암호화된 경우 정책에 추가 권한을 지정해야 합니다. 세부 정보는 [Amazon S3의 데이터 암호화](#)를 참조하세요.

```
{
  "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

위의 정책 예에서는 사용자의 홈 디렉터리가 디렉터리임을 나타내기 위해 후행 슬래시를 포함하도록 설정된 것으로 가정합니다. 그 반면에 후행 슬래시가 없이 사용자의 HomeDirectory를 설정하는 경우에는 이를 정책의 일부로 포함해야 합니다.

이전 예 정책에서, transfer:HomeFolder, transfer:HomeBucket, transfer:HomeDirectory 정책 파라미터의 사용을 기억해 두세요. 이러한 파라미터 HomeDirectory는 [HomeDirectory](#) 및 에 설명된 대로 사용자용으로 구성된 에 대해 설정됩니다 [API Gateway 메서드 구현](#). 이러한 파라미터의 정의는 다음과 같습니다.

- transfer:HomeBucket 파라미터는 HomeDirectory의 첫 번째 구성 요소로 대체됩니다.
- transfer:HomeFolder 파라미터가 HomeDirectory 파라미터의 나머지 부분으로 대체됩니다.
- transfer:HomeDirectory 파라미터에는 선행 슬래시(/)가 제거되어 Resource 문에서 S3 Amazon 리소스 이름(ARN)의 일부로 사용할 수 있습니다.

Note

귀하가 논리적 디렉터를 사용하는 경우—즉 사용자의 homeDirectoryType가 LOGICAL인 경우—이러한 정책 파라미터(HomeBucket, HomeDirectory, 및 HomeFolder)는 지원되지 않습니다.

예를 들어, Transfer Family 사용자에 대해 구성된 HomeDirectory 파라미터가 /home/bob/amazon/stuff/(이)라고 가정해 보겠습니다.

- transfer:HomeBucket를 /home(으)로 설정합니다.

- `transfer:HomeFolder`를 `/bob/amazon/stuff/(으)`로 설정합니다.
- `transfer:HomeDirectory`는 `home/bob/amazon/stuff/`가 됩니다.

첫 번째 "Sid"은(는) 사용자가 `/home/bob/amazon/stuff/`부터 시작하여 모든 디렉터리를 나열할 수 있게 해 줍니다.

두 번째 "Sid"은(는) 동일한 경로인 `/home/bob/amazon/stuff/`에 대한 사용자 `put` 및 `get` 액세스를 제한합니다.

읽기/쓰기 액세스 정책의 예

Amazon S3 버킷에 대한 읽기/쓰기 권한 부여

다음 예제 정책은 Amazon S3 버킷의 객체에 대한 읽기/쓰기 액세스 권한을 AWS Transfer Family 부여합니다.

유의할 사항:

- Replace *DOC-EXAMPLE-BUCKET* Amazon S3 버킷의 이름을 사용합니다.
- `GetObjectACL` 및 `PutObjectACL` 명령문은 크로스 계정 액세스를 활성화할 필요가 있는 경우에만 요구됩니다. 예컨대, Transfer Family 서버가 다른 계정의 버킷에 액세스할 필요가 있는 경우입니다.
- `GetObjectVersion` 및 `DeleteObjectVersion` 보고서는 액세스 중인 Amazon S3 버킷에서 버전 관리가 활성화된 경우에만 필요합니다.

Note

버킷에 대한 버전 관리를 활성화한 경우 Amazon S3에서만 버전 관리를 일시 중지하고 완전히 끌 수 없으므로 이러한 권한이 필요합니다. 자세한 내용은 [Unversioned, versioning-enabled 및 versioning-suspended 버킷을 참조하세요](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
```

```

        "s3:GetBucketLocation"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
}
]
}

```

Amazon 파일 시스템의 파일에 대한 EFS 파일 시스템 액세스 권한 부여

Note

정책 외에도 POSIX 파일 권한이 적절한 액세스 권한을 부여하고 있는지도 확인해야 합니다. 자세한 내용은 Amazon Elastic File System [File System 사용 설명서의 네트워크 파일 시스템 \(NFS\) 수준에서 사용자, 그룹 및 권한 작업을](#) 참조하세요.

다음 예제 정책은 루트 파일 시스템에 Amazon EFS 파일 시스템의 파일에 대한 액세스 권한을 부여합니다.

Note

다음 예에서는 `region` 리전과 함께 `account-id` 파일이 있는 계정 `file-system-id` Amazon Elastic File System(Amazon EFS)의 ID를 사용합니다.

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

다음 예제 정책은 사용자 파일 시스템에 Amazon EFS 파일 시스템의 파일에 대한 액세스 권한을 부여합니다.

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

Transfer Family 자습서

AWS Transfer Family 사용 설명서는 여러 사용 사례에 대한 자세한 설명을 제공합니다.

- [AWS Transfer Family 서버 엔드포인트 시작하기](#): 이 자습서에서는 SFTP Transfer Family 서버 및 서비스 관리형 사용자를 생성하는 방법을 안내한 다음 클라이언트를 사용하여 파일을 전송하는 방법을 보여줍니다.
- [SFTP 커넥터 설정 및 사용](#): 이 자습서에서는 SFTP 커넥터를 설정한 다음 Amazon S3 스토리지와 SFTP 서버 간에 파일을 전송하는 방법을 보여줍니다.
- [Amazon API Gateway 메서드를 사용자 지정 자격 증명 공급자로 설정](#): 이 자습서에서는 Amazon API Gateway 메서드를 설정하고 사용자 지정 자격 증명 공급자로 사용하여 AWS Transfer Family 서버에 파일을 업로드하는 방법을 보여줍니다.
- [파일 복호화를 위한 관리형 워크플로 설정](#): 이 자습서에서는 복호화 단계가 포함된 관리형 워크플로를 설정하는 방법과 암호화된 파일을 Amazon S3 버킷에 업로드한 다음 복호화된 파일을 보는 방법을 설명합니다.
- [AS2 구성 설정](#): 이 자습서에서는 AS2 Transfer Family 서버를 구성하는 데 필요한 단계를 안내합니다. 인증서 가져오기, 프로필 및 계약 생성, 선택적으로 AS2 커넥터 생성, 구성 테스트에 대한 지침이 있습니다.

주제

- [AWS Transfer Family 서버 엔드포인트 시작하기](#)
- [파일 복호화를 위한 관리형 워크플로 설정](#)
- [SFTP 커넥터 설정 및 사용](#)
- [Amazon API Gateway 메서드를 사용자 지정 자격 증명 공급자로 설정](#)
- [AS2 구성 설정](#)

AWS Transfer Family 서버 엔드포인트 시작하기

이 자습서를 사용하여 AWS Transfer Family (Transfer Family)를 시작합니다. Amazon S3 스토리지를 사용하여 공개적으로 액세스할 수 있는 엔드포인트가 있는 SFTP지원 서버를 생성하고, 서비스 관리형 인증을 사용하여 사용자를 추가하고, Cyberduck을 사용하여 파일을 전송하는 방법을 알아봅니다.

주제

- [사전 조건](#)
- [1단계: AWS Transfer Family 콘솔에 로그인](#)
- [2단계: SFTP활성화된 서버 생성](#)
- [3단계: 서비스 관리 사용자 추가](#)
- [4단계: 클라이언트를 사용하여 파일 전송](#)

사전 조건

시작하기 전에 먼저 [사전 조건](#) 요건을 충족해야 합니다. 이 설정의 일부로 Amazon Simple Storage Service(Amazon S3) 버킷과 AWS Identity and Access Management (IAM) 사용자 역할을 생성합니다.

AWS Transfer Family 콘솔을 사용하려면 권한이 필요하며, Amazon Simple Storage Service, Amazon Elastic File System, AWS Certificate Manager, Amazon Route 53과 같이 Transfer Family가 사용하는 다른 AWS 서비스를 구성하는 데 필요한 권한이 있습니다. 예를 들어 Transfer Family를 AWS 사용하여 파일을 로 또는 밖으로 전송하는 사용자의 경우 AmazonS3FullAccess는 Amazon S3 버킷을 설정하고 사용할 수 있는 권한을 부여합니다. Amazon S3 버킷을 생성하려면 이 정책의 일부 권한이 필요합니다.

Transfer Family 콘솔을 사용하려면 다음이 필요합니다.

- AWSTransferConsoleFullAccess 는 SFTP 사용자가 Transfer Family 리소스를 생성할 수 있는 권한을 부여합니다.
- IAMFullAccess (또는 특히 IAM 역할 생성을 허용하는 정책)은 Transfer Family가 Amazon CloudWatch Logs에서 서버의 로깅 역할 또는 서버에 로그인하는 사용자의 사용자 역할을 자동으로 생성하도록 하려는 경우에만 필요합니다.
- VPC 서버 유형을 생성하고 삭제하려면 ec2:CreateVpcEndpoint 및 ec2:DeleteVpcEndpoints 작업을 정책에 추가해야 합니다.

Note

AmazonS3FullAccess 및 IAMFullAccess 정책 자체는 의 일반적인 사용에 필요하지 않습니다 AWS Transfer Family. 여기에는 필요한 모든 권한이 포함되는지 확인할 수 있는 간단한 방법이 나와 있습니다. 또한 모든 AWS 고객이 사용할 수 있는 표준 정책인 AWS 관리형 정책입니다. 이러한 정책의 개별 권한을 보고 목적에 필요한 최소 권한을 결정할 수 있습니다.

1단계: AWS Transfer Family 콘솔에 로그인

Transfer Family에 로그인하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 계정 ID 또는 별칭에 AWS 계정사용자 ID를 입력합니다.
3. IAM 사용자 이름 에 Transfer Family에 대해 생성한 사용자 역할의 이름을 입력합니다.
4. 암호 에 AWS 계정 암호를 입력합니다.
5. 로그인을 선택합니다.

2단계: SFTP활성화된 서버 생성

Secure Shell (SSH) 파일 전송 프로토콜(SFTP)은 인터넷을 통한 데이터 보안 전송에 사용되는 네트워크 프로토콜입니다. 프로토콜은 의 전체 보안 및 인증 기능을 지원합니다SSH. 금융 서비스, 의료, 소매 및 광고와 같은 다양한 산업의 사업 파트너 간의 민감한 정보를 비롯한 데이터를 교환하는 데 널리 사용됩니다.

SFTP활성화 서버를 생성하려면

1. 탐색 창에서 서버를 선택한 다음 서버 생성을 선택합니다.
2. 프로토콜 선택 에서 SFTP를 선택한 다음 다음 를 선택합니다.
3. 자격 증명 제공자 선택에서 Transfer Family에 사용자 ID 및 키를 저장하도록 관리 서비스를 선택한 후 다음을 선택합니다.
4. 엔드포인트 선택에서 다음을 수행합니다.
 - a. 엔드포인트 타입으로는 공적으로 액세스 가능 엔드포인트 타입을 선택합니다.
 - b. 사용자 지정 호스트 이름의 경우 없음을 선택합니다.
 - c. 다음을 선택합니다.
5. 도메인 선택에서 Amazon S3를 선택합니다.
6. 추가 상세 정보 구성에서 다음을 수행합니다.
 - a. CloudWatch 로깅의 경우 새 역할을 생성할 수 있는 적절한 권한이 있는 한 Transfer Family가 IAM 자동으로 역할을 생성하도록 허용하려면 새 역할 생성을 선택합니다. 생성된 IAM 역할을 라고 합니다AWSTransferLoggingAccess.

- b. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다. 기본 보안 정책은 TransferSecurityPolicy-2020-06입니다.
 - c. Next(다음)를 선택합니다.
7. 검토 및 생성에서 서버 생성을 선택합니다. 서버 페이지로 이동합니다.

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때 서버에서 파일 작업을 수행할 수 있지만 먼저 사용자를 만들어야 합니다.

3단계: 서비스 관리 사용자 추가

SFTP활성화된 서버에 사용자를 추가하려면

1. 서버 페이지에서 사용자를 추가할 서버의 확인란을 선택합니다.
2. 사용자 추가를 선택합니다.
3. 사용자 구성 섹션의 사용자 이름에 사용자 이름을 입력합니다. 이 사용자 이름은 3~100자여야 합니다. 사용자 이름에는 a~z, A~Z, 0~9, 밑줄(_)와 하이픈(-), 마침표(.) 및 골뱅이 기호(@) 등의 문자를 사용할 수 있습니다. 사용자 이름은 하이픈, 마침표 및 @ 기호로 시작할 수 없습니다.
4. 액세스 에서 Amazon S3 버킷에 대한 액세스를 제공하는 이전에 생성한 IAM 역할을 선택합니다.

의 절차를 사용하여 이 IAM 역할을 생성했습니다 [IAM 역할 및 정책 생성](#). 이 IAM 역할에는 Amazon S3 버킷에 대한 액세스를 제공하는 IAM 정책이 포함됩니다. 또한 다른 IAM 정책에 정의된 AWS Transfer Family 서비스와의 신뢰 관계도 포함됩니다.

Note

서비스 관리형 사용자의 IAM 역할에는 원하는 버킷에 액세스할 수 있는 권한이 포함되어야 합니다. 원하는 버킷에 액세스할 수 있는 권한은 S3FullAccess 리소스에 대한 관리자 수준 권한을 부여하는 S3에서 다룹니다.

5. 정책에서 없음을 선택합니다.
6. 홈 디렉터리 에서 Amazon S3 버킷을 선택하여 를 사용하여 전송할 데이터를 저장합니다 AWS Transfer Family. 사용자가 클라이언트를 이용해 로그인하면 도착하게 되는 home 디렉터리의 경로를 입력합니다.

이 파라미터를 입력하지 않으면 Amazon S3 버킷의 root 디렉터리가 사용됩니다. 이 경우 IAM 역할이 이 root 디렉터리에 대한 액세스 권한을 제공하는지 확인하세요.

Note

사용자의 사용자 이름을 포함하는 디렉터리 경로 선택을 권장합니다. 이 경로를 통해 세션 정책을 효과적으로 사용할 수 있습니다. 세션 정책은 사용자의 home 디렉터리에 대한 Amazon S3 버킷에서의 사용자 액세스를 제한합니다.

- 제한됨에서 사용자가 해당 폴더 외부에 액세스할 수 없고 Amazon S3 버킷 또는 폴더 이름을 볼 수 없도록 확인란을 선택합니다.

Note

사용자에게 홈 디렉터리를 할당하고 해당 홈 디렉터리로 사용자를 제한하는 경우 이 정도면 지정된 폴더에 대한 사용자 액세스를 잠그기에 충분합니다. 추가 통제를 적용해야 하는 경우 세션 정책을 사용하세요.

- SSH 퍼블릭 키의 경우 SSH 키 페어의 퍼블릭 SSH 키 부분을 입력합니다.

서비스에서 사용자의 키를 확인해야 새 사용자를 추가할 수 있습니다.

Important

SSH 퍼블릭 키의 형식은 `ssh-rsa <string>`. SSH 키 페어를 생성하는 방법에 대한 지침은 섹션을 참조하세요 [서비스 관리 사용자를 위한 SSH 키 생성](#).

- (옵션) 키와 값에 하나 이상의 태그를 키-값 쌍로 입력하고 태그 추가를 선택합니다.
- 추가를 선택해 새 사용자를 원하는 서버에 추가합니다.

새 사용자는 서버 세부 정보 페이지의 사용자 섹션에 나타납니다.

4단계: 클라이언트를 사용하여 파일 전송

클라이언트에서 전송 작업을 지정하여 AWS Transfer Family 서비스를 통해 파일을 전송합니다. 는 여러 클라이언트를 AWS Transfer Family 지원합니다. 자세한 내용은 [클라이언트를 사용하여 서버 엔드 포인트를 통한 파일 전송](#)을 참조하세요.

이 섹션에는 Cyberduck 및 열기 를 사용하는 절차가 포함되어 있습니다SSH.

주제

- [Cyberduck 사용하기](#)
- [열기 사용SSH](#)

Cyberduck 사용하기

Cyberduck을 AWS Transfer Family 사용하여 파일을 전송하려면

1. [Cyberduck](#) 클라이언트를 엽니다.
2. 연결 열기를 선택합니다.
3. 연결 열기 대화 상자에서 SFTP (SSH 파일 전송 프로토콜)을 선택합니다.
4. 서버에 서버 엔드포인트를 입력합니다. 서버 엔드포인트는 서버 세부 정보 페이지에 있습니다. [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#)를 참조하세요.
5. 포트 번호에 **22**를 입력합니다. SFTP.
6. 사용자 이름에 [서버 엔드포인트에 대한 사용자 관리](#)에서 생성한 사용자 이름을 입력합니다.
7. SSH 프라이빗 키에서 SSH 프라이빗 키를 선택하거나 입력합니다.
8. 연결을 선택합니다.
9. 파일 전송을 실행합니다.

파일 위치에 따라, 다음 중 하나를 수행하세요.

- 로컬 디렉터리(소스)에서 전송할 파일을 선택하고, Amazon S3 디렉터리(대상)로 끌어다 놓습니다.
- Amazon S3 디렉터리(소스)에서 전송할 파일을 선택하고, 로컬 디렉터리(대상)로 끌어다 놓습니다.

열기 사용SSH

다음 지침에 따라 열기 를 사용하여 명령줄에서 파일을 전송합니다. SSH.

Note

이 클라이언트는 SFTP 활성화된 서버에서만 작동합니다.

OpenSSH 명령줄 유틸리티를 AWS Transfer Family 사용하여 파일을 전송하려면

1. Linux나 Macintosh에서 명령 터미널을 엽니다.
2. 프롬프트에서 다음 명령을 입력합니다. `% sftp -i transfer-key sftp_user@service_endpoint`

앞의 명령에서 `sftp_user` 는 사용자 이름이고 `transfer-key`는 SSH 프라이빗 키입니다. 여기서 `service_endpoint`는 선택한 서버의 AWS Transfer Family 콘솔에 표시된 서버의 엔드포인트입니다.

`sftp` 프롬프트가 나타날 것입니다.

3. (옵션) 사용자의 홈 디렉터리를 보려면 `sftp` 프롬프트에 다음 명령을 입력합니다. `sftp> pwd`
4. 다음 줄에 다음 텍스트를 입력합니다. `sftp> cd /mybucket/home/sftp_user`

본 시작하기 실습에서는 이 Amazon S3 버킷이 파일 전송 대상입니다.

5. 다음 줄에 다음 명령을 입력합니다. `sftp> put filename.txt`

`put` 명령은 파일을 Amazon S3 버킷으로 전송합니다.

파일 전송이 진행 중이거나 완료되었음을 나타내는, 다음과 비슷한 메시지가 표시됩니다.

```
Uploading filename.txt to /my-bucket/home/sftp_user/filename.txt
```

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

파일 복호화를 위한 관리형 워크플로 설정

이 자습서에서는 복호화 단계가 포함된 관리형 워크플로를 설정하는 방법을 설명합니다. 또한 자습서에서는 Amazon S3 버킷에 암호화된 파일을 업로드한 다음 동일한 버킷에서 복호화된 파일을 보는 방법을 보여줍니다.

Note

AWS 스토리지 블로그에는 [PGP 및 를 사용하여 파일을 암호화 및 복호화하고 파일을 암호화 및 복호화 AWS Transfer Family](#)하는 방법을 설명하는 게시물이 있습니다.

주제

- [1단계: 실행 역할 구성](#)
- [2단계: 관리형 워크플로 생성](#)
- [3단계: 서버에 워크플로 추가 및 사용자 생성](#)
- [4단계: PGP 키 페어 생성](#)
- [5단계: 예 PGP 프라이빗 키 저장 AWS Secrets Manager](#)
- [6단계: 파일 암호화](#)
- [7단계: 워크플로 실행 및 결과 보기](#)

1단계: 실행 역할 구성

Transfer Family가 워크플로를 시작하는 데 사용할 수 있는 AWS Identity and Access Management (IAM) 실행 역할을 생성합니다. 실행 역할을 생성하는 프로세스는 [IAM 워크플로 정책](#)에 설명되어 있습니다.

Note

[신뢰 관계를 구축하기 위해](#)에 설명된 대로 실행 역할을 생성하는 과정에서 실행 역할과 Transfer Family 사이에 신뢰 관계를 확실히 구축해야 합니다.

다음 실행 역할 정책에는 이 자습서에서 만들 워크플로를 성공적으로 실행하는 데 필요한 모든 권한이 포함되어 있습니다. 이 정책 예를 사용하려면 *user input placeholders*를 실제 정보로 바꾸세요. *DOC-EXAMPLE-BUCKET*을 암호화된 파일을 업로드할 Amazon S3 버킷 이름으로 바꿉니다.

Note

모든 워크플로에 이 예에 나열된 모든 권한이 필요한 것은 아닙니다. 특정 워크플로의 단계 타입에 따라 권한을 제한할 수 있습니다. 사전 정의된 각 단계 타입에 필요한 권한은 [사전 정의된 단계 사용](#)에 설명되어 있습니다. 사용자 지정 단계에 필요한 권한은 [IAM 사용자 지정 단계에 대한 권한](#)에 설명되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "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:::DOC-EXAMPLE-BUCKET/*",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"]
    "Condition": {
        "StringEquals": {
            "s3:RequestObjectTag/Archive": "yes"
        }
    }
},
{
    "Sid": "DecryptSecret",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"
    }
]
}

```

2단계: 관리형 워크플로 생성

이제 복호화 단계가 포함된 워크플로를 만들어야 합니다.

복호화 단계가 포함된 워크플로를 만들려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 워크플로를 선택한 다음, 워크플로 생성을 선택합니다.
3. 다음 세부 정보를 입력합니다.

- 설명을 입력합니다. 예를 들어, **Decrypt workflow example**.
 - 공칭 단계 섹션에서 단계 추가를 선택합니다.
4. 단계 타입 선택에서 파일 복호화를 선택한 후 다음을 선택합니다.
 5. 파라미터 구성 대화 상자에서 다음 사항을 지정합니다.
 - 설명이 포함된 단계 이름을 입력합니다. 예: **decrypt-step**. 단계 이름에는 공백은 허용되지 않습니다.
 - 복호화된 파일의 대상으로 Amazon S3을 선택합니다.
 - 대상 버킷 이름 에서 1단계에서 생성한 IAM 정책 **DOC-EXAMPLE-BUCKET**에서 로 지정한 것과 동일한 Amazon S3 버킷을 선택합니다.
 - 대상 키 접두사에는 대상 버킷에 복호화된 파일을 저장할 접두사(폴더)의 이름을 입력합니다. 예: **decrypted-files/**.

 Note

접두사에는 반드시 후행 슬래시(/)를 추가해야 합니다.

- 이 자습서에서는 기존 항목 덮어쓰기를 선택 해제해 두세요. 이 설정을 지우면 기존 파일과 이름이 같은 파일을 해독하려고 하면 워크플로 처리가 중지되고 새 파일은 처리되지 않습니다.

다음을 선택하여 검토 화면으로 이동합니다.

6. 해당 단계의 세부 정보를 검토합니다. 모든 내용이 정확하면 단계 생성을 선택합니다.
7. 워크플로에는 단일 복호화 단계만 필요하므로 추가로 구성할 단계가 없습니다. 워크플로 생성을 선택하여 새 워크플로를 생성합니다.

새 워크플로의 워크플로 ID를 기록해 둡니다. 다음 단계에서 이 ID가 필요합니다. 이 자습서에서는 **w-1234abcd5678efghi** 를 예제 워크플로 ID로 지정합니다.

3단계: 서버에 워크플로 추가 및 사용자 생성

이제 복호화 단계가 포함된 워크플로를 Transfer Family 서버에 연결해야 합니다. 이 자습서에서는 기존 Transfer Family 서버에 워크플로를 연결하는 방법을 보여줍니다. 또는 워크플로에 사용할 새 서버를 만들 수 있습니다.

워크플로를 서버에 연결한 후 서버에 할 수 있는 사용자를 생성하고 워크플로를 실행하도록 SFTP 트리거해야 합니다.

워크플로를 실행하도록 Transfer Family 서버를 구성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택한 다음 목록에서 서버 하나를 선택합니다. 이 서버가 SFTP 프로토콜을 지원하는지 확인합니다.
3. 서버의 세부 정보 페이지에서 추가 세부 정보 섹션까지 아래로 스크롤한 다음 편집을 선택합니다.
4. 추가 세부 정보 편집 페이지의 관리형 워크플로 섹션에서 워크플로를 선택하고 해당하는 실행 역할을 선택합니다.
 - 전체 파일 업로드를 위한 워크플로의 경우 [2단계: 관리형 워크플로 생성](#)에서 만든 워크플로를 선택합니다. 예: **w-1234abcd5678efghi**.
 - 관리형 워크플로 실행 역할 에서 에서 생성한 IAM 역할을 선택합니다 [1단계: 실행 역할 구성](#).
5. 페이지 맨 아래로 스크롤하고 저장을 선택하여 변경 내용을 저장합니다.

사용 중인 서버의 ID를 기록해 둡니다. PGP 키를 저장하는 데 사용하는 AWS Secrets Manager 보안 암호의 이름은 부분적으로 서버 ID를 기반으로 합니다.

워크플로를 트리거할 수 있는 사용자를 추가하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택한 다음 복호화 워크플로에 사용할 서버를 선택합니다.
3. 서버 세부 정보 페이지에서 사용자 섹션으로 스크롤하여 사용자 추가를 선택합니다.
4. 새 사용자의 경우 다음 세부 정보를 입력합니다.
 - 사용자 이름에 **decrypt-user**를 입력합니다.
 - 역할에서 서버에 액세스할 수 있는 사용자 역할을 선택합니다.
 - 홈 디렉터리의 경우 이전에 사용한 Amazon S3 버킷을 선택합니다. 예: **DOC-EXAMPLE-BUCKET**.
 - SSH 퍼블릭 키의 경우 보유한 프라이빗 키에 해당하는 퍼블릭 키에 붙여넣습니다. 세부 정보는 [서비스 관리 사용자를 위한 SSH 키 생성](#)을 참조하세요.
5. 추가를 선택하여 새 사용자를 저장합니다.

이 서버의 Transfer Family 사용자 이름을 기록해 둡니다. 암호는 부분적으로 사용자 이름을 기반으로 합니다. 단순화를 위해 이 자습서에서는 서버의 모든 사용자가 사용할 수 있는 기본 암호를 사용합니다.

4단계: PGP 키 페어 생성

[지원되는 PGP 클라이언트](#) 중 하나를 사용하여 PGP 키 페어를 생성합니다. 이 과정은 [PGP 키 생성](#)에 자세히 설명되어 있습니다.

PGP 키 페어를 생성하려면

1. 이 자습서에서는 gpg (GnuPG) 버전 2.0.22 클라이언트를 사용하여 를 암호화 알고리즘RSA으로 사용하는 PGP 키 페어를 생성할 수 있습니다. 이 클라이언트의 경우 다음 명령을 실행하고 이메일 주소와 암호를 입력합니다. 원하는 이름이나 이메일 주소를 사용할 수 있습니다. 자습서 뒷부분에서 값을 입력해야 하므로 사용하는 값을 기억해 두세요.

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

Note

GnuPG 버전 2.3.0 이상을 사용하는 경우 gpg --full-gen-key를 실행해야 합니다. 생성할 키 유형에 대한 메시지가 표시되면 RSA 또는 를 선택합니다ECC. 그러나 를 선택하는 경우 ECC다음 중 하나를 선택해야 합니다.NIST 또는 BrainPool 타원 곡선의 경우. 선택 안 함 Curve 25519.

2. 다음 명령을 실행하여 프라이빗 키를 내보냅니다. *user@example.com*을 키를 생성할 때 사용한 이메일 주소로 바꿉니다.

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

이 명령은 프라이빗 키를 **workflow-tutorial-key.pgp** 파일로 내보냅니다. 출력 파일의 이름을 원하는 대로 지정할 수 있습니다. 프라이빗 키를 AWS Secrets Manager에 추가한 후 프라이빗 키 파일을 삭제할 수도 있습니다.

5단계: 에 PGP 프라이빗 키 저장 AWS Secrets Manager

매우 구체적인 방식으로 Secrets Manager에 프라이빗 키를 저장해야 워크플로가 업로드된 파일에 대한 복호화 단계를 실행할 때 워크플로가 프라이빗 키를 찾을 수 있습니다.

Note

Secrets Manager에 암호를 저장하면 에 요금이 AWS 계정 발생합니다. 요금에 대한 자세한 내용은 [AWS Secrets Manager 요금](#)을 참조하세요.

Secrets Manager에 PGP 프라이빗 키를 저장하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Secrets Manager 콘솔을 엽니다 <https://console.aws.amazon.com/secretsmanager/>.
2. 왼쪽 탐색 창에서 암호를 선택합니다.
3. 암호 페이지에서 새 암호 저장을 선택합니다.
4. 암호 선택 페이지의 암호 타입에서 다른 타입의 암호를 선택합니다.
5. 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 — **PGPPrivateKey**를 입력합니다.
 - 값 — 프라이빗 키의 텍스트를 값 필드에 붙여넣습니다.
6. 행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 - **PGPPassphrase**를 입력합니다.
 - 값 - 에서 PGP 키 페어를 생성할 때 사용한 암호를 입력합니다 [4단계: PGP 키 페어 생성](#).
7. Next(다음)를 선택합니다.
8. 암호 구성 페이지에 암호를 위한 명칭과 설명을 입력합니다. 이 자습서에서는 모든 사용자가 사용할 수 있는 기본 암호를 만들 수 있습니다. 서버 ID가 **s-11112222333344445**에서 보안 암호의 이름을 지정합니다 **aws/transfer/s-11112222333344445/@pgp-default**. **s-11112222333344445**을 Transfer Family 서버의 ID로 바꿉니다. 암호에 대한 설명을 입력합니다.

Note

이전에 생성한 사용자에게 암호만 생성하려면 암호 이름을 **aws/transfer/s-11112222333344445/decrypt-user**로 지정합니다.

9. 다음을 선택한 후 교체 구성 페이지의 기본값을 그대로 사용합니다. 그 다음 다음을 선택합니다.
10. 검토 페이지에서 저장을 선택하여 암호를 만들고 저장합니다.

Secrets Manager에 PGP 프라이빗 키를 추가하는 방법에 대한 자세한 내용은 [PGP 키 저장 AWS Secrets Manager 에 사용을 참조하세요](#).

6단계: 파일 암호화

gpg 프로그램을 사용하여 워크플로에 사용할 파일을 암호화합니다. 파일을 암호화하려면 다음 명령을 실행합니다.

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

이 자동화를 실행하기 전에 다음 사항에 유의하세요.

- -r 인수의 경우 PGP 키 페어 *marymajor@example.com*를 생성할 때 사용한 이메일 주소로 를 바꿉니다.
- --openpgp 플래그는 옵션입니다. 이 플래그는 암호화된 파일이 [OpenPGP RFC4880](#) 표준을 준수하도록 합니다.
- 이 명령은 **testfile.txt**와 같은 위치에 이름이 **testfile.txt.gpg**라고 지정된 파일을 만듭니다.

7단계: 워크플로 실행 및 결과 보기

워크플로를 실행하려면 3단계에서 만든 사용자를 사용하여 Transfer Family 서버에 연결합니다. 그런 다음 [2.5단계에서 지정한 Amazon S3 버킷을 살펴보고 복호화된 파일을 볼 수 있도록 대상 파라미터를 구성](#)할 수 있습니다.

복호화 워크플로를 실행하려면

1. 명령 터미널을 엽니다.
2. 다음 명령을 실행하여 *your-endpoint*를 실제 엔드포인트 및 사용자의 SSH 프라이빗 키 *transfer-key*로 바꿉니다.

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

예를 들어 프라이빗 키가 ~/.ssh/decrypt-user에 저장되어 있고 엔드포인트가 s-11112222333344445.server.transfer.us-east-2.amazonaws.com인 경우, 명령은 다음과 같습니다.

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

3. `pwd` 명령을 실행합니다. 이 명령이 제대로 실행되면 다음과 같은 응답을 반환합니다.

```
Remote working directory: /DOC-EXAMPLE-BUCKET/decrypt-user
```

디렉터리에는 Amazon S3 버킷 이름이 반영됩니다.

4. 다음 명령을 실행하여 파일을 업로드하고 워크플로를 실행하도록 트리거합니다.

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

5. 복호화된 파일의 대상 폴더는 워크플로를 만들 때 지정한 `decrypted-files/` 폴더입니다. 이제 해당 폴더로 이동하여 내용을 나열할 수 있습니다.

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

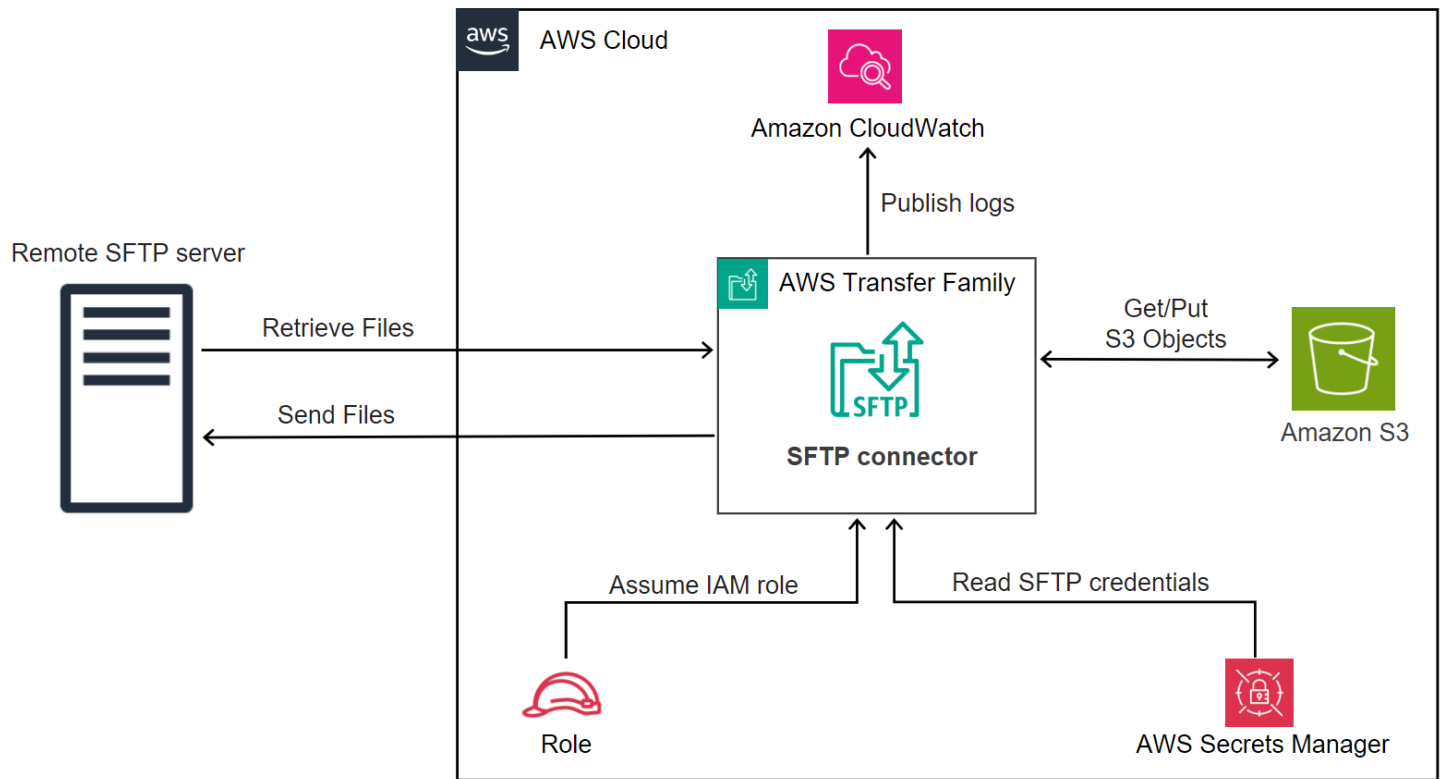
성공하면 `ls` 명령이 `testfile.txt` 파일을 나열합니다. 이 파일을 다운로드하여 이전에 암호화한 원본 파일과 동일한지 확인할 수 있습니다.

SFTP 커넥터 설정 및 사용

커넥터의 목적은 AWS 스토리지와 파트너의 SFTP 서버 간의 관계를 설정하는 것입니다. Amazon S3에서 파트너 소유의 외부 대상으로 파일을 보낼 수 있습니다. SFTP 커넥터를 사용하여 파트너의 SFTP 서버에서 파일을 검색할 수도 있습니다.

이 자습서에서는 SFTP 커넥터를 설정한 다음 Amazon S3 스토리지와 SFTP 서버 간에 파일을 전송하는 방법을 보여줍니다.

SFTP 커넥터는 에서 SFTP 보안 인증을 검색 AWS Secrets Manager 하여 원격 SFTP 서버에 인증하고 연결을 설정합니다. 커넥터는 원격 서버로 파일을 보내거나 원격 서버에서 파일을 검색하고 Amazon S3에 파일을 저장합니다. IAM 역할은 Amazon S3 버킷 및 Secrets Manager에 저장된 보안 인증 정보에 대한 액세스를 허용하는 데 사용됩니다. Amazon 에 로그인할 수도 있습니다 CloudWatch.



주제

- [1단계: 필요한 지원 리소스 생성](#)
- [2단계: SFTP 커넥터 생성 및 테스트](#)
- [3단계: SFTP 커넥터를 사용하여 파일 전송 및 검색](#)
- [원격 서버로 사용할 Transfer Family SFTP 서버를 생성하는 절차](#)

1단계: 필요한 지원 리소스 생성

SFTP 커넥터를 사용하여 Amazon S3와 원격 SFTP 서버 간에 파일을 복사할 수 있습니다. 이 자습서에서는 AWS Transfer Family 서버를 원격 SFTP 서버로 사용하고 있습니다. 다음 리소스를 생성하고 구성해야 합니다.

- Amazon S3 버킷을 생성하여 AWS 환경에 파일을 저장하고 원격 SFTP 서버에서 파일을 전송하고 검색합니다. [Amazon S3 버킷 생성](#).
- Secrets Manager에서 Amazon S3 스토리지 및 보안 암호에 액세스하기 위한 AWS Identity and Access Management 역할을 생성합니다. [필요한 권한을 가진 IAM 역할 생성](#).
- SFTP 프로토콜을 사용하는 Transfer Family 서버와 SFTP 커넥터를 사용하여 SFTP 서버 간에 파일을 전송하는 서비스 관리형 사용자를 생성합니다. [Transfer Family SFTP 서버 및 사용자 생성](#).

- SFTP 커넥터에서 원격 SFTP 서버에 로그인하는 데 사용하는 보안 인증 정보를 저장하는 AWS Secrets Manager 보안 암호를 생성합니다 [에서 보안 암호 생성 및 저장 AWS Secrets Manager](#).

Amazon S3 버킷 생성

Amazon S3 버킷을 생성하려면

1. 에서 AWS Transfer Family 콘솔에 로그인합니다 <https://console.aws.amazon.com/s3/>.
2. 리전을 선택하고 이름을 입력합니다.

이 자습서의 경우 버킷은 **에 US East (N. Virginia) us-east-1** 있고 이름은 **입니다 sftp-server-storage-east**.

3. 기본값을 수락하고 버킷 생성을 선택합니다.

Amazon S3 버킷 생성에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [S3 버킷을 생성하려면 어떻게 해야 할까요?](#)를 참조하세요.

필요한 권한을 가진 IAM 역할 생성

액세스 역할의 경우 다음 권한이 있는 정책을 생성합니다.

다음 예제에서는 에 액세스하는 데 필요한 권한을 부여합니다. **DOC-EXAMPLE-BUCKET** Amazon S3의 와 Secrets Manager에 저장된 지정된 보안 암호입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
```

```

    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters"
}
]
}

```

다음과 같이 항목을 바꿉니다.

- 에 대해 *DOC-EXAMPLE-BUCKET*, 자습서에서는 를 사용합니다 **s3-storage-east**.
- 에 대해 *region*, 자습서에서는 를 사용합니다 **us-east-1**.
- 에 대해 *account-id*에서 ID를 AWS 계정 사용합니다.
- 에 대해 *SecretName-6RandomCharacters*, 이름은 **using sftp-connector1**입니다(비밀에 6개의 무작위 문자가 있음).

또한 이 역할에 사용자의 전송 요청을 처리할 때 커넥터가 리소스에 액세스할 수 있는 신뢰 관계가 포함되어 있는지 확인해야 합니다. 신뢰 관계 설정에 대한 자세한 내용은 [신뢰 관계를 구축하기 위해](#)을 참조하세요.

Note

자습서에서 사용 중인 역할에 대한 세부 정보는 섹션을 참조하세요 [결합된 사용자 및 액세스 역할](#).

에서 보안 암호 생성 및 저장 AWS Secrets Manager

SFTP 커넥터의 사용자 보안 인증을 저장하려면 Secrets Manager에 보안 암호를 저장해야 합니다. 암호, SSH 프라이빗 키 또는 둘 다를 사용할 수 있습니다. 자습서에서는 프라이빗 키를 사용합니다.

Note

Secrets Manager에 암호를 저장하면 에 요금이 AWS 계정 발생합니다. 요금에 대한 자세한 내용은 [AWS Secrets Manager 요금](#)을 참조하세요.

보안 암호를 저장하는 절차를 시작하기 전에 프라이빗 키를 검색하고 형식을 지정합니다. 프라이빗 키는 원격 SFTP 서버의 사용자에게 대해 구성된 퍼블릭 키와 일치해야 합니다. 자습서의 경우 프라이빗 키는 원격 서버로 사용 중인 Transfer Family SFTP 서버에 테스트 사용자를 위해 저장된 퍼블릭 키와 일치해야 합니다.

이렇게 하려면 다음 명령을 실행합니다.

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

예를 들어 프라이빗 키 파일이 에 있는 경우 ~/.ssh/sftp-testuser-privatekey 명령은 다음과 같습니다.

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

이렇게 하면 키를 올바른 형식(새 줄 문자가 포함된)으로 표준 출력으로 출력합니다. 다음 절차(6단계)에 붙여넣어야 하므로 이 텍스트를 어딘가에 복사합니다.

SFTP 커넥터의 Secrets Manager에 사용자 자격 증명을 저장하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Secrets Manager 콘솔을 엽니다 <https://console.aws.amazon.com/secretsmanager/>.
2. 왼쪽 탐색 창에서 암호를 선택합니다.

3. 암호 페이지에서 새 암호 저장을 선택합니다.
4. 암호 선택 페이지의 암호 타입에서 다른 타입의 암호를 선택합니다.
5. 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 - **Username**를 입력합니다.
 - 값 - 사용자 이름인 **sftp-testuser**를 입력합니다.
6. 키를 입력하려면 일반 텍스트 탭을 사용하는 것이 좋습니다.
 - a. 행 추가를 선택한 다음 **PrivateKey**를 입력합니다.
 - b. 일반 텍스트 탭을 선택합니다. 필드에는 이제 다음 텍스트가 포함됩니다.

```
{"Username":"sftp-testuser","PrivateKey":""}
```

- c. 프라이빗 키(이전에 저장됨)의 텍스트를 빈 큰따옴표(“) 사이에 붙여 넣습니다.

화면은 다음과 같아야 합니다(키 데이터는 회색으로 표시됨).



7. Next(다음)를 선택합니다.
8. 보안 암호 구성 페이지에서 보안 암호의 이름을 입력합니다. 이 자습서에서는 보안 암호의 이름을 지정합니다 **aws/transfer/sftp-connector1**.
9. 다음을 선택한 후 교체 구성 페이지의 기본값을 그대로 사용합니다. 그 다음 다음을 선택합니다.
10. 검토 페이지에서 저장을 선택하여 암호를 만들고 저장합니다.

2단계: SFTP 커넥터 생성 및 테스트

이 섹션에서는 이전에 생성한 모든 리소스를 사용하는 SFTP 커넥터를 생성합니다. 자세한 내용은 [SFTP 커넥터 구성](#)을 참조하세요.

SFTP 커넥터를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택한 다음 커넥터 생성을 선택합니다.
3. 커넥터 유형에 SFTP 대해 를 선택하여 SFTP 커넥터를 생성한 다음 다음 를 선택합니다.

Transfer Family > Connectors > Create connector

Create connector Info

Create a connector that will be used to connect to your trading partner's server

Choose the connector type
Choose the protocol of the remote server to create a connector

☒ **SFTP**
Create a connector to connect to remote SFTP server

☐ **AS2**
Create a connector to connect to your trading partner's AS2 server

Cancel Next

4. 커넥터 구성 섹션에서 다음 정보를 제공합니다:

- 에 원격 SFTP 서버의 URL를 URL입력합니다. 자습서의 경우 원격 서버로 사용 중인 URL Transfer Family SFTP 서버의 를 입력합니다.

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

Replace **1111aaaa2222bbbb3** Transfer Family 서버 ID를 사용합니다.

- 액세스 역할 에 앞서 생성한 역할 를 입력합니다 **sftp-connector-role**.
- 로깅 역할 에서 를 선택합니다 **AWSTransferLoggingAccess**.

Note

AWSTransferLoggingAccess 는 AWS 관리형 정책입니다. 이 정책은 [여기](#)에 자세히 설명되어 있습니다. [AWS 관리형 정책: AWSTransferLoggingAccess](#).

Connector configuration**URL**

Specify the URL of remote server

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

Access role

IAM Role for Amazon S3 access and AWS Secrets Manager access

sftp-connector-role

**Logging role - optional** [Info](#)

IAM role for the connector to push events to your CloudWatch logs

AWSTransferLoggingAccess

**5. SFTP 구성 섹션에서 다음 정보를 제공합니다.**

- 커넥터 자격 증명 에서 SFTP 자격 증명에 포함된 Secrets Manager 리소스의 이름을 선택합니다. 자습서에서 를 선택합니다 **aws/transfer/sftp-connector1**.
- 신뢰할 수 있는 호스트 키 의 경우 호스트 키의 퍼블릭 부분에 붙여 넣습니다. SFTP 서버에 ssh-keyscan 대해 를 실행하여 이 키를 검색할 수 있습니다. 신뢰할 수 있는 호스트 키를 포맷하고 저장하는 방법에 대한 자세한 내용은 섹션을 참조하세요. [SftpConnectorConfig](#) 데이터 유형 설명서.

SFTP configuration [Info](#)

Connector credentials

Select the username and password / SSH private key that will be used to connect to the remote server from AWS Secret Manager

aws/transfer/sftp-connector1 ▼



Store a new secret 

Trusted host keys

Connector connects to the remote server only if the SSH public key matches one of the below

ssh-rsa AAAA[REDACTED]

Remove

Add trusted host key

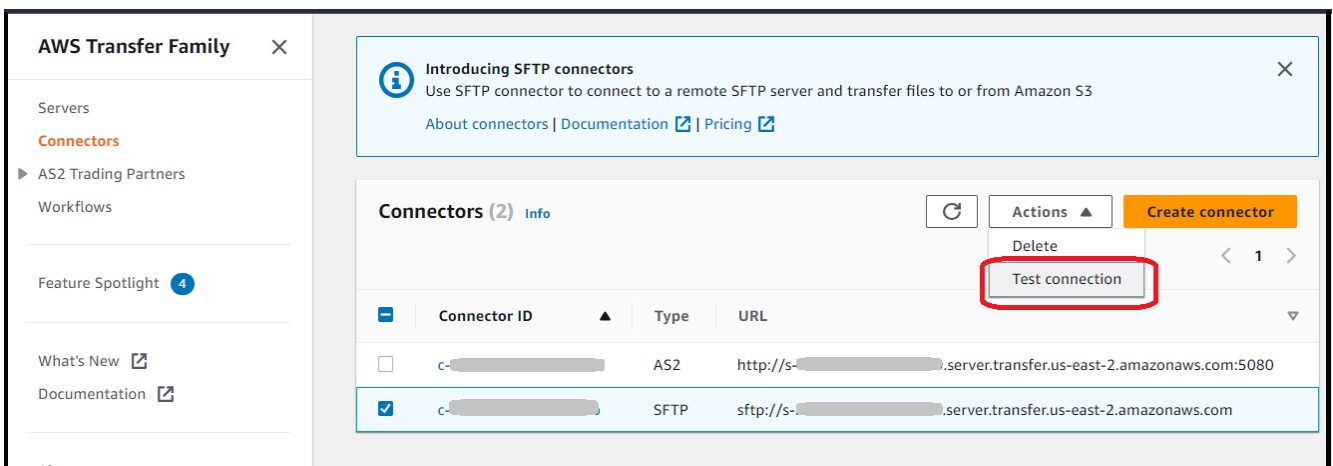
6. 모든 설정을 확인한 후 커넥터 생성을 선택하여 SFTP 커넥터를 생성합니다.

SFTP 커넥터를 생성한 후에는 새 커넥터를 사용하여 파일을 전송하기 전에 테스트하는 것이 좋습니다.

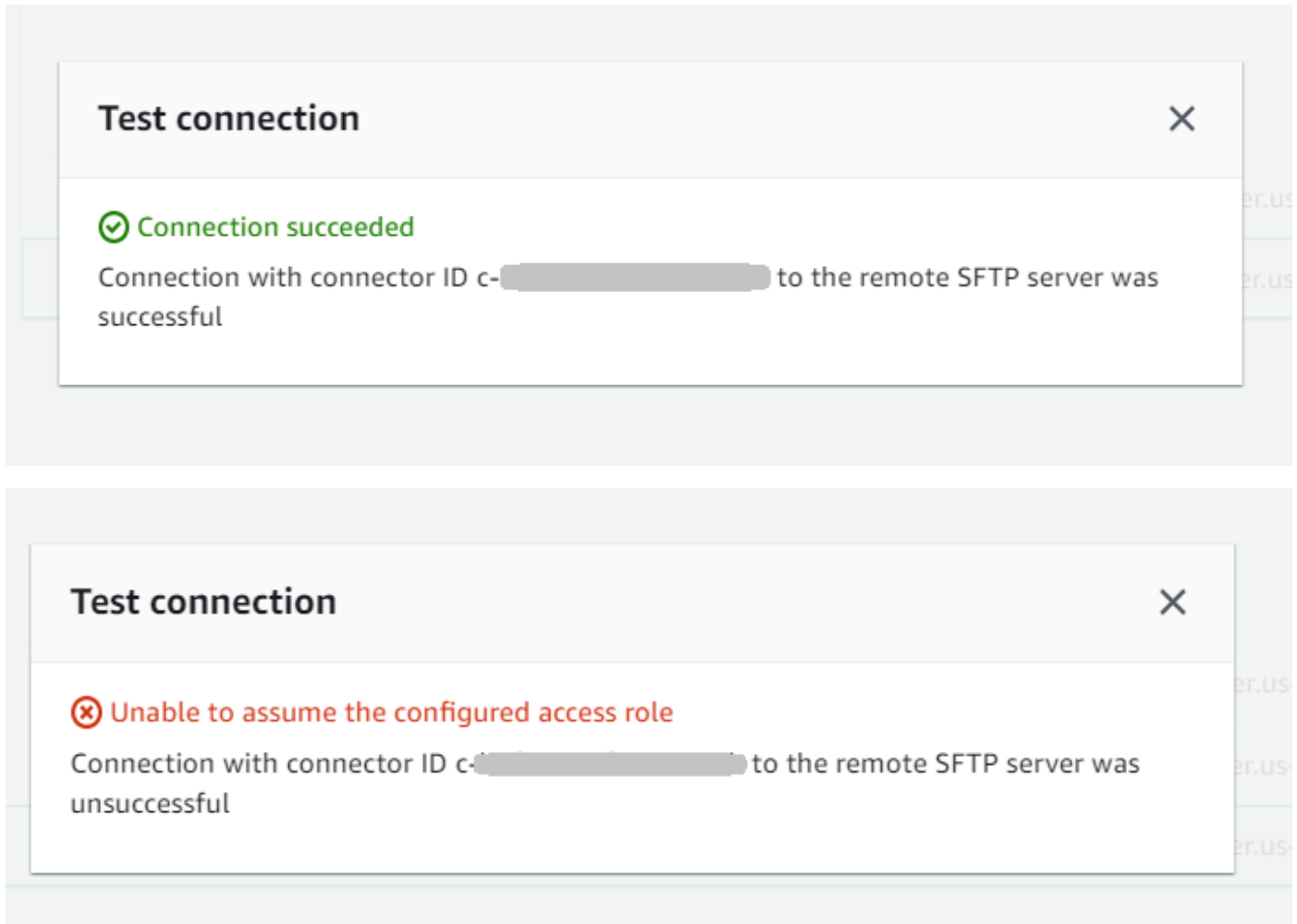
Test a connector using the console

SFTP 커넥터를 테스트하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택하고 커넥터를 선택합니다.
3. 작업 메뉴에서 테스트 연계를 선택합니다.



시스템은 테스트의 통과 또는 실패 여부를 나타내는 메시지를 반환합니다. 테스트가 실패하면 시스템은 테스트 실패 이유를 기반으로 오류 메시지를 제공합니다.



Test a connector using the CLI

를 사용하여 커넥터를 테스트하려면 명령 프롬프트에서 다음 명령을 AWS Command Line Interface 실행합니다(교체 *connector-id* 실제 커넥터 ID 포함):

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

테스트에 성공하면 다음 줄이 반환됩니다.

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

테스트에 실패하면 다음과 같은 설명 오류 메시지가 표시됩니다.

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

3단계: SFTP 커넥터를 사용하여 파일 전송 및 검색

간소화를 위해 Amazon S3 버킷에 파일이 이미 있다고 가정합니다.

Note

자습서에서는 소스 및 대상 스토리지 위치 모두에 Amazon S3 버킷을 사용합니다. SFTP 서버가 Amazon S3 스토리지를 사용하지 않는 경우 다음 명령 `sftp-server-storage-east`에서 볼 수 있는 위치에 관계없이 경로를 SFTP 서버에서 액세스할 수 있는 파일 위치의 경로로 바꿀 수 있습니다.

- Amazon S3 스토리지 `SEND-to-SERVER.txt`에서 SFTP 서버로 라는 파일을 보냅니다.
- `RETRIEVE-to-S3.txt` SFTP 서버에서 Amazon S3 스토리지로 라는 파일을 검색합니다.

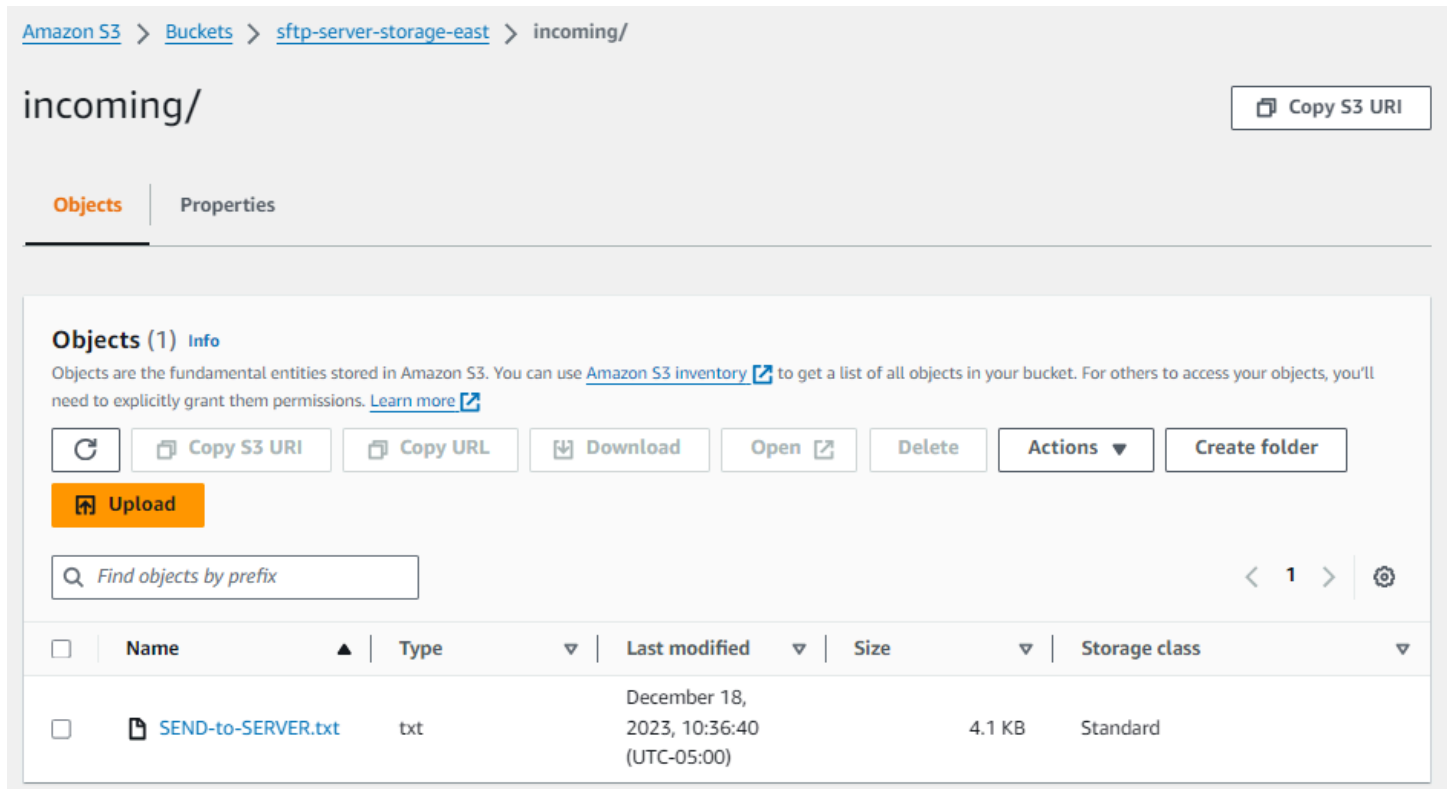
Note

다음 명령에서 를 바꿉니다. *connector-id* 커넥터 ID를 사용합니다.

먼저 Amazon S3 버킷에서 원격 SFTP 서버로 파일을 보냅니다. 명령 프롬프트에서 다음 명령을 실행합니다.

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/s3-storage-east/SEND-to-SERVER.txt" /
--remote-directory-path "/sftp-server-storage-east/incoming"
```

이제 `sftp-server-storage-east` 버킷이 이렇게 보일 것입니다.



파일이 예상대로 표시되지 않으면 CloudWatch 로그를 확인합니다.

CloudWatch 로그를 확인하려면

1. 에서 Amazon CloudWatch 콘솔 열기 <https://console.aws.amazon.com/cloudwatch/>
2. 왼쪽 탐색 메뉴에서 로그 그룹을 선택합니다.
3. 검색 창에 커넥터 ID를 입력하여 로그를 찾습니다.
4. 검색에서 반환되는 로그 스트림을 선택합니다.
5. 최신 로그 항목을 확장합니다.

성공하면 로그 항목은 다음과 같습니다.

```
{
  "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": "/s3-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": "500655546075",
"connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/connector-id",
"remote-directory-path": "/sftp-server-storage-east/incoming"
}

```

파일 전송이 실패하면 로그 항목에 문제를 지정하는 오류 메시지가 포함됩니다. 오류의 일반적인 원인은 IAM 권한 문제와 잘못된 파일 경로입니다.

다음으로 SFTP 서버에서 Amazon S3 버킷으로 파일을 검색합니다. 명령 프롬프트에서 다음 명령을 실행합니다.

```

aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths "/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/s3-storage-east/incoming"

```

전송에 성공하면 Amazon S3 버킷에 다음과 같이 전송된 파일이 포함됩니다.

Amazon S3 > Buckets > s3-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
☐	RETRIEVE-to-S3.txt	txt	December 18, 2023, 10:26:58 (UTC-05:00)	4.1 KB	Standard

성공하면 로그 항목은 다음과 같습니다.

```
{
```

```

    "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": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/c-connector-id",
    "local-directory-path": "/s3-storage-east/incoming"
  }

```

원격 서버로 사용할 Transfer Family SFTP 서버를 생성하는 절차

다음은 이 자습서의 원격 서버 역할을 하는 Transfer Family SFTP 서버를 생성하는 단계를 간략하게 설명합니다. 유의할 사항:

- Transfer Family 서버를 사용하여 원격 SFTP 서버를 나타냅니다. 일반적인 SFTP 커넥터 사용자에게는 자체 원격 SFTP 서버가 있습니다. [Transfer Family SFTP 서버 및 사용자 생성](#)을 참조하세요.
- Transfer Family 서버를 사용하기 때문에 서비스 관리형 SFTP 사용자도 사용하고 있습니다. 또한 간소화를 위해 이 사용자가 Transfer Family 서버에 액세스하는 데 필요한 권한을 커넥터를 사용하는 데 필요한 권한과 결합했습니다. 다시 말하지만 대부분의 SFTP 커넥터 사용 사례에는 Transfer Family 서버와 연결되지 않은 별도의 SFTP 사용자가 있습니다. [Transfer Family SFTP 서버 및 사용자 생성](#)을 참조하세요.
- 자습서의 경우 원격 SFTP 서버에 Amazon S3 스토리지를 사용하므로 한 버킷에서 다른 버킷으로 파일을 전송할 수 있도록 두 번째 버킷 **s3-storage-east**을 생성해야 합니다.

Transfer Family SFTP 서버 및 사용자 생성

사용자가 있는 SFTP 서버가 이미 있으므로 대부분의 사용자는 Transfer Family 서버와 사용자를 생성할 필요가 없으며 이 서버를 사용하여 파일을 주고 받을 SFTP 수 있습니다. 그러나 이 자습서에서는 간소화를 위해 Transfer Family 서버를 사용하여 원격 SFTP 서버로 작동합니다.

에 설명된 절차에 따라 서버를 [SFTP활성화 서버 생성](#) 생성하고 사용자를 [3단계: 서비스 관리 사용자 추가](#) 추가합니다. 자습서에서 사용 중인 사용자 세부 정보는 다음과 같습니다.

- 서비스 관리형 사용자 를 생성합니다 `sftp-testuser`.
 - 홈 디렉터리를 로 설정 `/sftp-server-storage-east/sftp-testuser`
 - 사용자를 생성할 때 퍼블릭 키를 저장합니다. 나중에 Secrets Manager에서 보안 암호를 생성할 때 해당 프라이빗 키를 제공해야 합니다.
- 역할: `sftp-connector-role`. 자습서의 경우 SFTP 사용자와 SFTP 커넥터 액세스 모두에 동일한 IAM 역할을 사용하고 있습니다. 조직의 커넥터를 생성할 때 별도의 사용자 및 액세스 역할이 있을 수 있습니다.
- 서버 호스트 키: 커넥터를 생성할 때 서버 호스트 키를 사용해야 합니다. 서버에 `ssh-keyscan` 대해를 실행하여 이 키를 검색할 수 있습니다. 예를 들어 서버 ID가 `s-1111aaaa2222bbbb3`이고 엔드포인트가 `us-east-1`에 있는 경우 `us-east-1`다음 명령은 서버 호스트 키를 검색합니다.

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

2단계: SFTP 커넥터 생성 및 테스트 절차에 붙여넣어야 하므로 이 텍스트를 어딘가에 복사합니다.

결합된 사용자 및 액세스 역할

자습서에서는 하나의 결합된 역할을 사용합니다. 이 역할은 SFTP 사용자뿐만 아니라 커넥터에 대한 액세스에도 사용됩니다. 다음 예제에는 자습서에서 작업을 수행하려는 경우 이 역할에 대한 세부 정보가 포함되어 있습니다.

다음 예제에서는 Amazon S3의 두 버킷과 Secrets Manager에 `aws/transfer/sftp-connector1` 저장된 이라는 이름의 보안 암호에 액세스하는 데 필요한 권한을 부여합니다. 자습서의 경우 이 역할의 이름은 `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:::s3-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:::s3-storage-east/*"
      ]
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:500655546075:secret:aws/transfer/sftp-connector1-6RandomCharacters"
    }
  ]
}

```

Transfer Family에 대한 역할 생성에 대한 전체 세부 정보는 [여기](#)에 설명된 절차에 따라 역할을 [사용자 역할 생성](#) 생성합니다.

Amazon API Gateway 메서드를 사용자 지정 자격 증명 공급자로 설정

이 자습서에서는 Amazon API Gateway 메서드를 설정하고 사용자 지정 자격 증명 공급자로 사용하여 AWS Transfer Family 서버에 파일을 업로드하는 방법을 보여줍니다. 이 자습서에서는 [기본 스택 템플릿](#)과 기타 기본 기능을 예로만 사용합니다.

주제

- [사전 조건](#)
- [1단계: CloudFormation 스택 생성](#)
- [2단계: 서버의 API 게이트웨이 메서드 구성 확인](#)
- [3단계: Transfer Family 서버 세부 정보 보기](#)
- [4단계: 사용자가 서버에 연결할 수 있는지 테스트](#)
- [5단계: SFTP 연결 및 파일 전송 테스트](#)
- [6단계: 버킷에 대한 액세스 제한](#)
- [Amazon을 사용하는 경우 Lambda 업데이트 EFS](#)

사전 조건

에서 Transfer Family 리소스를 생성하기 전에 스토리지와 사용자 역할을 AWS CloudFormation 생성합니다.

스토리지를 지정하고 사용자 역할을 생성하려면

1. 사용 중인 스토리지에 따라 다음 설명서를 참조하세요.
 - Amazon S3 버킷을 생성하려면 Amazon Simple Storage Service 사용 설명서의 [S3 버킷을 생성하려면 어떻게 해야 하나요?](#) 단원을 참조하세요.
 - Amazon EFS 파일 시스템을 생성하려면 섹션을 참조하세요 [Amazon EFS 파일 시스템 구성](#).
2. 사용자 역할을 생성하려면 [IAM 역할 및 정책 생성](#) 단원을 참조하세요.

다음 섹션에서 AWS CloudFormation 스택을 생성할 때 스토리지의 세부 정보와 사용자 역할을 입력합니다.

1단계: CloudFormation 스택 생성

제공된 템플릿에서 AWS CloudFormation 스택을 생성하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 스택 생성을 선택한 다음 새 리소스 사용(표준)을 선택합니다.
3. 사전 조건 - 템플릿 준비 창에서 템플릿 준비 완료를 선택합니다.
4. 이 링크인 [기본 스택 템플릿](#) 을 복사하여 Amazon S3 URL 필드에 붙여 넣습니다.

5. 다음을 클릭합니다.
6. 스택 이름을 비롯한 파라미터를 지정합니다. 다음 작업을 수행합니다.
 - UserName 및 의 기본값을 바꿉니다UserPassword.
 - 에 앞서 생성한 스토리지(Amazon S3 버킷 또는 Amazon EFS 파일 시스템)의 세부 정보를 UserHomeDirectory입력합니다.
 - 기본값을 이전에 생성한 사용자 역할UserRoleArn로 바꿉니다. AWS Identity and Access Management (IAM) 역할에 적절한 권한이 있어야 합니다. IAM 역할 및 버킷 정책의 예는 섹션을 참조하세요6단계: 버킷에 대한 액세스 제한.
 - 암호 대신 퍼블릭 키를 사용하여 인증하려면 UserPublicKey1 필드에 퍼블릭 키를 입력합니다. 를 사용하여 서버에 처음 연결할 SFTP때 암호 대신 프라이빗 키를 제공합니다.
7. 다음을 선택한 후 스택 옵션 구성 페이지에서 다시 다음을 선택합니다.
8. 생성 중인 스택의 세부 정보를 검토한 다음 스택 생성을 선택합니다.

Note

페이지 하단의 기능 아래에서 가 IAM 리소스를 생성할 수 있음을 AWS CloudFormation 확 인해야 합니다.

2단계: 서버의 API 게이트웨이 메서드 구성 확인

Note

보안을 개선하기 위해 웹 애플리케이션 방화벽을 구성할 수 있습니다. AWS WAF 는 Amazon API Gateway로 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있는 웹 애플리케이션 방화 벽입니다. 세부 정보는 [웹 애플리케이션 방화벽 추가](#)을 참조하세요.

서버의 API Gateway 메서드 구성을 확인하고 배포하려면

1. 에서 API 게이트웨이 콘솔을 엽니다<https://console.aws.amazon.com/apigateway/>.
2. 템플릿이 생성한 사용자 지정 자격 증명 공급자 기본 템플릿 전송API을 선택합니다. AWS CloudFormation
3. 리소스 창에서 를 선택한 GET다음 메서드 요청 을 선택합니다.

4. 작업 에서 배포를 API선택합니다. 배포 단계에서 prod를 선택한 다음 배포를 선택합니다.

API Gateway 메서드가 성공적으로 배포되면 스테이지 편집기 섹션에서 성능을 확인합니다.

 Note

페이지 상단에 나타나는 호출 URL 주소를 복사합니다. 이 정보는 다음 단계에 필요합니다.

3단계: Transfer Family 서버 세부 정보 보기

템플릿을 사용하여 AWS CloudFormation 스택을 생성하면 Transfer Family 서버가 자동으로 생성됩니다.

Transfer Family 서버 세부 정보 보기

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 생성한 스택을 선택합니다.
3. 리소스 탭을 선택합니다.

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	

서버ARN는 TransferServer 행의 물리적 ID 옆에 표시됩니다. 서버 ID는 에 포함되어 있습니다. 예를 들어 s-11112222333344445ARN입니다.

- 에서 AWS Transfer Family 콘솔을 열고 <https://console.aws.amazon.com/transfer/> 서버 페이지에서 새 서버를 선택합니다.

서버 ID는 에 TransferServer 리소스에 대해 표시된 ID와 일치합니다 AWS CloudFormation.

4단계: 사용자가 서버에 연결할 수 있는지 테스트

Transfer Family 콘솔을 사용하여 사용자가 서버에 연결할 수 있는지 테스트하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 서버 페이지에서 새 서버를 선택하고 작업을 선택한 다음 테스트를 선택합니다.
3. 사용자 이름 필드와 암호 필드에 로그인 자격 증명의 텍스트를 입력합니다. AWS CloudFormation 스택을 배포할 때 설정하는 값입니다.
4. 서버 프로토콜 의 경우 를 선택하고 소스 IP SFTP의 경우 를 입력합니다 **127.0.0.1**.
5. 테스트를 선택합니다.

사용자 인증이 성공하면 테스트는 `Status Code: 200` HTML 응답과 사용자 역할 및 권한의 세부 정보가 포함된 JSON 객체를 반환합니다. 예:

```
{
  "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\"
}
```

테스트가 실패하면 에 사용 중인 역할에 API Gateway AWS 관리형 정책 중 하나를 추가합니다 API.

5단계: SFTP 연결 및 파일 전송 테스트

SFTP 연결을 테스트하려면

1. Linux 또는 macOS 장치에서 명령 터미널을 엽니다.
2. 인증에 암호를 사용하는지 또는 키 쌍을 사용하는지 여부에 따라 다음 명령 중 하나를 입력합니다.
 - 암호를 사용하는 경우 이 명령 입력:

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

메시지가 표시되면 암호를 입력합니다.

- 키 쌍을 사용하는 경우 이 명령 입력:

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

Note

이러한 sftp 명령에 Transfer Family 서버가 위치해 있는 AWS 리전 에 해당하는 코드를 입력합니다. 예를 들어 서버가 미국 동부(오하이오)에 있는 경우 **us-east-2**를 입력합니다.

3. sftp> 프롬프트에서 디렉터리와 파일(pwd 및 ls)을 업로드(put)하고 다운로드(get)하고 볼 수 있는지 확인합니다.

6단계: 버킷에 대한 액세스 제한

특정 Amazon S3 버킷에 액세스할 수 있는 사용자를 제한할 수 있습니다. 다음 예제는 CloudFormation 스택 및 사용자에게 대해 선택한 정책에서 사용할 설정을 보여줍니다.

이 예제에서는 AWS CloudFormation 스택에 대해 다음 파라미터를 설정합니다.

- CreateServer: true
- UserHomeDirectory: /myuser-bucket
- UserName: myuser
- UserPassword: MySuperSecretPassword

Important

다음은 암호의 예시입니다. API Gateway 메서드를 구성할 때 강력한 암호를 입력해야 합니다.

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

UserPublicKey1은 퍼블릭/프라이빗 키 페어의 일부로 생성한 퍼블릭 키입니다.

*role-id*은(는) 생성한 사용자 역할에 따라 다릅니다. *myuser-api-gateway-role*에 연결된 정책은 다음과 같습니다.

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

를 사용하여 서버에 연결하려면 프롬프트에 다음 명령 중 하나를 SFTP 입력합니다.

- 암호를 사용하여 인증하는 경우 실행할 명령:

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

메시지가 표시되면 암호를 입력합니다.

- 키 쌍을 사용하여 인증하는 경우 실행할 명령:

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


Note

이러한 sftp 명령의 경우 Transfer Family 서버가 AWS 리전 있는 의 ID를 사용합니다. 예를 들어 서버가 미국 동부(오하이오)에 있는 경우 us-east-2를 사용하세요.

sftp 프롬프트가 표시되면 pwd 명령을 실행하여 홈 디렉터리를 볼 수 있습니다. 예:

```
sftp> pwd
Remote working directory: /myuser-bucket
```

사용자는 홈 디렉터리 상위 디렉터리는 일체 볼 수 없습니다. 예:

```
sftp> pwd
Remote working directory: /myuser-bucket
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

Amazon을 사용하는 경우 Lambda 업데이트 EFS

Transfer Family 서버의 스토리지 옵션으로 AmazonEFS를 선택한 경우 스택의 lambda 함수를 편집해야 합니다.

Lambda 함수에 POSIX 프로파일 추가하려면

1. 에서 Lambda 콘솔을 엽니다 <https://console.aws.amazon.com/lambda/>.
2. 이전에 생성한 Lambda 함수를 선택합니다. Lambda 함수의 형식은 다음과 같습니다. **stack-name-GetUserConfigLambda-lambda-identifier**, 여기서 **stack-name** 는 CloudFormation 스택 이름이며 **lambda-identifier** 는 함수의 식별자입니다.
3. 코드 탭에서 index.js를 선택하여 함수에 대한 코드를 표시합니다.
4. response에서 Policy과(와) HomeDirectory 사이에 다음 줄을 추가합니다.

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

가 **uid-value** 그리고 **gid-value** 는 각각 사용자 ID와 그룹 ID를 나타내는 0 이상의 정수입니다.

예를 들어, POSIX 프로파일 추가한 후 응답 필드는 다음과 같을 수 있습니다.

```
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 '/'
};
```

AS2 구성 설정

이 자습서에서는 를 사용하여 적용성 문 2(AS2) 구성을 설정하는 방법을 설명합니다 AWS Transfer Family. 여기에 설명된 단계를 완료하면 샘플 거래 파트너의 AS2 메시지를 수락할 준비가 된 AS2활성화된 서버가 있습니다. 또한 샘플 거래 파트너에게 AS2 메시지를 보내는 데 사용할 수 있는 커넥터가 있습니다.

Note

예제 설정의 일부 부분에서는 AWS Command Line Interface ()를 사용합니다 AWS CLI. 아직 를 설치하지 않은 경우 AWS Command Line Interface 사용 설명서의 [의 최신 버전 설치 또는 업데이트를 AWS CLI](#) AWS CLI참조하세요.

1. 사용자 자신과 사용자의 거래 파트너를 위한 인증서를 만듭니다. 사용할 수 있는 기존 인증서가 있다면 이 단계를 건너뛰어도 됩니다.

이 과정은 [1단계: 에 대한 인증서 생성 AS2](#)에 설명되어 있습니다.

2. AS2 프로토콜을 사용하는 AWS Transfer Family 서버를 생성합니다. 선택적으로 서버에 탄력적 IP 주소를 추가하여 인터넷에 연결되도록 할 수 있습니다.

이 과정은 [2단계: AS2 프로토콜을 사용하는 Transfer Family 서버 생성](#)에 설명되어 있습니다.

Note

인바운드 전송에만 사용할 Transfer Family 서버를 생성해야 합니다. 아웃바운드 전송만 수행하는 경우에는 Transfer Family 서버가 필요하지 않습니다.

3. 1단계에서 생성한 인증서를 가져옵니다.

이 과정은 [3단계: Transfer Family 인증서 리소스로 인증서 가져오기](#)에 설명되어 있습니다.

4. 거래 파트너를 설정하려면 로컬 프로필과 파트너 프로필을 생성하세요.

이 과정은 [4단계: 사용자와 사용자의 거래 파트너를 위한 프로필 생성](#)에 설명되어 있습니다.

5. 거래 파트너와 계약을 체결합니다.

이 과정은 [5단계: 사용자와 사용자의 파트너 간의 계약서 작성](#)에 설명되어 있습니다.

Note

인바운드 전송에 대한 계약만 작성해야 합니다. 아웃바운드 전송만 수행하는 경우에는 계약이 필요하지 않습니다.

6. 사용자와 사용자의 거래 파트너와 계약을 체결합니다.

이 과정은 [6단계: 사용자와 사용자의 거래 파트너 간의 커넥터를 생성합니다](#)에 설명되어 있습니다.

Note

아웃바운드 전송 전용 커넥터를 생성해야 합니다. 인바운드 전송만 수행하는 경우 커넥터가 필요하지 않습니다.

7. AS2 파일 교환을 테스트합니다.

이 과정은 [7단계: Transfer FamilyAS2를 사용하여 파일 교환 테스트](#)에 설명되어 있습니다.

이 단계를 완료한 후 다음을 수행할 수 있습니다.

- Transfer Familystart-file-transfer AWS Command Line Interface (AWS CLI) 명령을 사용하여 원격 AS2지원 파트너 서버로 파일을 전송합니다.
- 가상 프라이빗 클라우드(VPC) 엔드포인트를 통해 포트 5080의 원격 AS2지원 파트너 서버에서 파일을 수신합니다.

1단계: 예에 대한 인증서 생성 AS2

AS2 교환의 두 당사자 모두 X.509 인증서가 필요합니다. 원하는 방식으로 이러한 인증서를 생성할 수 있습니다. 이 주제에서는 명령줄에서 [열기SSL](#)를 사용하여 루트 인증서를 생성한 다음 하위 인증서에 서명하는 방법을 설명합니다. 양 당사자는 자체 인증서를 생성해야 합니다.

Note

AS2 인증서의 키 길이는 최소 2048비트에서 최대 4096비트여야 합니다.

파트너와 파일을 전송하려면 다음 사항에 유의하세요.

- 프로필에 인증서를 첨부할 수 있습니다. 인증서에는 퍼블릭 키 또는 프라이빗 키가 포함됩니다.
- 사용자의 거래 파트너가 사용자에게 퍼블릭 키를 보내면, 사용자는 그에게 사용자의 퍼블릭 키를 보냅니다.
- 거래 파트너는 퍼블릭 키로 메시지를 암호화하고 프라이빗 키로 서명합니다. 정반대로, 사용자는 거래 파트너의 퍼블릭 키로 메시지를 암호화하고 그 메시지에 사용자 프라이빗 키로 서명합니다.

Note

를 사용하여 키를 관리하려면 GUI [Portecle](#)는 사용할 수 있는 옵션 중 하나입니다.

예 인증서를 생성하려면

Important

파트너에게 사용자 프라이빗 키를 보내지 마세요. 이 예시에서, 사용자는 한 당사자를 위해 자체 서명된 퍼블릭 키와 프라이빗 키 세트를 생성합니다. 테스트 목적으로 두 거래 파트너 역할을 모두 수행하려는 경우 이 지침을 반복하여 거래 파트너당 하나씩 총 두 세트의 키를 생성할 수 있습니다. 이 경우 두 루트 인증 기관()을 생성할 필요가 없습니다CAs.

1. 다음 명령을 실행하여 2048비트 길이의 모듈러스로 RSA 프라이빗 키를 생성합니다.

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

2. 다음 명령을 실행하여 사용자의 root-ca-key.pem파일로 자체 서명된 인증서를 생성합니다.

```
/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
```

-subj 아규먼트는 다음 두 값으로 구성됩니다.

	명칭	설명
C	국가 코드	사용자 조직이 위치한 국가를 나타내는 2자리 코드입니다.
ST	주, 지역 또는 지방	해당 조직이 위치한 주 또는 지방의 이름. (이 경우 지역은 사용자의 AWS 리전을 의미하지 않습니다.)
L	시 이름	해당 조직이 위치한 시의 이름.
O	조직 이름	, LLC Corp 등과 같은 접미사를 포함하여 조직의 전체 법적 이름입니다.
OU	조직 단위 이름	조직 내에서 이 인증서를 다루는 부서.
CN	일반 이름 또는 정규화된 도메인 이름(FQDN)	이 예에서는 루트 인증서를 생성하므로 값은 R00TCA입니다. 이 예에서는 인증서의 용도를 설명하는데 CN를 사용합니다.

3. 로컬 프로필을 위한 서명 키와 암호화 키를 생성하세요.

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

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

Note

Open 과 같은 일부 AS2지원 서버는 서명 및 암호화 모두에 동일한 인증서를 사용해야 AS2합니다. 이 경우 두 가지 용도로 동일한 프라이빗 키와 인증서를 가져올 수 있습니다. 이렇게 하려면 이전 명령 두 개 대신 다음 명령을 실행합니다.

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

4. 다음 명령을 실행하여 루트 키가 서명할 인증서 서명 요청(CSRs)을 생성합니다.

```
/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
```

5. 다음으로, signing-cert.conf 파일과 encryption-cert.conf 파일을 만들어야 합니다.

- 텍스트 편집기를 사용하여 다음 내용을 포함하는 signing-cert.conf 파일을 생성합니다.

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

- 텍스트 편집기를 사용하여 다음 내용을 포함하는 encryption-cert.conf 파일을 생성합니다.

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

6. 마지막으로 다음 명령을 실행하여 서명된 인증서를 생성합니다.

```
/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
```

2단계: AS2 프로토콜을 사용하는 Transfer Family 서버 생성

이 절차에서는 Transfer Family 를 사용하여 AS2활성화된 서버를 생성하는 방법을 설명합니다 AWS CLI.

Note

많은 예 단계에서 파일에서 파라미터를 로드하는 명령을 사용합니다. 파일을 사용하여 파라미터를 로드하는 방법에 대한 자세한 내용은 [파일에서 파라미터를 로드하는 방법](#)을 참조하세요.

이 방법 대신 콘솔을 사용하려면 [Transfer Family 콘솔을 사용하여 AS2 서버 생성](#) 섹션을 참조하세요.

SFTP 또는 FTPS AWS Transfer Family 서버를 생성하는 방법과 마찬가지로 create-server AWS CLI 명령의 --protocols AS2 파라미터를 사용하여 AS2활성화된 서버를 생성합니다. 현재 Transfer Family는 AS2 프로토콜에서 VPC 엔드포인트 유형과 Amazon S3 스토리지만 지원합니다.

create-server 명령을 사용하여 Transfer Family용 AS2활성화 서버를 생성하면 VPC 엔드포인트가 자동으로 생성됩니다. 이 엔드포인트는 AS2 메시지를 수락할 수 있도록 TCP 포트 5080을 노출합니다.

VPC 엔드포인트를 인터넷에 공개적으로 노출하려는 경우 탄력적 IP 주소를 VPC 엔드포인트와 연결할 수 있습니다.

이러한 지침을 사용하려면 다음이 필요합니다.

- VPC ID(VPC(예: vpc-abcdef01)).
- VPC 서브넷IDs의 입니다(예: subnet-abcdef01, subnet-subnet-abcdef01, subnet-021345ab).
- 거래 파트너로부터 TCP 포트 5080의 수신 트래픽을 허용하는 하나 이상의 IDs 보안 그룹(예: sg-1234567890abcdef0 및 sg-abcdef01234567890).
- (선택 사항) VPC 엔드포인트와 연결할 탄력적 IP 주소입니다.
- 거래 파트너가 를 VPC 통해 에 연결되어 있지 않은 경우 인터넷 게이트웨이가 VPN필요합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이를 사용하여 인터넷에 연결](#)을 참조하세요.

AS2활성화된 서버를 생성하려면

1. 다음 명령을 실행합니다. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```
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. (선택 사항) VPC 엔드포인트를 퍼블릭으로 설정할 수 있습니다. update-server작업을 통해서만 Transfer Family 서버에 탄력적 IP 주소를 연결할 수 있습니다. 다음 명령은 서버를 중지하고 탄력적 IP 주소로 업데이트한 다음 다시 시작합니다.

```
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
```

이 start-server 명령은 서버의 퍼블릭 IP 주소가 포함된 DNS 레코드를 자동으로 생성합니다. 거래 파트너에게 서버 액세스 권한을 부여하려면 거래 파트너에게 다음 정보를 제공해야 합니다. 이 경우에는 *your-region*는 귀하의 AWS 리전을 참조합니다.

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

거래 파트너에게 URL 제공하는 전체 내용은 다음과 같습니다.

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

3. AS2활성화된 서버에 액세스할 수 있는지 테스트하려면 다음 명령을 사용합니다. VPC 엔드포인트의 프라이빗 DNS 주소 또는 퍼블릭 엔드포인트(엔드포인트에 탄력적 IP 주소를 연결한 경우)를 통해 서버에 액세스할 수 있는지 확인합니다.

서버가 올바르게 구성되어 있으면 연결이 성공합니다. 하지만 유효한 AS2 메시지를 전송하지 않기 때문에 HTTP 상태 코드 400(잘못된 요청) 응답을 받게 됩니다.

- 퍼블릭 엔드포인트의 경우 (이전 단계에서 탄력적 IP 주소를 연결한 경우) 서버 ID와 지역을 대체하여 다음 명령을 실행합니다.

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

- 내에서 연결하는 경우 다음 명령을 실행하여 VPC 엔드포인트의 프라이빗 DNS 이름을 VPC로 회합합니다.

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

이 describe-server 명령은 VpcEndpointId 파라미터에서 VPC 엔드포인트 ID를 반환합니다. 이 값을 사용하여 다음 명령을 실행합니다.

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

이 describe-vpc-endpoints 명령은 DNSEntries 배열을 반환하며, 여기에는 여러 DnsName 파라미터가 포함됩니다. 다음 명령에서 리전 DNS 이름(가용 영역을 포함하지 않는 이름)을 사용합니다.

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

예를 들어, 다음 명령은 이전 명령의 자리 표시자에 대한 샘플 값을 보여줍니다.

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

- (옵션) 로깅 역할을 구성합니다. Transfer Family는 Amazon 로그에 구조화된 JSON 형식으로 전송 및 수신된 메시지의 상태를 CloudWatch 기록합니다. Transfer Family에 계정의 CloudWatch 로그에 대한 액세스 권한을 제공하려면 서버에서 로깅 역할을 구성해야 합니다.

를 신뢰하는 AWS Identity and Access Management (IAM) 역할을 생성하고 AWSTransferLoggingAccess 관리형 정책을 transfer.amazonaws.com에 연결합니다. 세부 정보는 [IAM 역할 및 정책 생성](#)을 참조하세요. 방금 생성한 IAM 역할의 Amazon 리소스 이름(ARN)을 기록하고 다음 update-server 명령을 실행하여 서버와 연결합니다.

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

Note

로깅 역할은 옵션이지만 메시지 상태를 확인하고 구성 문제를 해결할 수 있도록 로깅 역할을 설정하는 것이 좋습니다.

3단계: Transfer Family 인증서 리소스로 인증서 가져오기

이 절차에서는 AWS CLI를 사용하여 인증서를 가져오는 방법을 설명합니다. 이 방법 대신 Transfer Family 콘솔을 사용하려면 [the section called “AS2 인증서 가져오기”](#) 섹션을 참조하세요.

1단계에서 만든 서명 및 암호화 인증서를 가져오려면 다음 `import-certificate` 명령을 실행합니다. 암호화와 서명에 동일한 인증서를 사용하는 경우 동일한 인증서를 두 번 가져오세요 (한 번은 SIGNING 사용량과 함께, 다른 한 번은 ENCRYPTION 사용량과 함께).

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

이 명령은 사용자 서명 `CertificateId`를 반환합니다. 다음 섹션에서는 이 인증서 ID를 *my-signing-cert-id*라고 합니다.

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

이 명령은 암호화 `CertificateId`를 반환합니다. 다음 섹션에서는 이 인증서 ID를 *my-encrypt-cert-id*라고 합니다.

그런 다음, 다음 명령을 실행하여 파트너의 암호화 및 서명 인증서를 가져옵니다.

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

이 명령은 파트너의 암호화 CertificateId를 반환합니다. 다음 섹션에서는 이 인증서 ID를 *partner-encrypt-cert-id*라고 합니다.

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

이 명령은 파트너의 서명 CertificateId를 반환합니다. 다음 섹션에서는 이 인증서 ID를 *partner-signing-cert-id*라고 합니다.

4단계: 사용자와 사용자의 거래 파트너를 위한 프로필 생성

이 절차에서는 를 사용하여 AS2 프로필을 생성하는 방법을 설명합니다 AWS CLI. 이 방법 대신 Transfer Family 콘솔을 사용하려면 [the section called “AS2 프로필 생성”](#) 섹션을 참조하세요.

다음 명령을 실행하여 로컬 AS2 프로필을 생성합니다. 이 명령은 퍼블릭 키와 프라이빗 키가 포함된 인증서를 참조합니다.

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

이 명령은 프로필 ID를 반환합니다. 다음 섹션에서는 이 ID를 *my-profile-id*라고 합니다.

이제 다음 명령을 실행하여 파트너 프로필을 생성합니다. 이 명령어는 파트너의 퍼블릭 키 인증서만 사용합니다. 이 명령을 사용하려면 *user input placeholders*를 파트너의 AS2 이름 및 인증서와 같은 자체 정보로 바꿉니다IDs.

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

이 명령은 파트너의 프로필 ID를 반환합니다. 다음 섹션에서는 이 ID를 *partner-profile-id*라고 합니다.

Note

이전 명령에서 를 바꿉니다.MYCORP 조직의 이름을 사용하여 PARTNER-COMPANY 거래 파트너의 조직 이름을 사용합니다.

5단계: 사용자와 사용자의 파트너 간의 계약서 작성

이 절차에서는 를 사용하여 AS2 계약을 생성하는 방법을 설명합니다 AWS CLI. 이 방법 대신 Transfer Family 콘솔을 사용하려면 [the section called “AS2 계약 생성”](#) 섹션을 참조하세요.

계약은 두 프로파일(로컬 및 파트너), 인증서, 두 당사자 간의 인바운드 AS2 전송을 허용하는 서버 구성을 하나로 통합합니다. 다음 명령을 실행하여 항목을 나열할 수 있습니다.

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

이 단계에서는 버킷에 대한 읽기/쓰기 액세스 권한이 있는 Amazon S3 버킷 및 IAM 역할이 필요합니다. 이 역할을 생성하는 지침은 Transfer Family SFTP, FTP 및 FTPS 프로토콜과 동일하며 에서 사용할 수 있습니다 [IAM 역할 및 정책 생성](#).

계약을 생성하려면 다음 항목이 필요합니다.

- Amazon S3 버킷 이름(지정된 경우 객체 접두사 포함)
- 버킷ARN에 액세스할 수 있는 IAM 역할의
- 사용자의 Transfer Family 서버 ID
- 사용자의 프로필 ID 및 사용자 파트너의 프로필 ID

다음 명령을 실행하여 계약을 생성합니다.

```
aws transfer create-agreement --description "ExampleAgreementName" --server-id your-server-id \
--local-profile-id your-profile-id --partner-profile-id your-partner-profile-id --base-
directory /DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox \
--access-role arn:aws:iam::111111111111:role/TransferAS2AccessRole
```

성공한 경우 계약의 ID가 반환됩니다. 그리고 다음 명령을 사용하여 계약의 세부 정보를 볼 수 있습니다.

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

6단계: 사용자와 사용자의 거래 파트너 간의 커넥터를 생성합니다.

이 절차에서는 를 사용하여 AS2 커넥터를 생성하는 방법을 설명합니다 AWS CLI. 이 방법 대신 Transfer Family 콘솔을 사용하려면 [the section called “AS2 커넥터 구성”](#) 섹션을 참조하세요.

이 StartFileTransfer API 작업을 사용하여 커넥터를 사용하여 Amazon S3에 저장된 파일을 거래 파트너의 AS2 엔드포인트로 전송할 수 있습니다. 다음 명령을 실행하여 이전에 생성한 프로필을 찾을 수 있습니다.

```
aws transfer list-profiles
```

커넥터를 생성할 때 파트너의 AS2 서버 를 제공해야 합니다URL. 다음 텍스트를 testAS2Config.json라는 파일에 복사합니다.

```
{
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "LocalProfileId": "your-profile-id",
  "MdnResponse": "SYNC",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject",
  "PartnerProfileId": "partner-profile-id",
  "SigningAlgorithm": "SHA256"
}
```

Note

의 경우 DES_EDE3_CBC 알고리즘이 필요한 레거시 클라이언트를 지원해야 하는 경우가 아니면 알고리즘을 지정하지 EncryptionAlgorithm마세요. 암호화 알고리즘이 약하기 때문입니다.

이제 다음 명령을 실행하여 커넥터를 생성합니다.

```
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
```

7단계: Transfer FamilyAS2를 사용하여 파일 교환 테스트

거래 파트너로부터 파일 받기

퍼블릭 탄력적 IP 주소를 VPC 엔드포인트와 연결한 경우 Transfer Family는 퍼블릭 IP 주소가 포함된 DNS 이름을 자동으로 생성했습니다. 하위 도메인은 AWS Transfer Family 서버 ID(형식)입니다 s-1234567890abcdef0. 다음 형식으로 서버를 URL 거래 파트너에게 제공합니다.

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

퍼블릭 탄력적 IP 주소를 VPC 엔드포인트와 연결하지 않은 경우 포트 5080에서 HTTP POST 거래 파트너의 AS2 메시지를 수락할 수 있는 VPC 엔드포인트의 호스트 이름을 찾습니다. VPC 엔드포인트 세부 정보를 검색하려면 다음 명령을 사용합니다.

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

예를 들어 이전 명령이 VPC 엔드포인트 ID 를 반환한다고 가정합니다 vpce-1234abcd5678efghi. 그런 다음 다음 명령을 사용하여 DNS 이름을 검색합니다.

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

이 명령은 다음 명령을 실행하는 데 필요한 VPC 엔드포인트의 모든 세부 정보를 반환합니다.

DNS 이름은 DnsEntries 배열에 나열됩니다. VPC 엔드포인트VPC에 액세스하려면 거래 파트너가 내에 있어야 합니다(예: AWS PrivateLink 또는 를 통해VPN). 다음 형식으로 URL 파트너에게 VPC 엔드포인트를 제공합니다.

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

예를 들어, 다음은 이전 명령의 자리 표시자에 대한 샘플 값을 URL 보여줍니다.

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

이 예에서 성공적인 전송은 지정한 base-directory 파라미터에 [5단계: 사용자와 사용자의 파트너 간의 계약서 작성](#)의 지정된 위치에 저장됩니다. 이름이 myfile1.txt 및 myfile2.txt 인 파일이 성공적으로 수신되면 파일은 `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`로 저장됩니다

다. 여기서 파일은 `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile1.messageId.txt` 및 `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile2.messageId.txt` 저장됩니다.

Transfer Family 서버를 생성할 때 로깅 역할을 구성한 경우 CloudWatch 로그에서 AS2 메시지 상태를 확인할 수도 있습니다.

거래 파트너에게 파일을 보내세요.

Transfer Family를 사용하여 다음 `start-file-transfer` AWS Command Line Interface (AWS CLI) 명령에 설명된 대로 커넥터 ID와 파일 경로를 참조하여 AS2 메시지를 보낼 수 있습니다.

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/
myfile2.txt"
```

커넥터의 세부 정보를 가져오려면 다음 명령을 실행합니다.

```
aws transfer list-connectors
```

이 `list-connectors` 명령은 커넥터의 커넥터 IDsURLs, 및 Amazon 리소스 이름(ARNs)을 반환합니다.

특정 커넥터의 속성을 반환하려면 사용하려는 ID로 다음 명령을 실행합니다.

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

`describe-connector` 명령은 URL, 역할, 프로파일, 메시지 처리 알림(MDNs), 태그 및 모니터링 지표를 포함하여 커넥터의 모든 속성을 반환합니다.

JSON 및 파일을 확인하여 파트너가 MDN 파일을 성공적으로 수신했는지 확인할 수 있습니다. 이러한 파일 이름은 [파일 이름 및 위치](#)에 설명된 규칙에 따라 지정됩니다. 커넥터를 생성할 때 로깅 역할을 구성한 경우 CloudWatch 로그에서 AS2 메시지 상태를 확인할 수도 있습니다.

SFTP, FTPS또는 FTP 서버 엔드포인트 구성

이 주제에서는 하나 이상의 SFTP, 및 FTPS FTP 프로토콜을 사용하는 AWS Transfer Family 서버 엔드포인트를 생성하고 사용하는 방법에 대한 세부 정보를 제공합니다.

주제

- [자격 증명 공급자 옵션](#)
- [AWS Transfer Family 엔드포인트 유형 매트릭스](#)
- [SFTP, FTPS또는 FTP 서버 엔드포인트 구성](#)
- [클라이언트를 사용하여 서버 엔드포인트를 통한 파일 전송](#)
- [서버 엔드포인트에 대한 사용자 관리](#)
- [논리적 디렉터리를 사용하여 Transfer Family 디렉터리 구조를 단순화합니다.](#)

자격 증명 공급자 옵션

AWS Transfer Family 는 사용자를 인증하고 관리하기 위한 몇 가지 방법을 제공합니다. 다음 표에서는 Transfer Family와 함께 사용할 수 있는 ID 공급자를 비교합니다.

작업	AWS Transfer Family 서비스 관리형	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
지원되는 프로토콜	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
키 기반 인증	예	아니요	예	예
암호 인증	아니요	예	예	예
AWS Identity and Access Management (IAM) 및 POSIX	예	예	예	예
논리적 홈 디렉터리	예	예	예	예

작업	AWS Transfer Family 서비스 관리형	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
파라미터화된 액세스(사용자 이름 기반)	예	예	예	예
임시 액세스 구조	예	아니요	예	예
AWS WAF	아니요	아니요	예	아니요

참고:

- IAM 는 Amazon S3 백업 스토리지에 대한 액세스를 제어하는 데 사용되며 Amazon 에 POSIX 사용 됩니다EFS.
- 임시는 런타임에 사용자 프로필을 전송할 수 있는 기능을 의미합니다. 예컨대, 사용자 이름을 변수로 전달하여 사용자를 홈 디렉터리에 연결할 수 있습니다.
- 에 대한 자세한 내용은 섹션을 AWS WAF참조하세요 [웹 애플리케이션 방화벽 추가](#).
- Microsoft Azure AD와 통합된 Lambda 함수를 Transfer Family ID 공급자로 사용하는 방법을 설명하는 블로그 게시물이 있습니다. 자세한 내용은 [Azure Active Directory를 AWS Transfer Family 사용하여 인증 및 AWS Lambda](#)를 참조하세요.
- 사용자 지정 자격 증명 공급자를 사용하는 Transfer Family 서버를 빠르게 배포하는 데 도움이 되는 여러 AWS CloudFormation 템플릿을 제공합니다. 세부 정보는 [Lambda 함수 템플릿](#)을 참조하세요.

다음 절차에서는 SFTP-enabled 서버, FTPS-enabled 서버, FTP-enabled 서버 또는 AS2-enabled 서버를 생성할 수 있습니다.

다음 단계

- [SFTP활성화 서버 생성](#)
- [FTPS활성화 서버 생성](#)
- [FTP활성화 서버 생성](#)
- [구성 AS2](#)

AWS Transfer Family 엔드포인트 유형 매트릭스

Transfer Family 서버를 생성하는 경우 사용할 엔드포인트 타입을 선택합니다. 다음 표에서는 각 엔드포인트 타입의 특성에 대해 설명합니다.

엔드포인트 타입 매트릭스

기능	퍼블릭	VPC - 인터넷	VPC - 내부	VPC_Endpoint(사용되지 않음)
지원되는 프로토콜	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
액세스	인터넷을 통해 이 엔드포인트 유형은 에서 특별한 구성이 필요하지 않습니다VPC.	인터넷을 통해, AWS Direct Connect 또는 를 통한 온프레미스 데이터 센터와 같이 VPC 및 VPC 연결된 환경 내에서VPN.	AWS Direct Connect 또는 를 통한 온프레미스 데이터 센터와 같이 VPC 및 VPC 연결된 환경 내에서VPN.	AWS Direct Connect 또는 를 통한 온프레미스 데이터 센터와 같이 VPC 및 VPC 연결된 환경 내에서VPN.
고정 IP 주소	정적 IP 주소는 연결할 수 없습니다. 는 변경될 수 있는 IP 주소를 AWS 제공합니다.	탄력적 IP 주소를 엔드포인트에 연결할 수 있습니다. 이는 AWS에서 소유한 IP 주소일 수도 있고 자체 IP 주소일 수도 있습니다(자체 IP 주소 사용). 엔드포인트에 연결된 탄력적 IP 주소는 변경되지 않습니다.	엔드포인트에 연결된 사설 IP 주소는 변경되지 않습니다.	엔드포인트에 연결된 사설 IP 주소는 변경되지 않습니다.

기능	퍼블릭	VPC - 인터넷	VPC - 내부	VPC_Endpoint(사용되지 않음)
		서버에 연결된 사설 IP 주소도 변경되지 않습니다.		

기능	퍼블릭	VPC - 인터넷	VPC - 내부	VPC_Endpoint(사용되지 않음)
소스 IP 허용 목록	이 엔드포인트 타입은 소스 IP 주소별 허용 목록을 지원하지 않습니다. 엔드포인트는 공개적으로 액세스할 수 있으며 포트 22를 통해 트래픽을 수신합니다.  Note 호스팅 엔드포인트 VPC의 경우 SFTP Transfer Family 서버는 포트 22(기본 값) 또는 포트 2222를 통해 작동할 수 있습니다.	소스 IP 주소별로 액세스를 허용하려면 서버 엔드포인트에 연결된 보안 그룹과 엔드포인트가 있는 서브넷에 ACLs 연결된 네트워크를 사용할 수 있습니다.	소스 IP 주소별로 액세스를 허용하려면 서버 엔드포인트에 연결된 보안 그룹과 엔드포인트가 있는 서브넷에 연결된 네트워크 액세스 제어 목록(네트워크 ACLs)을 사용할 수 있습니다.	소스 IP 주소별로 액세스를 허용하려면 서버 엔드포인트에 연결된 보안 그룹과 엔드포인트가 있는 서브넷에 ACLs 연결된 네트워크를 사용할 수 있습니다.

기능	퍼블릭	VPC - 인터넷	VPC - 내부	VPC_Endpoint(사용되지 않음)
클라이언트 방화벽 허용 목록	서버의 DNS 이름을 허용해야 합니다. IP 주소는 변경될 수 있으므로 클라이언트 방화벽 허용 목록에 IP 주소를 사용하지 마세요.	서버 DNS 이름 또는 서버에 연결된 탄력적 IP 주소를 허용할 수 있습니다.	프라이빗 IP 주소 또는 엔드포인트 DNS 이름을 허용할 수 있습니다.	프라이빗 IP 주소 또는 엔드포인트 DNS 이름을 허용할 수 있습니다.

Note

VPC_ENDPOINT 엔드포인트 타입은 이제 더 이상 사용되지 않으며 새 서버를 만드는 데 사용할 수 없습니다. 를 사용하는 대신 이전 표에 설명된 대로 내부 또는 인터넷 연결로 사용할 수 있는 새 VPC 엔드포인트 유형(EndpointType=VPC)을 EndpointType=VPC_ENDPOINT로 사용합니다. 세부 정보는 [VPC_사용 중단ENDPOINT](#)를 참조하세요.

AWS Transfer Family 서버의 보안 상태를 강화하려면 다음 옵션을 고려해 보세요.

- 내부 액세스가 있는 VPC 엔드포인트를 사용하면 또는 를 통해 온프레미스 데이터 센터와 같이 VPC 또는 VPC연결된 환경 내의 클라이언트만 서버에 액세스할 수 있습니다 AWS Direct Connect VPN.
- 클라이언트가 인터넷을 통해 엔드포인트에 액세스하고 서버를 보호하도록 허용하려면 인터넷 연결 액세스가 있는 VPC 엔드포인트를 사용합니다. 그런 다음 사용자의 클라이언트를 호스팅하는 특정 IP 주소의 트래픽만 허용하도록 의 VPC보안 그룹을 수정합니다.
- 암호 기반 인증이 필요하고 서버에서 맞춤 ID 공급자를 사용하는 경우 암호 정책을 통해 사용자가 취약한 암호를 만들지 못하도록 하고 로그인 시도 실패 횟수를 제한하는 것이 좋습니다.
- AWS Transfer Family 는 관리형 서비스이므로 셸 액세스를 제공하지 않습니다. 기본 SFTP 서버에 직접 액세스하여 Transfer Family 서버에서 OS 기본 명령을 실행할 수 없습니다.
- 내부 액세스 권한이 있는 VPC 엔드포인트 앞에 Network Load Balancer를 사용합니다. 로드 밸런서의 리스너 포트를 포트 22에서 다른 포트로 변경합니다. 이렇게 하면 포트 스캐너와 봇이 서버를 탐

색할 위험을 줄일 수 있지만 제거하지는 못합니다. 포트 22가 스캔에 가장 많이 사용되기 때문입니다. 자세한 내용은 [이제 Network Load Balancer에서 보안 그룹 지원 블로그 게시물을 참조하세요.](#)

Note

Network Load Balancer 를 사용하는 경우 AWS Transfer Family CloudWatch 로그에는 실제 클라이언트 IP 주소가 NLB 아닌 의 IP 주소가 표시됩니다.

SFTP, FTPS또는 FTP 서버 엔드포인트 구성

AWS Transfer Family 서비스를 사용하여 파일 전송 서버를 생성할 수 있습니다. 다음 파일 전송 프로토콜을 사용할 수 있습니다.

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP) - 를 통한 파일 전송SSH. 세부 정보는 [the section called “SFTP활성화 서버 생성”](#)을 참조하세요.

Note

SFTP Transfer Family 서버를 생성하는 AWS CDK 예제를 제공합니다. 이 예제는 TypeScript를 사용하며 여기에서 사용할 수 [GitHub 있습니다.](#)

- 파일 전송 프로토콜 보안(FTPS) - TLS 암호화를 사용한 파일 전송. 세부 정보는 [the section called “FTPS활성화 서버 생성”](#)을 참조하세요.
- 파일 전송 프로토콜(FTP) - 암호화되지 않은 파일 전송입니다. 세부 정보는 [the section called “FTP 활성화 서버 생성”](#)을 참조하세요.
- 적용성 선언문 2(AS2) - 구조화된 business-to-business 데이터 전송을 위한 파일 전송입니다. 세부 정보는 [the section called “구성 AS2”](#)을 참조하세요. 의 경우 데모 목적으로 AWS CloudFormation 스택을 빠르게 생성할 AS2수 있습니다. 이 절차는 [템플릿을 사용하여 Transfer Family AS2 스택 데모 생성](#)에 설명되어 있습니다.

여러 프로토콜로 서버를 만들 수 있습니다.

Note

같은 서버 엔드포인트에 여러 프로토콜을 사용하도록 설정한 상태에서 여러 프로토콜에서 동일한 사용자 이름을 사용하여 액세스를 제공하려는 경우 ID 공급자에 각 프로토콜별 보안 인

중이 설정되어 있으면 그렇게 할 수 있습니다. 의 경우 SFTP 및 와 별도의 보안 인증을 유지하는 FTP것이 좋습니다FTPS. 이는 SFTP 및 와 달리 가 보안 인증 정보를 일반 텍스트로 FTPS FTP 전송하기 때문입니다. SFTP 또는 에서 FTP 자격 증명을 격리하여 FTP 자격 증명에 공유되거나 노출FTPS되면 워크로드가 SFTP 또는 를 사용하여 안전하게 FTPS 유지됩니다.

서버를 생성할 때 특정 를 선택하여 해당 서버에 할당된 사용자의 파일 작업 요청을 AWS 리전 수행합니다. 서버에 하나 이상의 프로토콜을 할당하는 동시에 다음 ID 공급자 타입 중 하나를 할당합니다:

- SSH 키를 사용하여 관리되는 서비스입니다. 세부 정보는 [서비스 관리형과 작업](#)을 참조하세요.
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). 이 방법을 사용하면 Microsoft Active Directory 그룹을 통합하여 Transfer Family 서버에 대한 액세스를 제공할 수 있습니다. 세부 정보는 [AWS 디렉터리 서비스 자격 증명 공급자 사용](#)을 참조하세요.
- 맞춤 메서드. 사용자 지정 자격 증명 공급자 메서드는 AWS Lambda 또는 Amazon API Gateway를 사용하고 디렉터리 서비스를 통합하여 사용자를 인증하고 권한을 부여할 수 있습니다. 이 서비스는 사용자의 서버만 식별하는 식별자를 자동으로 할당합니다. 세부 정보는 [사용자 지정 자격 증명 공급자와 작업](#)을 참조하세요. Transfer Family는 AWS CloudFormation 사용자 지정 자격 증명 공급자를 사용하는 서버를 빠르게 배포하는 데 사용할 수 있는 템플릿을 제공합니다.
- [인증에 위한 Lambda 함수](#) 는 인증에 Lambda 함수를 사용하는 CloudFormation 템플릿을 설명합니다.
- [API Gateway 메서드를 사용하여 인증](#)에서는 인증에 Amazon API Gateway 메서드를 사용하는 템플릿을 설명합니다 CloudFormation.

또한 기본 서버 엔드포인트를 사용하거나 Amazon Route 53 서비스를 사용하거나 선택한 도메인 이름 시스템() 서비스를 사용하여 서버에 엔드포인트 유형(공개 액세스 또는 VPC 호스팅DNS) 및 호스트 이름을 할당합니다. 서버 호스트 이름은 서버 호스트 이름이 AWS 리전 생성된 에서 고유해야 합니다.

또한 Amazon CloudWatch 로깅 역할을 할당하여 CloudWatch 로그에 이벤트를 푸시하고, 서버에서 사용할 수 있도록 활성화된 암호화 알고리즘이 포함된 보안 정책을 선택하고, 키-값 페어인 태그 형태로 서버에 메타데이터를 추가할 수 있습니다.

Important

인스턴스화한 서버와 데이터 전송에 대한 비용이 발생합니다. Transfer Family 사용 비용 견적을 AWS Pricing Calculator 얻는 데 사용할 요금 및 에 대한 자세한 내용은 [AWS Transfer Family 요금](#) 섹션을 참조하세요.

SFTP활성화 서버 생성

Secure Shell (SSH) 파일 전송 프로토콜(SFTP)은 인터넷을 통한 데이터 보안 전송에 사용되는 네트워크 프로토콜입니다. 프로토콜은 의 전체 보안 및 인증 기능을 지원합니다SSH. 금융 서비스, 의료, 소매 및 광고와 같은 다양한 산업의 비즈니스 파트너들 사이의 민감한 정보를 비롯한 데이터를 교환하는 데 널리 사용됩니다.

Note

SFTP Transfer Family용 서버는 포트 22를 통해 작동합니다. 호스팅 엔드포인트VPC의 경우 SFTP Transfer Family 서버는 포트 2222를 통해 작동할 수도 있습니다. 세부 정보는 [Virtual Private Cloud\(VPC\)에 서버 생성](#)을 참조하세요.

참고 항목

- SFTP Transfer Family 서버를 생성하는 AWS CDK 예제를 제공합니다. 이 예제에서는 TypeScript를 사용하며 여기에서 사용할 수 GitHub [있습니다](#).
- 내부에서 Transfer Family 서버를 배포하는 방법에 대한 자세한 내용은 IP 허용 목록 사용을 VPC참조하세요. [AWS Transfer Family](#)

SFTP활성화된 서버를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 열고 탐색 창에서 서버를 <https://console.aws.amazon.com/transfer/> 선택한 다음 서버 생성을 선택합니다.
2. 프로토콜 선택 에서 SFTP를 선택한 다음 다음 를 선택합니다.

Choose 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 **Next**

3. 자격 증명 공급자 선택에서 사용자 액세스를 관리하는 데 사용할 자격 증명 공급자를 선택합니다. 다음과 같은 옵션이 있습니다:

- 서비스 관리형 - 사용자 ID 및 키를 에 저장합니다 AWS Transfer Family.

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

Cancel Previous **Next**

- AWS Directory Service for Microsoft Active Directory – 엔드포인트에 액세스할 AWS Directory Service 디렉터리를 제공합니다. 그러면 Active Directory에 저장된 자격 증명을 사용하여 사용자를 인증할 수 있습니다. AWS Managed Microsoft AD 자격 증명 공급자 작업에 대한 자세한 내용은 [섹션을 참조하세요 AWS 디렉터리 서비스 자격 증명 공급자 사용](#).

Note

- 크로스 계정 및 공유 디렉터리는 에서 지원되지 않습니다 AWS Managed Microsoft AD.
- Directory Service를 자격 증명 공급자로 사용하여 서버를 설정하려면 몇 가지 AWS Directory Service 권한을 추가해야 합니다. 세부 정보는 [사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory](#)을 참조하세요.

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

- 맞춤 ID 공급자 – 다음 옵션 중 하나를 선택합니다.
 - AWS Lambda 를 사용하여 자격 증명 공급자 연결 - Lambda 함수가 지원하는 기존 자격 증명 공급자를 사용할 수 있습니다. 귀하는 Lambda 함수의 명칭을 제공합니다. 자세한 내용은 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.
 - Amazon API Gateway를 사용하여 자격 증명 공급자 연결 - 자격 증명 공급자로 사용하기 위해 Lambda 함수가 지원하는 API 게이트웨이 메서드를 생성할 수 있습니다. Amazon API GatewayURL와 호출 역할을 제공합니다. 자세한 내용은 [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.

어느 옵션이든 귀하가 인증 방법도 지정할 수 있습니다.

- 암호 또는 키 - 사용자는 암호 또는 키로 인증할 수 있습니다. 이것이 기본값입니다.
- 암호 ONLY - 사용자가 연결할 암호를 제공해야 합니다.
- 키 ONLY - 사용자가 연결할 프라이빗 키를 제공해야 합니다.
- 암호 AND 키 - 사용자는 연결할 프라이빗 키와 암호를 모두 제공해야 합니다. 서버가 먼저 키를 확인한 다음 키가 유효하면 암호를 입력하라는 메시지가 표시됩니다. 제공된 프라이빗 키가 저장된 퍼블릭 키와 일치하지 않는 경우 인증이 실패합니다.

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

[i](#) Either a valid password or valid private key will be required during user authentication

4. Next(다음)를 선택합니다.
5. 엔드포인트 선택에서 다음을 수행합니다.

- a. 엔드포인트 타입으로는 공적으로 액세스 가능 엔드포인트 타입을 선택합니다. VPC 호스팅 엔드포인트는 섹션을 참조하세요 [Virtual Private Cloud\(VPC\)에 서버 생성](#).
- b. (옵션) 맞춤 호스트 이름의 경우 없음을 선택합니다.

에서 제공하는 서버 호스트 이름을 가져옵니다 AWS Transfer Family. 서버 호스트 이름은 `serverId.server.transfer.regionId.amazonaws.com` 형식을 취합니다.

맞춤 호스트 이름의 경우 서버 엔드포인트의 맞춤 별칭을 지정합니다. 사용자 지정 호스트 이름 사용에 대한 자세한 내용은 [사용자 지정 호스트 이름으로 작업](#)를 참조하세요.

- c. (선택 사항) FIPS 활성화된 에서 FIPS 활성화된 엔드포인트 확인란을 선택하여 엔드포인트가 연방 정보 처리 표준()을 준수하는지 확인합니다 FIPS.

Note

FIPS-활성화된 엔드포인트는 북미 AWS 리전에서만 사용할 수 있습니다. 사용할 수 있는 리전은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요. 에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#) 를 FIPS참조하세요.

- d. Next(다음)를 선택합니다.

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

Custom hostname
Specify a custom alias for your server endpoint.

None ▼

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel Previous **Next**

6. 도메인 선택 페이지에서 선택한 프로토콜을 통해 데이터를 저장하고 액세스하는 데 사용할 AWS 스토리지 서비스를 선택합니다.

- 선택한 프로토콜을 통해 파일을 객체로 저장하고 액세스하려면 Amazon S3를 선택하세요.
- 선택한 프로토콜을 통해 Amazon EFS EFS 파일 시스템에 파일을 저장하고 액세스하려면 Amazon을 선택합니다.

Next(다음)를 선택합니다.

7. 추가 상세 정보 구성에서 다음을 수행합니다.

- 로깅의 경우 기존 로그 그룹을 지정하거나 새 로그 그룹을 생성합니다(기본 옵션).

기존 로그 그룹을 선택하는 경우 와 연결된 로그 그룹을 선택해야 합니다 AWS 계정.

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/ [dropdown] [refresh] [Create log group]

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Info Logging role is only required when selecting a workflow in the Managed workflows section below.

로그 그룹 생성을 선택하면 CloudWatch 콘솔(<https://console.aws.amazon.com/cloudwatch/>) 이 로그 그룹 생성 페이지로 열립니다. 자세한 내용은 [로그에서 CloudWatch 로그 그룹 생성을 참조하세요](#).

- b. (선택 사항) 관리형 워크플로 에서 Transfer Family가 워크플로를 실행할 때 수임해야 하는 워크플로IDs(및 해당 역할)를 선택합니다. 업로드 완료 시 실행할 워크플로 하나와 부분 업로드 시 실행할 워크플로 하나를 선택할 수 있습니다. 관리형 워크플로를 사용하여 파일을 처리하는 방법에 대한 자세한 내용은 [AWS Transfer Family 관리형 워크플로](#)를 참조하세요.

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. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

Note

기본적으로:

- FIPS 활성화된 엔드포인트를 선택하지 않으면 TransferSecurityPolicy-2020-06 보안 정책이 서버에 연결됩니다.
- FIPS 활성화된 엔드포인트를 선택하면 TransferSecurityPolicy-FIPS-2020-06 보안 정책이 서버에 연결됩니다.

보안 정책에 대한 자세한 설명은 섹션을 참조하세요 [에 대한 보안 정책 AWS Transfer Family](#).

Cryptographic algorithm options Info

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

- d. (선택 사항) 서버 호스트 키에 클라이언트가 서버를 연결할 때 서버를 식별하는 데 사용할 RSAED25519, 또는 ECDSA 프라이빗 키를 입력합니다. (옵션) 설명을 추가하여 여러 서버 호스트 키를 구분합니다.

서버를 생성한 후 호스트 키를 추가할 수 있습니다. 키를 교체하거나 키 및 ECDSA 키와 같은 다른 유형의 키를 사용하려는 경우 여러 호스트 RSA 키를 사용하는 것이 유용합니다.

Note

서버 호스트 키 섹션은 기존 SFTP 지원 서버에서 사용자를 마이그레이션하는 데만 사용됩니다.

Server Host Key [Info](#)

Private key - *optional*

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - *optional*

Add a description to differentiate between multiple private keys

Enter optional description

i You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (옵션) 태그의 키 및 값에서 하나 이상의 태그를 키-값 쌍을 입력한 다음 태그 추가를 선택합니다.
- f. Next(다음)를 선택합니다.

Tags

Key	Value	
Enter key	Enter value	Remove tag
Add tag		

- g. Amazon S3 디렉터리의 성능을 최적화할 수 있습니다. 예를 들어 홈 디렉터리로 이동하고 하위 디렉터리가 10,000개라고 가정해 보겠습니다. 즉, S3 버킷에는 10,000개의 폴더가 있습니다. 이 시나리오에서 `ls` (list) 명령을 실행하면 목록 작업이 6~8분 정도 걸립니다. 하지만 디렉터리를 최적화하는 경우 이 작업은 몇 초 밖에 걸리지 않습니다.

Optimized Directories Info

Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- h. (선택 사항) 조직 정책 또는 약관과 같은 사용자 지정 메시지를 최종 사용자에게 표시하도록 AWS Transfer Family 서버를 구성합니다. 디스플레이 배너의 경우 사전 인증 디스플레이 배너 텍스트 상자에 사용자가 인증하기 전에 표시할 텍스트 메시지를 입력합니다.

Display banners

Pre-authentication display banner - *optional*
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

- i. (옵션) 다음 추가 옵션을 구성할 수 있습니다.
- SetStat 옵션 : 클라이언트가 Amazon S3 버킷 SETSTAT에 업로드하는 파일에 를 사용하려고 할 때 생성되는 오류를 무시하려면 이 옵션을 활성화합니다. 자세한 내용은 의 SetStatOption 설명서를 참조하세요 [ProtocolDetails](#).
 - TLS 세션 재개: 이 옵션은 이 서버의 프로토콜 중 FTPS 하나로 를 활성화한 경우에만 사용할 수 있습니다.
 - 수동 IP : 이 옵션은 이 서버의 프로토콜 중 FTP 하나로 FTPS 또는 를 활성화한 경우에만 사용할 수 있습니다.

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. 검토 및 생성에서 옵션을 검토합니다.

- 모든 항목을 편집하려면 단계 옆에 있는 편집을 선택합니다.

Note

편집하기로 선택한 단계 이후의 각 단계를 검토해야 합니다.

- 변경 사항이 없는 경우 서버 생성을 선택하여 서버를 생성하세요. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때부터 서버는 사용자의 파일 작업을 수행할 수 있습니다.

Servers (1)							Actions	Add user	Create server
☐	Hostname	Server ID	State	users	Endpoint type	Domain			
☐	-	s-	Starting	No Users	Public	Amazon S3			

FTPS활성화 서버 생성

SSL (FTPS)를 통한 파일 전송 프로토콜은 의 확장입니다FTP. 전송 계층 보안(TLS) 및 보안 소켓 계층(SSL) 암호화 프로토콜을 사용하여 트래픽을 암호화합니다. FTPS에서는 제어 및 데이터 채널 연결을 동시에 또는 독립적으로 암호화할 수 있습니다.

FTPS활성화 서버를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 열고 탐색 창에서 서버를 <https://console.aws.amazon.com/transfer/> 선택한 다음 서버 생성 을 선택합니다.
2. 프로토콜 선택 에서 를 선택합니다FTPS.

서버 인증서 에서 클라이언트가 서버를 통해 연결할 때 서버를 식별하는 데 사용할 AWS Certificate Manager (ACM)에 저장된 인증서를 선택한 FTPS 다음 다음 다음을 선택합니다.

새 퍼블릭 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [퍼블릭 인증서 요청](#)을 참조하세요.

기존 인증서를 로 가져오려면 AWS Certificate Manager 사용 설명서의 [로 인증서 가져오기ACM](#)를 ACM참조하세요.

프라이빗 IP 주소를 FTPS 통해 사용할 프라이빗 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [프라이빗 인증서 요청을 참조하세요](#).

다음 암호화 알고리즘 및 키 크기를 사용하는 인증서가 지원됩니다:

- 2048비트RSA(RSA_2048)
- 4096비트RSA(RSA_4096)
- 타원 프라임 곡선 256비트(EC_prime256v1)
- 타원 프라임 곡선 384 비트(EC_secp384r1)
- 타원 프라임 곡선 521비트(EC_secp521r1)

Note

인증서는 지정된 FQDN 또는 IP 주소와 발급자에 대한 정보가 있는 유효한 SSL/TLS X.509 버전 3 인증서여야 합니다.

Choose 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

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate

Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS

[▼](#) [↻](#)

[Cancel](#) [Next](#)

3. 자격 증명 공급자 선택에서 사용자 액세스를 관리하는 데 사용할 자격 증명 공급자를 선택합니다. 다음과 같은 옵션이 있습니다:

- AWS Directory Service for Microsoft Active Directory – 엔드포인트에 액세스할 AWS Directory Service 디렉터리를 제공합니다. 그러면 Active Directory에 저장된 자격 증명을 사용하여 사용자를 인증할 수 있습니다. AWS Managed Microsoft AD 자격 증명 공급자 작업에 대한 자세한 내용은 [섹션을 참조하세요](#) [AWS 디렉터리 서비스 자격 증명 공급자 사용](#).

Note

- 크로스 계정 및 공유 디렉터리는 에서 지원되지 않습니다 AWS Managed Microsoft AD.
- Directory Service를 자격 증명 공급자로 사용하여 서버를 설정하려면 몇 가지 AWS Directory Service 권한을 추가해야 합니다. 세부 정보는 [사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory](#)을 참조하세요.

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

- 맞춤 ID 공급자 – 다음 옵션 중 하나를 선택합니다.
 - AWS Lambda 를 사용하여 자격 증명 공급자 연결 - Lambda 함수가 지원하는 기존 자격 증명 공급자를 사용할 수 있습니다. 귀하는 Lambda 함수의 명칭을 제공합니다. 자세한 내용은 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.
 - Amazon API Gateway를 사용하여 자격 증명 공급자 연결 - 자격 증명 공급자로 사용하기 위해 Lambda 함수가 지원하는 API 게이트웨이 메서드를 생성할 수 있습니다. Amazon API GatewayURL와 호출 역할을 제공합니다. 자세한 내용은 [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.

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

- Next(다음)를 선택합니다.
- 엔드포인트 선택에서 다음을 수행합니다.

[i](#) Note

FTPS Transfer Family용 서버는 포트 21(제어 채널) 및 포트 범위 8192~8200(데이터 채널)을 통해 작동합니다.

- a. 엔드포인트 유형 에서 VPC 호스팅 엔드포인트 유형을 선택하여 서버의 엔드포인트를 호스팅합니다. VPC 호스팅 엔드포인트 설정에 대한 자세한 내용은 섹션을 참조하세요 [Virtual Private Cloud\(VPC\)에 서버 생성](#).

 Note

공적 액세스 가능 엔드포인트는 지원되지 않습니다.

- b. (선택 사항) FIPS 활성화된 에서 FIPS 활성화된 엔드포인트 확인란을 선택하여 엔드포인트가 연방 정보 처리 표준()을 준수하는지 확인합니다 FIPS.

 Note

FIPS-활성화된 엔드포인트는 북미 AWS 리전에서만 사용할 수 있습니다. 사용할 수 있는 리전은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요. 에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#) 를 FIPS참조하세요.

- c. Next(다음)를 선택합니다.

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. 도메인 선택 페이지에서 선택한 프로토콜을 통해 데이터를 저장하고 액세스하는 데 사용할 AWS 스토리지 서비스를 선택합니다.

- 선택한 프로토콜을 통해 파일을 객체로 저장하고 액세스하려면 Amazon S3를 선택하세요.
- 선택한 EFS 프로토콜을 통해 Amazon EFS 파일 시스템에 파일을 저장하고 액세스하려면 Amazon을 선택합니다.

Next(다음)를 선택합니다.

7. 추가 상세 정보 구성에서 다음을 수행합니다.

- a. 로깅의 경우 기존 로그 그룹을 지정하거나 새 로그 그룹을 생성합니다(기본 옵션).

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

기존 로그 그룹을 선택하는 경우와 연결된 로그 그룹을 선택해야 합니다 AWS 계정.

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

로그 그룹 생성을 선택하면 CloudWatch 콘솔(<https://console.aws.amazon.com/cloudwatch/>) 이 로그 그룹 생성 페이지로 열립니다. 자세한 내용은 [로그에서 CloudWatch 로그 그룹 생성을 참조하세요](#).

- b. (선택 사항) 관리형 워크플로에서 Transfer Family가 워크플로를 실행할 때 수입해야 하는 워크플로IDs(및 해당 역할)를 선택합니다. 업로드 완료 시 실행할 워크플로 하나와 부분 업로드

시 실행할 워크플로 하나를 선택할 수 있습니다. 관리형 워크플로를 사용하여 파일을 처리하는 방법에 대한 자세한 내용은 [AWS Transfer Family 관리형 워크플로](#)를 참조하세요.

- c. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

Note

기본적으로:

- FIPS 활성화된 엔드포인트를 선택하지 않으면 TransferSecurityPolicy-2020-06 보안 정책이 서버에 연결됩니다.
- FIPS 활성화된 엔드포인트를 선택하면 TransferSecurityPolicy-FIPS-2020-06 보안 정책이 서버에 연결됩니다.

보안 정책에 대한 자세한 설명은 [섹션을 참조하세요](#)에 대한 보안 정책 AWS Transfer Family.

- d. 서버 호스트 키의 경우 비워 두세요.

Note

서버 호스트 키 섹션은 기존 SFTP지원 서버에서 사용자를 마이그레이션하는 데만 사용됩니다.

Server Host Key [Info](#)**Private key - optional**

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

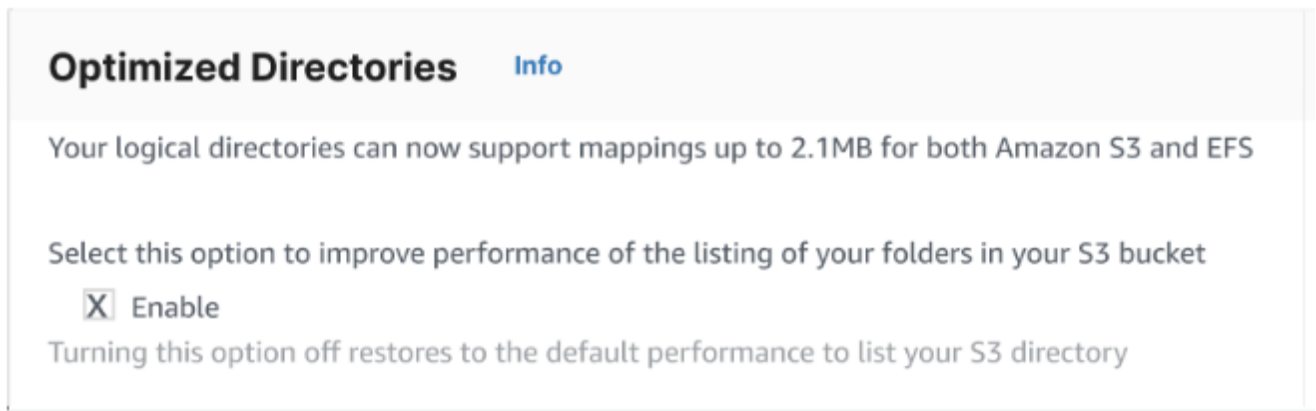
Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

Note You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (옵션) 태그의 키 및 값에서 하나 이상의 태그를 키-값 쌍을 입력한 다음 태그 추가를 선택합니다.
- f. Amazon S3 디렉터리의 성능을 최적화할 수 있습니다. 예를 들어 홈 디렉터리로 이동하고 하위 디렉터리가 10,000개라고 가정해 보겠습니다. 즉, S3 버킷에는 10,000개의 폴더가 있습니다. 이 시나리오에서 `ls (list)` 명령을 실행하면 목록 작업이 6~8분 정도 걸립니다. 하지만 디렉터리를 최적화하는 경우 이 작업은 몇 초 밖에 걸리지 않습니다.



- g. Next(다음)를 선택합니다.

- h. (선택 사항) 최종 사용자에게 조직 정책 또는 약관과 같은 사용자 지정 메시지를 표시하도록 AWS Transfer Family 서버를 구성할 수 있습니다. 성공적으로 인증한 사용자에게 사용자 지정 오늘 메시지(MOTD)를 표시할 수도 있습니다.

디스플레이 배너의 경우 사전 인증 디스플레이 배너 텍스트 상자에 사용자가 인증하기 전에 표시할 텍스트 메시지를 입력하고, 인증 후 디스플레이 배너 텍스트 상자에는 인증에 성공한 후 사용자에게 표시할 텍스트를 입력합니다.

Display banners

Pre-authentication display banner - optional
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

Post-authentication display banner - optional
Enter the message you want displayed after the client has connected to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

i SFTP clients will only be able to see the pre-authentication message. FTPS and FTP clients will be able to see both pre-authentication and post-authentication messages.

i. (옵션) 다음 추가 옵션을 구성할 수 있습니다.

- **SetStat 옵션** : 클라이언트가 Amazon S3 버킷 SETSTAT에 업로드하는 파일에 를 사용하려고 할 때 생성되는 오류를 무시하려면 이 옵션을 활성화합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 SetStatOption 설명서를 참조하세요.
- **TLS 세션 재개** : 는 FTPS 세션의 제어 및 데이터 연결 간에 협상된 보안 암호를 재개하거나 공유하는 메커니즘을 제공합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 TlsSessionResumptionMode 설명서를 참조하세요.
- **패시브 IP** : FTP 및 FTPS 프로토콜에 대한 패시브 모드를 나타냅니다. 방화벽, 라우터 또는 로드 밸런서의 퍼블릭 IP IPv4 주소와 같은 단일 주소를 입력합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 PassiveIp 설명서를 참조하세요.

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. 검토 및 생성에서 옵션을 검토합니다.

- 모든 항목을 편집하려면 단계 옆에 있는 편집을 선택합니다.

Note

편집하기로 선택한 단계 이후의 각 단계를 검토해야 합니다.

- 변경 사항이 없는 경우 서버 생성을 선택하여 서버를 생성하세요. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때부터 서버는 사용자의 파일 작업을 수행할 수 있습니다.

Servers (1)

Actions ▾

Add user

Create server

<

1

>

☐	Hostname ▲	Server ID ▼	State ▼	users ▼	Endpoint type ▼	Domain ▼
☐	-	s-	Starting	No Users	Public	Amazon S3

다음 단계: 다음 단계에서는 [사용자 지정 자격 증명 공급자와 작업](#)를 계속 진행하여 사용자를 설정하세요.

FTP활성화 서버 생성

파일 전송 프로토콜(FTP)은 데이터 전송에 사용되는 네트워크 프로토콜입니다. FTP 는 제어 및 데이터 전송에 별도의 채널을 사용합니다. 통제 채널은 종료되거나 비활성 제한 시간이 초과될 때까지 열려 있습니다. 데이터 채널은 전송 기간 동안 활성 상태입니다. FTP 는 일반 텍스트를 사용하며 트래픽 암호화를 지원하지 않습니다.

Note

를 활성화할 때는 VPC호스팅 엔드포인트에 대한 내부 액세스 옵션을 선택해야 FTP합니다. 서버가 퍼블릭 네트워크를 통과하는 데이터가 필요한 경우 SFTP 또는 와 같은 보안 프로토콜을 사용해야 합니다FTPS.

FTP활성화된 서버를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 열고 탐색 창에서 서버를 <https://console.aws.amazon.com/transfer/> 선택한 다음 서버 생성 을 선택합니다.
2. 프로토콜 선택 에서 FTP를 선택한 다음 다음 를 선택합니다.

Choose 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 **Next**

3. 자격 증명 공급자 선택에서 사용자 액세스를 관리하는 데 사용할 자격 증명 공급자를 선택합니다. 다음과 같은 옵션이 있습니다:
 - AWS Directory Service for Microsoft Active Directory – 엔드포인트에 액세스할 AWS Directory Service 디렉터리를 제공합니다. 그러면 Active Directory에 저장된 자격 증명을 사용하여 사용

자를 인증할 수 있습니다. AWS Managed Microsoft AD 자격 증명 공급자 작업에 대한 자세한 내용은 섹션을 참조하세요 [AWS 디렉터리 서비스 자격 증명 공급자 사용](#).

Note

- 크로스 계정 및 공유 디렉터리는 에서 지원되지 않습니다 AWS Managed Microsoft AD.
- Directory Service를 자격 증명 공급자로 사용하여 서버를 설정하려면 몇 가지 AWS Directory Service 권한을 추가해야 합니다. 세부 정보는 [사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory](#)을 참조하세요.

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

- 맞춤 ID 공급자 – 다음 옵션 중 하나를 선택합니다.
 - AWS Lambda 를 사용하여 자격 증명 공급자 연결 - Lambda 함수가 지원하는 기존 자격 증명 공급자를 사용할 수 있습니다. 귀하는 Lambda 함수의 명칭을 제공합니다. 자세한 내용은 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.
 - Amazon API Gateway를 사용하여 자격 증명 공급자 연결 - 자격 증명 공급자로 사용하기 위해 Lambda 함수가 지원하는 API 게이트웨이 메서드를 생성할 수 있습니다. Amazon API GatewayURL과 호출 역할을 제공합니다. 자세한 내용은 [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.

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

- Next(다음)를 선택합니다.
- 엔드포인트 선택에서 다음을 수행합니다.

[i](#) Note

FTP Transfer Family용 서버는 포트 21(제어 채널) 및 포트 범위 8192~8200(데이터 채널)을 통해 작동합니다.

- a. 엔드포인트 유형 에서 VPC 호스팅을 선택하여 서버의 엔드포인트를 호스팅합니다. VPC 호스팅 엔드포인트 설정에 대한 자세한 내용은 섹션을 참조하세요 [Virtual Private Cloud\(VPC\)에 서버 생성](#).

 Note

공적 액세스 가능 엔드포인트는 지원되지 않습니다.

- b. FIPS 활성화된 의 경우 FIPS 활성화된 엔드포인트 확인란을 선택 취소합니다.

 Note

FIPS-enabled 엔드포인트는 FTP 서버에서 지원되지 않습니다.

- c. Next(다음)를 선택합니다.

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. 도메인 선택 페이지에서 선택한 프로토콜을 통해 데이터를 저장하고 액세스하는 데 사용할 AWS 스토리지 서비스를 선택합니다.

- 선택한 프로토콜을 통해 파일을 객체로 저장하고 액세스하려면 Amazon S3를 선택하세요.
- 선택한 EFS 프로토콜을 통해 Amazon EFS 파일 시스템에 파일을 저장하고 액세스하려면 Amazon을 선택합니다.

Next(다음)를 선택합니다.

7. 추가 상세 정보 구성에서 다음을 수행합니다.

- a. 로깅의 경우 기존 로그 그룹을 지정하거나 새 로그 그룹을 생성합니다(기본 옵션).

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

기존 로그 그룹을 선택하는 경우와 연결된 로그 그룹을 선택해야 합니다 AWS 계정.

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

로그 그룹 생성을 선택하면 CloudWatch 콘솔(<https://console.aws.amazon.com/cloudwatch/>) 이 로그 그룹 생성 페이지로 열립니다. 자세한 내용은 [로그에서 CloudWatch 로그 그룹 생성을 참조하세요](#).

- b. (선택 사항) 관리형 워크플로에서 Transfer Family가 워크플로를 실행할 때 수입해야 하는 워크플로IDs(및 해당 역할)를 선택합니다. 업로드 완료 시 실행할 워크플로 하나와 부분 업로드

시 실행할 워크플로 하나를 선택할 수 있습니다. 관리형 워크플로를 사용하여 파일을 처리하는 방법에 대한 자세한 내용은 [AWS Transfer Family 관리형 워크플로](#)를 참조하세요.

- c. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

Note

Transfer Family는 최신 보안 정책을 FTP 서버에 할당합니다. 그러나 FTP 프로토콜은 암호화를 사용하지 않으므로 FTP 서버는 보안 정책 알고리즘을 사용하지 않습니다. 서버가 FTPS 또는 SFTP 프로토콜을 사용하지 않는 한 보안 정책은 사용되지 않습니다.

- d. 서버 호스트 키의 경우 비워 두세요.

Note

서버 호스트 키 섹션은 기존 SFTP지원 서버에서 사용자를 마이그레이션하는 데만 사용됩니다.

Server Host Key [Info](#)

Private key - *optional*

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - *optional*

Add a description to differentiate between multiple private keys

Enter optional description

 You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (옵션) 태그의 키 및 값에서 하나 이상의 태그를 키-값 쌍을 입력한 다음 태그 추가를 선택합니다.
- f. Amazon S3 디렉터리의 성능을 최적화할 수 있습니다. 예를 들어 홈 디렉터리로 이동하고 하위 디렉터리가 10,000개라고 가정해 보겠습니다. 즉, S3 버킷에는 10,000개의 폴더가 있습니다. 이 시나리오에서 `ls` (list) 명령을 실행하면 목록 작업이 6~8분 정도 걸립니다. 하지만 디렉터리를 최적화하는 경우 이 작업은 몇 초 밖에 걸리지 않습니다.

Optimized Directories [Info](#)

Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- g. Next(다음)를 선택합니다.

- h. (선택 사항) 조직 정책 또는 약관과 같은 사용자 지정 메시지를 최종 사용자에게 표시하도록 AWS Transfer Family 서버를 구성할 수 있습니다. 성공적으로 인증한 사용자에게 사용자 지정 오늘 메시지(MOTD)를 표시할 수도 있습니다.

디스플레이 배너의 경우 사전 인증 디스플레이 배너 텍스트 상자에 사용자가 인증하기 전에 표시할 텍스트 메시지를 입력하고, 인증 후 디스플레이 배너 텍스트 상자에는 인증에 성공한 후 사용자에게 표시할 텍스트를 입력합니다.

- i. (옵션) 다음 추가 옵션을 구성할 수 있습니다.
- SetStat 옵션 : 클라이언트가 Amazon S3 버킷 SETSTAT에 업로드하는 파일에 를 사용하려고 할 때 생성되는 오류를 무시하려면 이 옵션을 활성화합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 SetStatOption 설명서를 참조하세요.

- TLS 세션 재개 : 는 FTPS 세션의 제어 및 데이터 연결 간에 협상된 보안 암호를 재개하거나 공유하는 메커니즘을 제공합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 TlsSessionResumptionMode 설명서를 참조하세요.
- 패시브 IP : FTP 및 FTPS 프로토콜에 대한 패시브 모드를 나타냅니다. 방화벽, 라우터 또는 로드 밸런서의 퍼블릭 IP IPv4 주소와 같은 단일 주소를 입력합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 PassiveIp 설명서를 참조하세요.

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

8. 검토 및 생성에서 옵션을 검토합니다.

- 모든 항목을 편집하려면 단계 옆에 있는 편집을 선택합니다.

Note

편집하기로 선택한 단계 이후의 각 단계를 검토해야 합니다.

- 변경 사항이 없는 경우 서버 생성을 선택하여 서버를 생성하세요. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때부터 서버는 사용자의 파일 작업을 수행할 수 있습니다.

Servers (1)							Actions	Add user	Create server
☐	Hostname	Server ID	State	users	Endpoint type	Domain			
☐	-	s-	Starting	No Users	Public	Amazon S3			

다음 단계 - 그 다음 단계에서는 [사용자 지정 자격 증명 공급자와 작업](#)로 계속 진행하여 사용자를 설정하세요.

Virtual Private Cloud(VPC)에 서버 생성

퍼블릭 인터넷을 통하지 않고 Amazon S3 버킷 또는 Amazon EFS 파일 시스템과 데이터를 주고 받는 데 사용할 수 있도록 가상 프라이빗 클라우드(VPC) 내에서 서버의 엔드포인트를 호스팅할 수 있습니다.

Note

2021년 5월 19일 이후에는 2021년 5월 19일 이전에 AWS 계정이 아직 생성되지 않은 경우 계정 EndpointType=VPC_ENDPOINT에서 를 사용하여 서버를 생성할 수 없습니다. 2021년 2월 21일 또는 그 이전에 EndpointType=VPC_ENDPOINT AWS 계정에 가 포함된 서버를 이미 생성한 경우 영향을 받지 않습니다. 이 날짜 이후에는 EndpointType=VPC를 사용하세요. 자세한 내용은 [the section called “VPC_ 사용 중단ENDPOINT”](#) 단원을 참조하십시오.

Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 AWS 리소스를 호스팅하는 경우 VPC와 서버 간에 프라이빗 연결을 설정할 수 있습니다. 그러면 퍼블릭 IP 주소 지정을 사용하거나 인터넷 게이트웨이 필요 없이 이 서버를 사용하여 클라이언트를 통해 Amazon S3 버킷과 데이터를 주고 받을 수 있습니다.

Amazon 를 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 VPC 수 있습니다. VPC 를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블 및 네트워크 게이트웨이와 같은 네트워크 설정을 제어할 수 있습니다. 에 대한 자세한 내용은 [Amazon 사용 설명서의 Amazon이란 무엇입니까VPC?](#)를 VPCs참조하세요. VPC

다음 섹션에서는 를 생성하고 서버에 연결하는 방법에 VPC 대한 지침을 찾습니다. 개요로 다음과 같이 이 작업을 수행합니다.

1. VPC 엔드포인트를 사용하여 서버를 설정합니다.

2. VPC 엔드포인트를 VPC 통해 내에 있는 클라이언트를 사용하여 서버에 연결합니다. 이렇게 하면 AWS Transfer Family를 사용하여 Amazon S3 버킷에 저장된 데이터를 클라이언트를 통해 전송할 수 있습니다. 네트워크와 퍼블릭 인터넷 연결이 끊긴 경우에도 이 전송을 수행할 수 있습니다.
3. 또한 서버의 엔드포인트를 인터넷에 연결하도록 선택한 경우 탄력적 IP 주소를 엔드포인트와 연결할 수 있습니다. 이렇게 하면 외부의 클라이언트가 서버에 VPC 연결할 수 있습니다. VPC 보안 그룹을 사용하여 요청이 허용된 주소에서만 시작된 인증된 사용자에게 대한 액세스를 제어할 수 있습니다.

주제

- [내에서만 액세스할 수 있는 서버 엔드포인트 생성 VPC](#)
- [서버용 인터넷 경계 엔드포인트 생성](#)
- [서버의 엔드포인트 타입 변경](#)
- [VPC_ 사용 중단ENDPOINT](#)
- [AWS Transfer Family 서버 엔드포인트 유형을 VPC_ENDPOINT에서 로 업데이트 VPC](#)

내에서만 액세스할 수 있는 서버 엔드포인트 생성 VPC

다음 절차에서는 내 리소스만 액세스할 수 있는 서버 엔드포인트를 생성합니다VPC.

내에 서버 엔드포인트를 생성하려면 VPC

1. 에서 AWS Transfer Family 콘솔을 엽니다<https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택한 다음 서버 생성을 선택합니다.
3. 프로토콜 선택에서 하나 이상의 프로토콜을 선택한 후 다음을 선택합니다. 프로토콜에 대한 자세한 내용은 [2단계: SFTP활성화된 서버 생성](#)를 참조하세요.
4. 자격 증명 공급자 선택에서 에 사용자 자격 증명 및 키를 저장하도록 관리되는 서비스를 선택한 AWS Transfer Family다음 다음 다음을 선택합니다.

Note

이 절차에서는 서비스 관리형 옵션을 사용합니다. 사용자 지정 을 선택하면 Amazon API Gateway 엔드포인트와 엔드포인트에 액세스할 수 있는 AWS Identity and Access Management (IAM) 역할을 제공합니다. 이렇게 하면 디렉터리 서비스를 통합해 사용자를 인증하고 승인할 수 있습니다. 사용자 지정 자격 증명 공급자와의 작업에 대한 자세한 내용은 [사용자 지정 자격 증명 공급자와 작업](#)를 참조하세요.

5. 엔드포인트 선택에서 다음을 수행합니다.

Note

FTP Transfer Family용 및 FTPS 서버는 포트 21(제어 채널) 및 포트 범위 8192-8200(데이터 채널)을 통해 작동합니다.

- a. 엔드포인트 유형 에서 VPC 호스팅 엔드포인트 유형을 선택하여 서버의 엔드포인트를 호스팅합니다.
- b. 액세스에서 내부를 선택하여 엔드포인트의 사설 IP 주소를 사용하는 클라이언트만 엔드포인트에 액세스할 수 있도록 합니다.

Note

인터넷 연결 옵션에 대한 자세한 내용은 [서버용 인터넷 경계 엔드포인트 생성](#)를 참조하세요. 내부 액세스VPC용으로만 에서 생성된 서버는 사용자 지정 호스트 이름을 지원하지 않습니다.

- c. 에서 기존 VPC IDVPC를 선택하거나 생성 VPC를 선택하여 새 를 생성합니다VPC.
- d. 가용 영역 섹션에서 가용 영역 및 관련 서브넷을 최대 3개까지 선택합니다.
- e. 보안 그룹 섹션에서 기존 보안 그룹 ID를 IDs 선택하거나 보안 그룹 생성을 선택하여 새 보안 그룹을 생성합니다. 보안 그룹에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [에 대한 보안 그룹을 VPC](#) 참조하세요. 보안 그룹을 생성하려면 Amazon Virtual Private Cloud 사용 설명서의 [보안 그룹 생성](#)을 참조하세요.

Note

는 VPC 자동으로 기본 보안 그룹과 함께 제공됩니다. 서버를 시작할 때 다른 보안 그룹 또는 그룹을 지정하지 않을 경우 기본 보안 그룹이 서버에 연결됩니다.

보안 그룹의 인바운드 규칙의 경우 포트 22, 2222 또는 둘 다를 사용하도록 SSH 트래픽을 구성할 수 있습니다. 포트 22는 기본적으로 구성됩니다. 포트 2222를 사용하려면 보안 그룹에 인바운드 규칙을 추가합니다. 유형에 사용자 지정 TCP을 선택한 다음 포트 범위 **2222**에 를 입력하고 소스에 SSH 포트 22 규칙에 대해 가지고 있는 것과 동일한 CIDR 범위를 입력합니다.

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type info	Protocol info	Port range info	Source info
sg-...	HTTP	TCP	80	Custom 0.0.0.0/0
sg-...	RDP	TCP	3389	Custom 0.0.0.0/0
sg-...	HTTPS	TCP	443	Custom 0.0.0.0/0
sg-...	Custom TCP	TCP	2222	Custom 72.21.196.64/32
sg-...	SSH	TCP	22	Custom 72.21.196.64/32

Add rule

- f. (선택 사항) FIPS 활성화된 에서 FIPS 활성화된 엔드포인트 확인란을 선택하여 엔드포인트가 연방 정보 처리 표준()을 준수하는지 확인합니다FIPS.

Note

FIPS-활성화된 엔드포인트는 북미 AWS 리전에서만 사용할 수 있습니다. 사용할 수 있는 리전은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요. 에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#)를 FIPS참조하세요.

- g. Next(다음)를 선택합니다.
6. 추가 상세 정보 구성에서 다음을 수행합니다.
- a. CloudWatch 로깅 에서 다음 중 하나를 선택하여 사용자 활동의 Amazon CloudWatch 로깅을 활성화합니다.
- 새 역할을 생성할 수 있는 적절한 권한이 있는 한 Transfer Family가 IAM 자동으로 역할을 생성할 수 있도록 새 역할을 생성합니다. 생성된 IAM 역할을 라고 합니다AWSTransferLoggingAccess.
 - 기존 역할을 선택하여 계정에서 기존 IAM 역할을 선택합니다. 로깅 역할에서 역할을 선택합니다. 이 IAM 역할에는 서비스가 로 설정된 신뢰 정책이 포함되어야 합니다transfer.amazonaws.com.

CloudWatch 로깅에 대한 자세한 내용은 섹션을 참조하세요 [CloudWatch 로깅 역할 구성](#).

Note

- 로깅 역할을 지정 CloudWatch 하지 않으면 에서 최종 사용자 활동을 볼 수 없습니다.
- CloudWatch 로깅 역할을 설정하지 않으려면 기존 역할 선택을 선택하되 로깅 역할은 선택하지 마세요.

- b. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

Note

다른 정책을 선택하지 않는 한 TransferSecurityPolicy-2020-06 보안 정책이 기본적으로 서버에 연결됩니다.

보안 정책에 대한 자세한 설명은 [섹션을 참조하세요](#) [에 대한 보안 정책 AWS Transfer Family](#).

- c. (선택 사항) 서버 호스트 키에 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용할 RSAED25519, 또는 ECDSA 프라이빗 키를 입력합니다SFTP.

Note

이 섹션은 기존 SFTP지원 서버에서 사용자를 마이그레이션하는 경우에만 해당됩니다.

- d. (옵션) 태그의 키 및 값에서 하나 이상의 태그를 키-값 쌍을 입력한 다음 태그 추가를 선택합니다.
- e. 다음을 선택합니다.
7. 검토 및 생성에서 옵션을 검토합니다. 경우에 따라 다음 작업을 수행합니다.
- 이들 중 하나를 편집하려면 단계 옆에 있는 편집을 선택합니다.

Note

편집하기로 선택한 단계 이후의 각 단계를 검토해야 합니다.

- 변경 사항이 없으면 서버 생성을 선택하여 서버를 생성합니다. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때부터 서버는 사용자의 파일 작업을 수행할 수 있습니다.

서버용 인터넷 경계 엔드포인트 생성

다음 절차에서는 서버 엔드포인트를 만듭니다. 이 엔드포인트는 VPC의 기본 보안 그룹에서 소스 IP 주소가 허용되는 클라이언트만 인터넷을 통해 액세스할 수 있습니다. 또한 탄력적 IP 주소를 사용하여 엔드포인트가 인터넷 경계가 되도록 하면 클라이언트는 탄력적 IP 주소를 사용하여 방화벽에서 엔드포인트에 대한 액세스를 허용할 수 있습니다.

Note

SFTP 및 만 인터넷 연결 VPC 호스팅 엔드포인트에서 사용할 FTPS 수 있습니다.

인터넷 경계 엔드포인트를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택한 다음 서버 생성을 선택합니다.
3. 프로토콜 선택에서 하나 이상의 프로토콜을 선택한 후 다음을 선택합니다. 프로토콜에 대한 자세한 내용은 [2단계: SFTP 활성화된 서버 생성](#)를 참조하세요.
4. 자격 증명 공급자 선택에서 에 사용자 자격 증명 및 키를 저장하도록 관리되는 서비스를 선택한 AWS Transfer Family 다음 다음 다음을 선택합니다.

Note

이 절차에서는 서비스 관리형 옵션을 사용합니다. 사용자 지정 을 선택하면 Amazon API Gateway 엔드포인트와 엔드포인트에 액세스할 수 있는 AWS Identity and Access Management (IAM) 역할을 제공합니다. 이렇게 하면 디렉터리 서비스를 통합해 사용자를 인증하고 승인할 수 있습니다. 사용자 지정 자격 증명 공급자와의 작업에 대한 자세한 내용은 [사용자 지정 자격 증명 공급자와 작업](#)를 참조하세요.

5. 엔드포인트 선택에서 다음을 수행합니다.

- a. 엔드포인트 유형 에서 VPC 호스팅 엔드포인트 유형을 선택하여 서버의 엔드포인트를 호스팅합니다.
- b. 액세스의 경우 인터넷 연결을 선택하여 클라이언트가 인터넷을 통해 엔드포인트에 액세스할 수 있게 합니다.

Note

인터넷 연결을 선택하면 각 서브넷 또는 서브넷에서 기존 탄력적 IP 주소를 선택할 수 있습니다. 또는 VPC 콘솔(<https://console.aws.amazon.com/vpc/>)로 이동하여 하나 이상의 새 탄력적 IP 주소를 할당할 수 있습니다. 이러한 주소는 사용자가 소유 AWS 하거나 사용자가 소유할 수 있습니다. 이미 사용 중인 탄력적 IP 주소는 엔드포인트와 연결할 수 없습니다.

- c. (옵션) 사용자 지정 호스트 이름의 경우 다음 중 하나를 선택합니다.

Note

탄력적 IP 주소를 통해 직접 연결하거나 상용 라우팅 53 내에서 를 가리키는 호스트 이름 레코드를 생성 AWS GovCloud (US) 해야 하는 고객EIP. GovCloud 엔드포인트에서 Route 53을 사용하는 방법에 대한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 [AWS GovCloud \(US\) 리소스로 Amazon Route 53 설정을 참조하세요](#).

- Amazon Route 53 DNS별칭 - 사용하려는 호스트 이름이 Route 53에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 기타 DNS - 사용하려는 호스트 이름이 다른 DNS 공급자에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 없음 - 서버의 엔드포인트를 사용하고 사용자 지정 호스트 이름은 사용하지 않을 경우. 서버 호스트 이름은 `server-id.server.transfer.region.amazonaws.com` 형식을 취합니다.

Note

의 고객의 경우 없음을 AWS GovCloud (US)선택하면 이 형식으로 호스트 이름이 생성되지 않습니다.

사용자 지정 호스트 이름 사용에 대한 자세한 내용은 [사용자 지정 호스트 이름으로 작업을 참조](#)를 참조하세요.

- d. 에서 기존 VPC ID를 선택하거나 생성 VPC를 선택하여 새 VPC를 생성합니다.
- e. 가용 영역 섹션에서 가용 영역 및 관련 서브넷을 최대 3개까지 선택합니다. IPv4 주소 에서 각 서브넷의 탄력적 IP 주소를 선택합니다. 클라이언트가 방화벽에서 엔드포인트에 대한 액세스를 허용하는 데 사용할 수 있는 IP 주소입니다.
- f. 보안 그룹 섹션에서 기존 보안 그룹 ID를 선택하거나 보안 그룹 생성을 선택하여 새 보안 그룹을 생성합니다. 보안 그룹에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [에 대한 보안 그룹을 VPC](#) 참조하세요. 보안 그룹을 생성하려면 Amazon Virtual Private Cloud 사용 설명서의 [보안 그룹 생성](#)을 참조하세요.

Note

는 VPC 자동으로 기본 보안 그룹과 함께 제공됩니다. 서버를 시작할 때 다른 보안 그룹 또는 그룹을 지정하지 않을 경우 기본 보안 그룹이 서버에 연결됩니다.

보안 그룹의 인바운드 규칙의 경우 포트 22, 2222 또는 둘 다를 사용하도록 SSH 트래픽을 구성할 수 있습니다. 포트 22는 기본적으로 구성됩니다. 포트 2222를 사용하려면 보안 그룹에 인바운드 규칙을 추가합니다. 유형에 사용자 지정 TCP을 선택한 다음 포트 범위 **2222**에 를 입력하고 소스에 SSH 포트 22 규칙에 대해 가지고 있는 것과 동일한 CIDR 범위를 입력합니다.

VPC > Security Groups > sg- > default > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source
sg-	HTTP	TCP	80	Custom 0.0.0.0/0
sg-	RDP	TCP	3389	Custom 0.0.0.0/0
sg-	HTTPS	TCP	443	Custom 0.0.0.0/0
sg-	Custom TCP	TCP	2222	Custom 72.21.196.64/32
sg-	SSH	TCP	22	Custom 72.21.196.64/32

Add rule

- g. (선택 사항) FIPS 활성화된 에서 FIPS 활성화된 엔드포인트 확인란을 선택하여 엔드포인트가 연방 정보 처리 표준()을 준수하는지 확인합니다FIPS.

 Note

FIPS-활성화된 엔드포인트는 북미 AWS 리전에서만 사용할 수 있습니다. 사용할 수 있는 리전은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요. 에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#)를 FIPS참조하세요.

- h. Next(다음)를 선택합니다.

6. 추가 상세 정보 구성에서 다음을 수행합니다.

- a. CloudWatch 로깅 에서 다음 중 하나를 선택하여 사용자 활동의 Amazon CloudWatch 로깅을 활성화합니다.
- 새 역할을 생성할 수 있는 적절한 권한이 있는 한 Transfer Family가 IAM 자동으로 역할을 생성할 수 있도록 새 역할을 생성합니다. 생성된 IAM 역할을 라고 합니다AWSTransferLoggingAccess.
 - 기존 역할을 선택하여 계정에서 기존 IAM 역할을 선택합니다. 로깅 역할에서 역할을 선택합니다. 이 IAM 역할에는 서비스가 로 설정된 신뢰 정책이 포함되어야 합니다transfer.amazonaws.com.

CloudWatch 로깅에 대한 자세한 내용은 섹션을 참조하세요 [CloudWatch 로깅 역할 구성](#).

 Note

- 로깅 역할을 지정 CloudWatch 하지 않으면 에서 최종 사용자 활동을 볼 수 없습니다.
- CloudWatch 로깅 역할을 설정하지 않으려면 기존 역할 선택을 선택하고 로깅 역할은 선택하지 마세요.

- b. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

Note

다른 정책을 선택하지 않는 한 TransferSecurityPolicy-2020-06 보안 정책이 기본적으로 서버에 연결됩니다.

보안 정책에 대한 자세한 설명은 섹션을 참조하세요 [에 대한 보안 정책 AWS Transfer Family](#).

- c. (선택 사항) 서버 호스트 키에 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용할 RSAED25519, 또는 ECDSA 프라이빗 키를 입력합니다 SFTP.

Note

이 섹션은 기존 SFTP 지원 서버에서 사용자를 마이그레이션하는 경우에만 해당됩니다.

- d. (옵션) 태그의 키 및 값에서 하나 이상의 태그를 키-값 쌍을 입력한 다음 태그 추가를 선택합니다.
- e. Next(다음)를 선택합니다.
- f. (선택 사항) 관리형 워크플로에서 Transfer Family가 워크플로를 실행할 때 수임해야 하는 워크플로 IDs(및 해당 역할)를 선택합니다. 업로드 완료 시 실행할 워크플로 하나와 부분 업로드 시 실행할 워크플로 하나를 선택할 수 있습니다. 관리형 워크플로를 사용하여 파일을 처리하는 방법에 대한 자세한 내용은 [AWS Transfer Family 관리형 워크플로](#)를 참조하세요.

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. 검토 및 생성에서 옵션을 검토합니다. 경우에 따라 다음 작업을 수행합니다.

- 이들 중 하나를 편집하려면 단계 옆에 있는 편집을 선택합니다.

Note

편집하기로 선택한 단계 이후의 각 단계를 검토해야 합니다.

- 변경 사항이 없으면 서버 생성을 선택하여 서버를 생성합니다. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

서버 ID를 선택하여 방금 생성한 서버의 세부 설정을 볼 수 있습니다. 퍼블릭 IPv4 주소 열이 채워지면 제공한 탄력적 IP 주소가 서버의 엔드포인트와 성공적으로 연결됩니다.

Note

의 서버VPC가 온라인 상태인 경우 서브넷만 수정할 수 있으며 [UpdateServer](#) 를 통해서만 가능합니다API. 서버 엔드포인트의 탄력적 IP 주소를 추가하거나 변경하려면 [서버를 중지](#)해야 합니다.

서버의 엔드포인트 타입 변경

인터넷을 통해 액세스할 수 있는 기존 서버가 있는 경우(즉, 퍼블릭 엔드포인트 유형이 있는 경우) 엔드포인트를 VPC 엔드포인트로 변경할 수 있습니다.

Note

에 로 VPC 표시된 기존 서버가 있는 경우 새 VPC 엔드포인트 유형으로 수정하는 것이 VPC_ENDPOINT 좋습니다. 이 새로운 엔드포인트 유형을 사용하면 더 이상 Network Load Balancer(NLB)를 사용하여 탄력적 IP 주소를 서버의 엔드포인트와 연결할 필요가 없습니다. 또한 VPC 보안 그룹을 사용하여 서버의 엔드포인트에 대한 액세스를 제한할 수 있습니다. 그러나 필요에 따라 VPC_ENDPOINT 엔드포인트 타입을 계속 사용할 수 있습니다.

다음 절차에서는 서버가 현재 퍼블릭 엔드포인트 타입 또는 이전 VPC_ENDPOINT 타입을 사용하는 것으로 가정합니다.

서버의 엔드포인트 타입을 변경하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.

2. 탐색 창에서 서버를 선택합니다.
3. 엔드포인트 타입을 변경하려는 서버의 확인란을 선택합니다.

Important

엔드포인트를 변경하려면 먼저 서버를 중지해야 합니다.

4. 작업에서 중지를 선택합니다.
5. 표시되는 확인 대화 상자에서 중지를 선택하여 서버 중지를 확인합니다.

Note

다음 단계로 진행하기 전에 엔드포인트 세부 정보에서 서버 상태가 오프라인으로 변경될 때까지 기다리세요. 몇 분 정도 걸릴 수 있습니다. 상태 변경을 보려면 서버 페이지에서 새로 고침을 선택해야 할 수도 있습니다.

서버가 오프라인이 될 때까지는 어떤 편집도 할 수 없습니다.

6. 엔드포인트 세부 정보에서 편집을 선택합니다.
7. 엔드포인트 구성 편집에서 다음을 수행합니다.
 - a. 엔드포인트 유형 편집 에서 VPC 호스팅 을 선택합니다.
 - b. 액세스에서 다음 중 하나를 선택합니다.
 - 엔드포인트의 사설 IP 주소를 사용하는 클라이언트만 엔드포인트에 액세스할 수 있도록 하려면 내부로 설정합니다.
 - 클라이언트가 퍼블릭 인터넷을 통해 엔드포인트에 액세스할 수 있도록 하려면 인터넷 연결을 선택합니다.

Note

인터넷 연결을 선택하면 각 서브넷 또는 서브넷에서 기존 탄력적 IP 주소를 선택할 수 있습니다. 또는 VPC 콘솔(<https://console.aws.amazon.com/vpc/>)로 이동하여 하나 이상의 새 탄력적 IP 주소를 할당할 수 있습니다. 이러한 주소는 사용자가 소유 AWS 하거나 사용자가 소유할 수 있습니다. 이미 사용 중인 탄력적 IP 주소는 엔드포인트와 연결할 수 없습니다.

- c. (인터넷 연결 액세스 전용 옵션) 사용자 지정 호스트 이름의 경우 다음 중 하나를 선택합니다.

- Amazon Route 53 DNS별칭 - 사용하려는 호스트 이름이 Route 53에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 기타 DNS - 사용하려는 호스트 이름이 다른 DNS 공급자에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 없음 - 서버의 엔드포인트를 사용하고 사용자 지정 호스트 이름은 사용하지 않을 경우. 서버 호스트 이름은 `serverId.server.transfer.regionId.amazonaws.com` 형식을 취합니다.

사용자 지정 호스트 이름 사용에 대한 자세한 내용은 [사용자 지정 호스트 이름으로 작업을 참조](#)하세요.

- d. 에서 기존 VPC IDVPC를 선택하거나 생성 VPC를 선택하여 새 를 생성합니다VPC.
- e. 가용 영역 섹션에서 가용 영역 및 관련 서브넷을 최대 3개까지 선택합니다. 인터넷 연결을 선택한 경우 각 서브넷의 탄력적 IP 주소도 선택합니다.

Note

최대 3개의 가용 영역을 원하지만 사용 가능한 영역이 충분하지 않은 경우 VPC 콘솔 ()에서 해당 영역을 생성합니다<https://console.aws.amazon.com/vpc/>. 서브넷 또는 탄력적 IP 주소를 수정할 경우 서버를 업데이트하는 데 몇 분 정도 걸립니다. 서버 업데이트가 완료될 때까지는 변경 내용을 저장할 수 없습니다.

- f. 저장을 선택합니다.
8. 작업에서 시작을 선택하고 서버 상태가 온라인으로 변경될 때까지 기다립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

Note

퍼블릭 엔드포인트 유형을 VPC 엔드포인트 유형으로 변경한 경우 서버의 엔드포인트 유형이 로 변경되었습니다VPC.

기본 보안 그룹이 엔드포인트에 연결되어 있습니다. 보안 그룹을 변경하거나 추가하려면 [보안 그룹 생성](#)을 참조하세요.

VPC_ 사용 중단ENDPOINT

AWS Transfer Family 는 새 AWS 계정에 EndpointType=VPC_ENDPOINT 대해 를 사용하여 서버를 생성하는 기능을 중단합니다. 2021년 5월 19일부터 엔드포인트 유형이 인 AWS Transfer Family 서버를 소유하지 않은 AWS 계정VPC_ENDPOINT은 를 사용하여 새 서버를 생성할 수 없습니다EndpointType=VPC_ENDPOINT. VPC_ENDPOINT 엔드포인트 타입을 사용하는 서버를 이미 소유하고 있는 경우 가능한 한 빨리 EndpointType=VPC 사용을 시작하는 것이 좋습니다. 자세한 내용은[AWS Transfer Family 서버 엔드포인트 유형을 VPC_ENDPOINT에서 로 업데이트를 참조하세요 VPC](#).

2020년 초에 새 VPC 엔드포인트 타입을 출시했습니다. 자세한 내용은 의 에서 [AWS Transfer Family VPC 보안 그룹 및 탄력적 IP 주소 를 SFTP 지원합니다](#). 이 새로운 엔드포인트는 기능이 더 풍부하고 비용 효율적이며 PrivateLink 요금이 부과되지 않습니다. 자세한 내용은 [AWS PrivateLink 요금 섹션을](#) 참조하세요.

이 엔드포인트 타입은 이전 엔드포인트 타입(VPC_ENDPOINT)과 기능적으로 동일합니다. 탄력적 IP 주소를 엔드포인트에 직접 연결하여 인터넷에 연결되도록 하고 소스 IP 필터링에 보안 그룹을 사용할 수 있습니다. 자세한 내용은 [IP 허용 목록 사용을 참조하여 AWS Transfer Family for SFTP server 블로그 게시물을 보호합니다](#).

공유 환경에서 이 엔드포인트를 호스팅할 수도 있습니다VPC. 자세한 내용은 이제 에서 [AWS Transfer Family 공유 서비스 VPC 환경 지원 섹션을](#) 참조하세요.

외에도 를 사용하여 FTPS 및 를 활성화VPCEndpointType할 SFTP수 있습니다FTP. 이러한 기능 및 FTPS/FTP 지원을 에 추가할 계획은 없습니다EndpointType=VPC_ENDPOINT. 또한 AWS Transfer Family 콘솔에서 이 엔드포인트 유형을 옵션으로 제거했습니다.

Transfer Family 콘솔, , AWS CLI, API SDKs또는 를 사용하여 서버의 엔드포인트 유형을 변경할 수 있습니다 AWS CloudFormation. 서버의 엔드포인트 타입을 변경하려면 [AWS Transfer Family 서버 엔드포인트 유형을 VPC_ENDPOINT에서 로 업데이트 VPC](#)를 참조하세요.

질문이 있는 경우 AWS Support 또는 AWS 계정 팀에 문의하세요.

Note

EndpointType=VPC_에 이러한 기능 및FTPS/또는 FTP 지원을 추가할 계획은 없습니다 ENDPOINT. AWS Transfer Family 콘솔에서 더 이상 옵션으로 제공하지 않습니다.

추가 질문이 있는 경우 AWS Support 또는 계정 팀을 통해 문의할 수 있습니다.

AWS Transfer Family 서버 엔드포인트 유형을 VPC_ENDPOINT에서 로 업데이트 VPC

AWS Management Console, AWS CloudFormation 또는 Transfer Family를 사용하여 서버의 `EndpointType`에서 로 API 업데이트할 수 `VPC_ENDPOINT` 있습니다VPC. 이러한 각 방법을 사용하여 서버 엔드포인트 타입을 업데이트하는 자세한 절차와 예가 다음 섹션에 나와 있습니다. 여러 AWS 리전과 여러 AWS 계정에 서버가 있는 경우 다음 섹션에 제공된 예제 스크립트를 수정하여 업데이트해야 하는 `VPC_ENDPOINT` 유형을 사용하여 서버를 식별할 수 있습니다.

주제

- [VPC_ENDPOINT 엔드포인트 타입을 사용한 서버 식별](#)
- [를 사용하여 서버 엔드포인트 유형 업데이트 AWS Management Console](#)
- [를 사용하여 서버 엔드포인트 유형 업데이트 AWS CloudFormation](#)
- [를 EndpointType 사용하여 서버 업데이트 API](#)

VPC_ENDPOINT 엔드포인트 타입을 사용한 서버 식별

AWS Management Console을 사용하여 `VPC_ENDPOINT`를 사용하는 서버를 식별할 수 있습니다.

콘솔을 사용하여 **VPC_ENDPOINT** 엔드포인트 타입을 사용하는 서버를 식별하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택하면 해당 리전의 사용자 계정에 있는 서버 목록이 표시됩니다.
3. 엔드포인트 타입별로 서버 목록을 정렬하면 `VPC_ENDPOINT`를 사용하는 모든 서버를 볼 수 있습니다.

여러 AWS 리전 및 계정**VPC_ENDPOINT**에서 를 사용하여 서버를 식별하려면

여러 AWS 리전과 여러 AWS 계정에 서버가 있는 경우 다음 예제 스크립트를 수정하여 `VPC_ENDPOINT` 엔드포인트 유형을 사용하여 서버를 식별할 수 있습니다. 예제 스크립트는 Amazon EC2 [DescribeRegions](#) 및 Transfer Family [ListServers](#) API 호출을 사용하여 를 사용하는 모든 서버의 서버 IDs 및 리전 목록을 가져옵니다VPC_ENDPOINT. AWS 계정이 많은 경우 세션 프로파일을 사용하여 자격 증명 공급자에 인증하는 경우 읽기 전용 감사자 액세스 권한이 있는 IAM 역할을 사용하여 계정을 루프할 수 있습니다.

1. 다음은 간단한 예입니다.

```
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. 업데이트할 서버 목록을 확보한 후에는 다음 섹션에 설명된 방법 중 하나를 사용하여 EndpointType을 VPC(으)로 업데이트할 수 있습니다.

를 사용하여 서버 엔드포인트 유형 업데이트 AWS Management Console

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.
3. 엔드포인트 타입을 변경하려는 서버의 확인란을 선택합니다.

Important

엔드포인트를 변경하려면 먼저 서버를 중지해야 합니다.

4. 작업에서 중지를 선택합니다.
5. 표시되는 확인 대화 상자에서 중지를 선택하여 서버 중지를 확인합니다.

Note

다음 단계로 진행하기 전에 서버 상태가 오프라인으로 변경될 때까지 기다리세요. 몇 분 정도 걸릴 수 있습니다. 상태 변경을 보려면 서버 페이지에서 새로 고침을 선택해야 할 수도 있습니다.

6. 상태가 오프라인으로 변경되면 서버 세부 정보 페이지를 표시할 서버를 선택합니다.
7. 엔드포인트 세부 정보 섹션에서 편집을 선택합니다.
8. 엔드포인트 유형에 대해 VPC 호스팅을 선택합니다.
9. 저장을 선택합니다.
10. 작업에서 시작을 선택하고 서버 상태가 온라인으로 변경될 때까지 기다립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

를 사용하여 서버 엔드포인트 유형 업데이트 AWS CloudFormation

이 섹션에서는 를 AWS CloudFormation 사용하여 서버를 로 업데이트EndpointType하는 방법을 설명합니다VPC. 를 사용하여 배포한 Transfer Family 서버에 이 절차를 사용합니다 AWS CloudFormation. 이 예제에서는 Transfer Family 서버를 배포하는 데 사용되는 원래 AWS CloudFormation 템플릿이 다음과 같이 표시됩니다.

```
AWS::CloudFormation::Template
  AWSTemplateFormatVersion: '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

```

템플릿이 다음과 같이 변경되어 업데이트되었습니다.

- EndpointType이(가) VPC(으)로 변경되었습니다.
- AWS::EC2::VPCEndpoint 리소스가 제거됩니다.
- SecurityGroupId, SubnetIds, 및 VpcId(이)가 AWS::Transfer::Server 리소스의 EndpointDetails 섹션으로 이동되었습니다.
- EndpointDetails의 VpcEndpointId 속성이 삭제되었습니다.

업데이트된 템플릿입니다.

```

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

를 사용하여 배포된 Transfer Family 서버의 엔드포인트 유형을 업데이트하려면 AWS CloudFormation

1. 다음 단계를 사용하여 업데이트하려는 서버를 중지합니다.
 - a. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
 - b. 탐색 창에서 서버를 선택합니다.
 - c. 엔드포인트 타입을 변경하려는 서버의 확인란을 선택합니다.

 Important

엔드포인트를 변경하려면 먼저 서버를 중지해야 합니다.

- d. 작업에서 중지를 선택합니다.
- e. 표시되는 확인 대화 상자에서 중지를 선택하여 서버 중지를 확인합니다.

 Note

다음 단계로 진행하기 전에 서버 상태가 오프라인으로 변경될 때까지 기다리세요. 몇 분 정도 걸릴 수 있습니다. 상태 변경을 보려면 서버 페이지에서 새로 고침을 선택해야 할 수도 있습니다.

2. CloudFormation 스택 업데이트
 - a. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
 - b. Transfer Family 서버를 생성하는 데 사용할 스택을 선택합니다.
 - c. 업데이트를 선택합니다.
 - d. 현재 템플릿 교체를 선택합니다.
 - e. 새 템플릿을 업로드합니다. CloudFormation 변경 세트는 템플릿 변경 사항이 실행 중인 리소스에 어떤 영향을 미치는지 이해하는 데 도움이 됩니다. 이 예제에서는 Transfer 서버 리소스가 수정되고 VPCEndpoint 리소스가 제거됩니다. VPC 엔드포인트 유형 서버는 사용자를 대신하여 VPC 엔드포인트를 생성하여 원본 VPCEndpoint 리소스를 대체합니다.

새 템플릿을 업로드한 후 변경 세트는 다음과 유사합니다.

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-6a7d04e12d49ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. 스택을 업데이트합니다.
3. 스택 업데이트가 완료되면 에서 Transfer Family 관리 콘솔로 이동합니다 <https://console.aws.amazon.com/transfer/>.
4. 서버를 시작합니다. 에서 업데이트한 서버를 선택한 AWS CloudFormation 다음 작업 메뉴에서 시작을 선택합니다.

를 EndpointType 사용하여 서버 업데이트 API

[describe-server](#) AWS CLI 명령 또는 [UpdateServer](#) API 명령을 사용할 수 있습니다. 다음 예제 스크립트는 Transfer Family 서버를 중지하고, 를 업데이트하고 EndpointType, VPC_를 제거하고ENDPOINT, 서버를 시작합니다.

```
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])

```

사용자 지정 호스트 이름으로 작업

서버 호스트 이름은 사용자가 서버에 연결할 때 클라이언트에 입력하는 호스트 이름입니다. 에서 작업할 때 서버 호스트 이름에 등록된 사용자 지정 도메인을 사용할 수 있습니다 AWS Transfer Family. 예를 들어 mysftpserver.mysubdomain.domain.com 같은 사용자 지정 호스트 이름을 사용할 수 있습니다.

등록된 사용자 지정 도메인의 트래픽을 서버 엔드포인트로 리디렉션하려면 Amazon Route 53 또는 도메인 이름 시스템(DNS) 공급자를 사용할 수 있습니다. Route 53은 AWS Transfer Family 기본적으로 지원하는 DNS 서비스입니다.

주제

- [Amazon Route 53을 DNS 공급자로 사용](#)
- [다른 DNS 공급자 사용](#)
- [콘솔에서 생성하지 않은 서버의 사용자 지정 호스트 이름](#)

콘솔에서, 사용자 지정 호스트 이름을 설정하려면 다음 방법 중 하나를 선택합니다.

- Amazon Route 53 DNS별칭 - 사용하려는 호스트 이름이 Route 53에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 기타 DNS - 사용하려는 호스트 이름이 다른 DNS 공급자에 등록된 경우. 이후 호스트 이름을 입력하면 됩니다.
- 없음 - 서버의 엔드포인트를 사용하고 사용자 지정 호스트 이름은 사용하지 않을 경우.

이 옵션은 새 서버를 만들거나 기존 서버의 구성을 수정할 때 설정합니다. 새 서버 생성에 대한 자세한 정보는 [2단계: SFTP활성화된 서버 생성](#) 섹션을 참조하세요. 기존 서버 구성 편집에 대한 자세한 내용은 [서버 세부 정보 편집](#) 섹션을 참조하세요.

서버 호스트 이름에 자체 도메인을 사용하는 방법과 가 Route 53을 AWS Transfer Family 사용하는 방법에 대한 자세한 내용은 다음 섹션을 참조하세요.

Amazon Route 53을 DNS 공급자로 사용

서버를 생성할 때 Amazon Route 53을 DNS 공급자로 사용할 수 있습니다. Route 53을 도메인과 함께 사용하려면 먼저 도메인을 등록합니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 [도메인 등록 방식](#)을 참조하세요.

Route 53을 사용하여 서버에 DNS 라우팅을 제공하는 경우는 입력한 사용자 지정 호스트 이름을 AWS Transfer Family 사용하여 호스팅 영역을 추출합니다. 가 호스팅 영역을 AWS Transfer Family 추출하면 다음과 같은 세 가지 상황이 발생할 수 있습니다.

1. Route 53을 처음 사용하고 호스팅 영역이 없는 경우 새 호스팅 영역과 CNAME 레코드를 AWS Transfer Family 추가합니다. 이 CNAME 레코드의 값은 서버의 엔드포인트 호스트 이름입니다. CNAME 는 대체 도메인 이름입니다.
2. Route 53에 호스팅 영역이 있지만 CNAME 레코드가 없는 경우, AWS Transfer Family 에서 호스팅 영역에 CNAME 레코드를 추가합니다.
3. 서비스가 호스팅 영역에 존재하는 CNAME 레코드를 감지하면, CNAME 레코드가 이미 존재함을 알려주는 오류 메시지가 표시됩니다. 이 경우, CNAME 레코드 값을 서버의 호스트 이름으로 변경합니다.

Note

이 단계가 서버 생성 워크플로의 일부인 경우, 서버가 생성되고 사용자 지정 호스트 이름은 없음으로 설정됩니다.

Route 53의 호스팅 영역에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 [호스팅 영역](#)을 참조하십시오.

다른 DNS 공급자 사용

서버를 생성할 때 Amazon Route 53 이외의 DNS 공급자를 사용할 수도 있습니다. 대체 DNS 공급자를 사용하는 경우 도메인의 트래픽이 서버 엔드포인트로 전달되는지 확인합니다.

이렇게 하려면 도메인을 서버의 엔드포인트 호스트 이름으로 설정합니다. 엔드포인트 호스트 이름은 콘솔에서 형식으로 표시됩니다.

serverid.server.transfer.*region*.amazonaws.com

Note

서버에 VPC 엔드포인트가 있는 경우 호스트 이름의 형식이 위에 설명된 형식과 다릅니다. VPC 엔드포인트를 찾으려면 서버 세부 정보 페이지에서 VPC를 선택한 다음 VPC 대시보드에서 VPC 엔드포인트 ID를 선택합니다. 엔드포인트는 나열된 엔드포인트의 DNS 이름입니다.

콘솔에서 생성하지 않은 서버의 사용자 지정 호스트 이름

AWS 클라우드 개발 키트 (AWS CDK) AWS CloudFormation, 또는 를 사용하여 서버를 생성할 때 해당 서버에 사용자 지정 호스트 이름이 있어야 하는 경우 태그를 추가CLI해야 합니다. 콘솔을 사용하여 Transfer Family 서버를 생성하는 경우 태깅이 자동으로 수행됩니다.

Note

또한 도메인에서 서버 엔드포인트로 트래픽을 리디렉션하는 DNS 레코드를 생성해야 합니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 [레코드 작업](#)을 참조하십시오.

사용자 지정 호스트 이름에 사용할 키:

- 콘솔에 사용자 지정 호스트 이름을 표시하려면 transfer:customHostname를 추가합니다.
- Route 53을 DNS 공급자로 사용하는 경우 를 추가합니다transfer:route53HostedZoneId. 이 태그는 사용자 지정 호스트 이름을 Route 53 호스팅 영역 ID에 연결합니다.

사용자 지정 호스트 이름을 추가하려면 다음 CLI 명령을 실행합니다.

```
aws transfer tag-resource --arn arn:aws:transfer:region:AWS #:server/server-ID --tags
Key=transfer:customHostname,Value="custom-host-name"
```

예:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Route 53을 사용하는 경우 다음 명령을 실행하여 사용자 지정 호스트 이름을 Route 53 호스팅 영역 ID에 연결합니다.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

예:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

이전 명령의 샘플 값을 가정하고 다음 명령을 실행하여 태그를 봅니다.

```
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

퍼블릭, 호스팅 영역 및 IDs 해당 영역은 Amazon Route 53에서 사용할 수 있습니다.

에 로그인 AWS Management Console 하고 에서 Route 53 콘솔을 엽니다 <https://console.aws.amazon.com/route53/>.

클라이언트를 사용하여 서버 엔드포인트를 통한 파일 전송

클라이언트에서 전송 작업을 지정하여 AWS Transfer Family 서비스를 통해 파일을 전송합니다. 는 다음 클라이언트를 AWS Transfer Family 지원합니다.

- 프로토콜 버전 3을 지원합니다SFTP.
- OpenSSH(macOS 및 Linux)

Note

이 클라이언트는 Secure Shell(SSH) 파일 전송 프로토콜()에 대해 활성화된 서버에서만 작동합니다SFTP.

- WinSCP(Microsoft Windows만 해당)
- Cyberduck (Windows, macOS, 및 Linux)
- FileZilla (Windows, macOS 및 Linux)

모든 클라이언트에는 다음과 같은 제한 사항이 적용됩니다:

- 연결당 최대 동시 다중 SFTP 세션 수는 10개입니다.
- Amazon S3 및 AmazonEFS(NFSv4프로토콜로 인해)은 파일 이름이 UTF-8 인코딩이어야 합니다. 다른 인코딩을 사용하면 예상치 못한 결과가 발생할 수 있습니다. Amazon S3의 경우, [객체 키 명칭 지정 가이드라인](#)을 참조하세요.
- SSL (FTPS)를 통한 파일 전송 프로토콜의 경우 명시적 모드만 지원됩니다. 묵시적 모드는 지원되지 않습니다.
- 파일 전송 프로토콜(FTP) 및 FTPS의 경우 수동 모드만 지원됩니다.
- FTP 및 의 경우 STREAM 모드FTPS만 지원됩니다.
- FTP 및 의 경우 이미지/바이너리 모드FTPS만 지원됩니다.
- FTP 및 의 경우 FTPS TLS - 데이터 연결에 TLS 대한 PROT C(보호되지 않음)가 기본값이지만 프로토콜에서는 PROT AWS Transfer Family FTPS C가 지원되지 않습니다. 따라서 의 경우 데이터 작업을 수락하려면 PROT P를 발급FTPS해야 합니다.

- Amazon S3를 서버 스토리지로 사용하고 있고 클라이언트에 단일 전송에 복수 연결을 사용하는 옵션이 포함되어 있는 경우, 해당 옵션을 비활성화해야 합니다. 그렇지 않으면 대용량 파일 업로드가 예상치 못한 방식으로 실패할 수 있습니다. Amazon을 EFS 스토리지 백엔드로 사용하는 경우는 단일 전송에 대해 여러 연결을 EFS 지원합니다.

다음은 FTP 및 에 사용할 수 있는 명령 목록입니다FTPS.

가용 명령					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTS	QUIT	STAT	USER

Note

APPE는 지원되지 않습니다.

의 경우 SFTPA Amazon Elastic File System(Amazon)을 사용하는 서버에서 논리적 홈 디렉터리를 사용하는 사용자는 현재 다음 작업이 지원되지 않습니다EFS.

지원되지 않는 SFTP 명령			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH요청된 파일 이 symlink인 경우 _FXP_STAT	SSH요청된 경로 에 symlink 구성 요 소가 포함된 경우 _FXP_REALPATH

퍼블릭-프라이빗 키 쌍을 생성합니다.

파일을 전송하려면 먼저 퍼블릭-프라이빗 키 쌍을 사용할 수 있어야 합니다. 이전에 키 쌍을 생성하지 않은 경우, [서비스 관리 사용자를 위한 SSH 키 생성](#)를 참조하세요.

주제

- [사용 가능한 SFTP/FTPS/FTP 명령](#)
- [Amazon VPC 엔드포인트 찾기](#)
- [setstat 오류 방지](#)
- [열기 사용SSH](#)
- [Win 사용SCP](#)
- [Cyberduck 사용하기](#)
- [사용 FileZilla](#)
- [Perl 클라이언트 사용](#)
- [업로드 후 처리](#)

사용 가능한 SFTP/FTPS/FTP 명령

다음 표에서는 AWS Transfer Family, SFTP/FTPS, FTP 프로토콜에 대해 사용 가능한 명령을 설명합니다.

Note

이 표에는 버킷과 객체만 지원하는 Amazon S3의 파일 및 디렉터리가 나와 있습니다. 계층 구조는 없습니다. 그러나 객체 키 명칭에 접두사를 사용하여 계층 구조를 암시하고 폴더와 유사한 방식으로 데이터를 구성할 수 있습니다. 이 동작은 Amazon Simple Storage Service 사용자가이드에서 [객체 메타데이터 작업](#)에 설명되어 있습니다.

SFTP/FTPS/FTP 명령

Command	Amazon S3	Amazon EFS
cd	지원	지원
chgrp	지원되지 않음	지원(root 또는 owner만 해당)

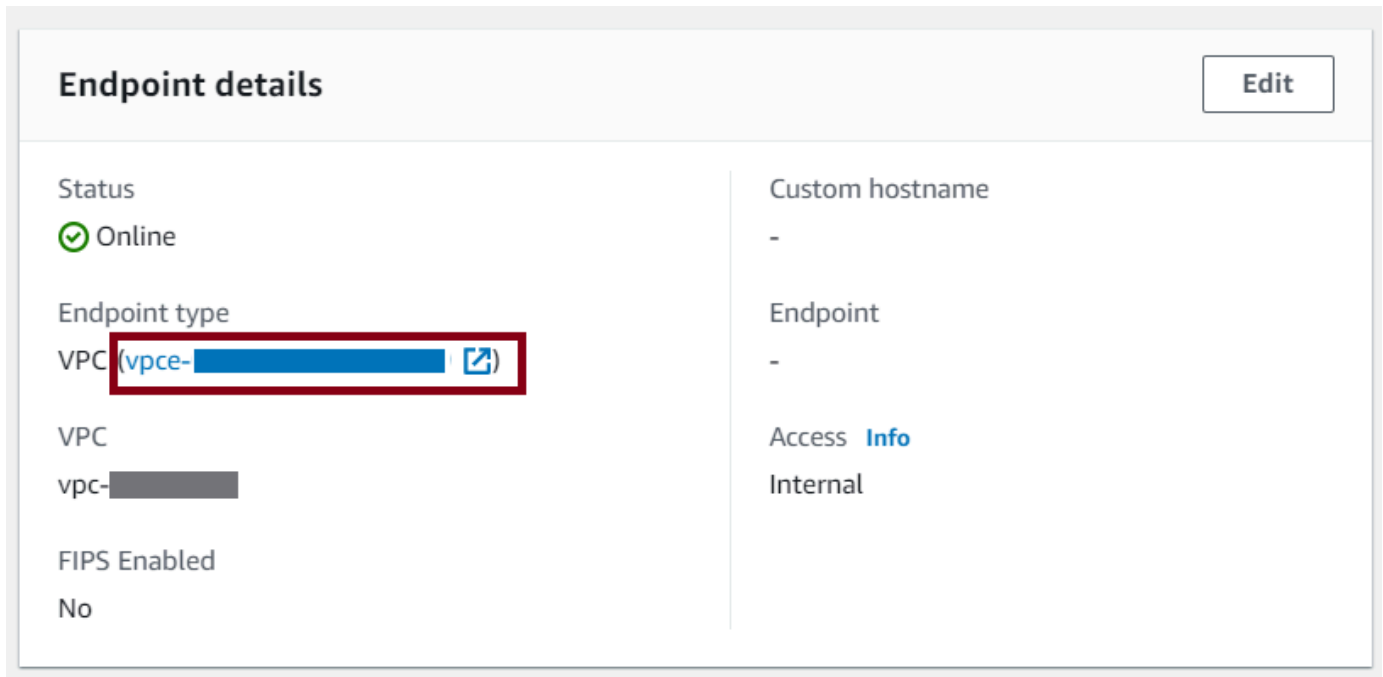
Command	Amazon S3	Amazon EFS
chmod	지원되지 않음	지원(root만 해당)
chmtime	지원되지 않음	지원
chown	지원되지 않음	지원(root만 해당)
get	지원	지원(심볼 링크 해결 포함)
ln -s	지원되지 않음	지원
ls/dir	지원	지원
mkdir	지원	지원
put	지원	지원
pwd	지원	지원
rename	파일에만 지원됨	지원 Note 기존 파일 또는 디렉터리를 덮어쓰는 명령 변경은 지원되지 않습니다.
rm	지원	지원
rmdir	지원(빈 디렉터리만 해당)	지원
version	지원	지원

Amazon VPC 엔드포인트 찾기

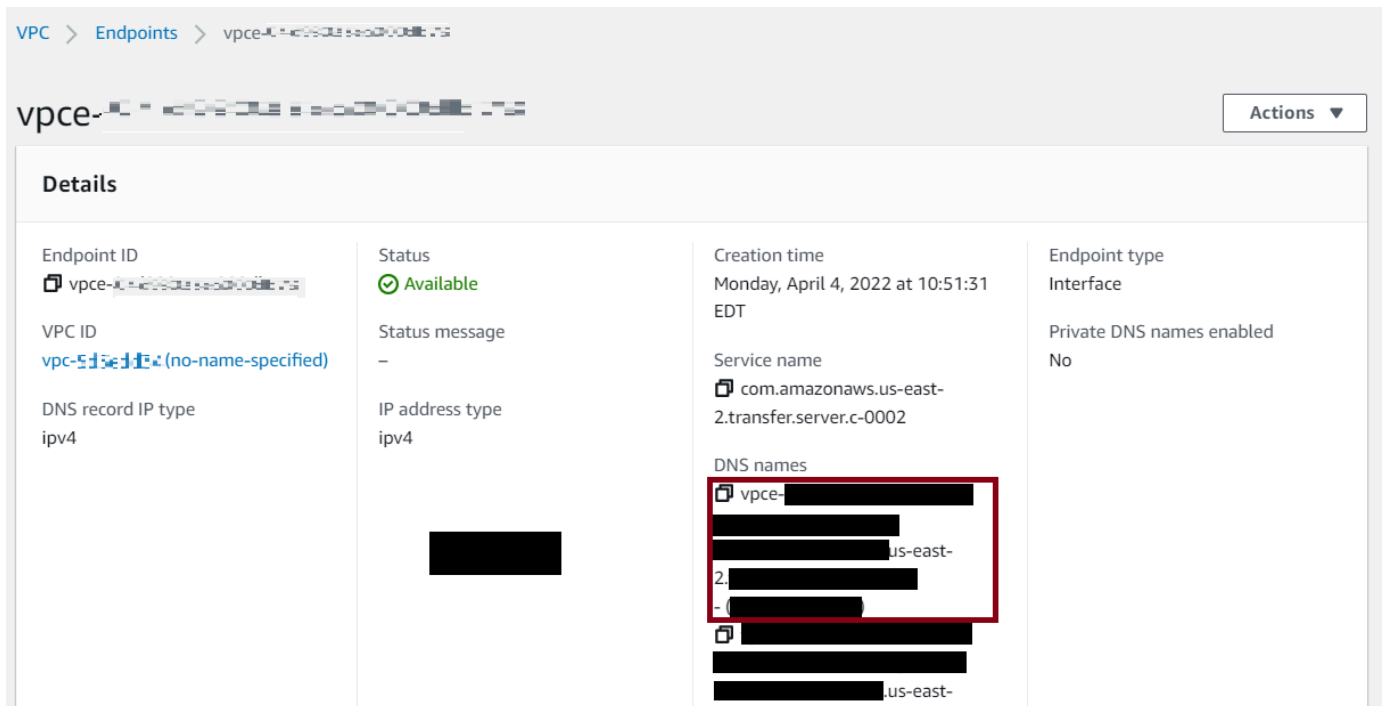
Transfer Family 서버의 엔드포인트 유형이 인 경우 파일 전송에 사용할 엔드포인트를 VPC식별하는 방법은 간단하지 않습니다. 이 경우 다음 절차에 따라 Amazon VPC 엔드포인트를 찾습니다.

Amazon VPC 엔드포인트 찾기

1. 서버의 세부 정보 페이지로 이동합니다.
2. 엔드포인트 세부 정보 창에서 를 선택합니다VPC.



3. Amazon VPC 대시보드에서 VPC 엔드포인트 ID 를 선택합니다.
4. DNS 이름 목록에서 서버 엔드포인트는 나열된 첫 번째 엔드포인트입니다.



setstat 오류 방지

일부 SFTP 파일 전송 클라이언트는 파일을 업로드할 SETSTAT 때와 같은 명령을 사용하여 타임스탬프 및 권한을 포함하여 원격 파일의 속성을 변경하려고 시도할 수 있습니다. 그러나 이러한 명령은 Amazon S3와 같은 객체 스토리지 시스템과 호환되지 않습니다. 이러한 비호환성으로 인해 이러한 클라이언트에서 파일을 업로드하면 파일이 성공적으로 업로드된 경우에도 오류가 발생할 수 있습니다.

- CreateServer 또는 UpdateServer 를 호출할 때 ProtocolDetails 옵션을 API 사용하여 클라이언트가 S3 버킷 SETSTAT에 업로드하는 파일에 를 사용하려고 할 때 생성되는 오류를 SetStatOption 무시합니다.
- Transfer Family 서버가 SETSTAT 명령을 무시ENABLE_NO_OP하도록 값을 로 설정하고 SFTP 클라이언트를 변경할 필요 없이 파일을 업로드합니다.
- SetStatOption ENABLE_NO_OP 설정은 오류를 무시하지만 로그에서 CloudWatch 로그 항목을 생성하므로 클라이언트가 SETSTAT 전화를 거는 시기를 확인할 수 있습니다.

이 옵션에 대한 자세한 API 내용은 섹션을 참조하세요 [ProtocolDetails](#).

열기 사용SSH

다음 지침에 따라 열기 를 사용하여 명령줄에서 파일을 전송합니다SSH.

Note

이 클라이언트는 SFTP활성화된 서버에서만 작동합니다.

OpenSSH 명령줄 유틸리티를 AWS Transfer Family 사용하여 파일을 전송하려면

1. Linux, macOS 또는 Windows에서 명령 터미널을 엽니다.
2. 프롬프트에서 다음 명령을 입력합니다.

```
sftp -i transfer-key sftp_user@service_endpoint
```

앞의 명령에서 *sftp_user* 는 사용자 이름이고 *transfer-key*는 SSH 프라이빗 키입니다. 여기서 *service_endpoint*는 선택한 서버의 AWS Transfer Family 콘솔에 표시된 서버의 엔드포인트입니다.

Note

이 명령은 기본 `ssh_config` 파일에 있는 설정을 사용합니다. 이전에 이 파일을 편집하지 않은 한 는 포트 22를 SFTP 사용합니다. 다음과 같이 명령에 **-P** 플래그를 추가하여 다른 포트(예: 2222)를 지정할 수 있습니다.

```
sftp -P 2222 -i transfer-key sftp_user@service_endpoint
```

또는 포트 2222를 항상 사용하려는 경우 `ssh_config` 파일의 기본 포트를 업데이트할 수 있습니다.

sftp 프롬프트가 나타날 것입니다.

3. (옵션) 사용자의 홈 디렉터리를 보려면 sftp 프롬프트에 다음 명령을 입력합니다.

```
pwd
```

4. 파일 시스템에서 Transfer Family 서버로 파일을 업로드하려면 `put` 명령을 사용합니다. 예를 들어 업로드하려면 `hello.txt` (파일이 파일 시스템의 현재 디렉터리에 있다고 간주) sftp 프롬프트에서 다음 명령을 실행합니다.

```
put hello.txt
```

파일 전송이 진행 중이거나 완료되었음을 나타내는, 다음과 비슷한 메시지가 표시됩니다.

```
Uploading hello.txt to /my-bucket/home/sftp_user/hello.txt
```

```
hello.txt 100% 127 0.1KB/s 00:00
```

Note

서버가 생성된 후 환경의 DNS 서비스에서 서버 엔드포인트 호스트 이름을 확인하는 데 몇 분 정도 걸릴 수 있습니다.

Win 사용SCP

다음 지침에 따라 Win 을 사용하여 명령줄에서 파일을 전송합니다SCP.

Note

WinSCP 5.19를 사용하는 경우 자격 AWS 증명을 사용하여 Amazon S3에 직접 연결하고 파일을 업로드/다운로드할 수 있습니다. 자세한 내용은 [Amazon S3 서비스에 연결](#)을 참조하세요.

Win을 AWS Transfer Family 사용하여 파일을 전송하려면SCP

1. WinSCP 클라이언트를 엽니다.
2. 로그인 대화 상자의 파일 프로토콜 에서 프로토콜: SFTP 또는 를 선택합니다FTP.

암호화에 대해 FTP를 선택한 경우 다음 중 하나를 선택합니다.

- 에 대한 암호화 없음 FTP
 - TLS/SSL 에 대한 명시적 암호화 FTPS
3. 호스트 명칭에 서버 엔드포인트를 입력합니다. 서버 엔드포인트는 서버 세부 정보 페이지에 있습니다. 자세한 내용은 [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#) 단원을 참조하십시오.

Note

서버에서 VPC 엔드포인트를 사용하는 경우 섹션을 참조하세요[Amazon VPC 엔드포인트 찾기](#).

4. 포트 번호에 다음을 입력합니다:
 - SFTP용 22
 - 21 FTP/용FTPS
5. 사용자 이름에는 특정 ID 공급자용으로 생성한 사용자 이름을 입력합니다.

Note

사용자 이름은 자격 증명 공급자에 대해 생성하거나 구성한 사용자 중 하나여야 합니다. 는 다음 자격 증명 공급자를 AWS Transfer Family 제공합니다.

- [서비스 관리형과 작업](#)
- [AWS 디렉터리 서비스 자격 증명 공급자 사용](#)
- [사용자 지정 자격 증명 공급자와 작업](#)

6. 고급을 선택하여 고급 사이트 설정 대화 상자를 엽니다. SSH 섹션에서 인증을 선택합니다.
7. 프라이빗 키 파일의 경우 파일 시스템에서 SSH 프라이빗 키 파일을 찾아 선택합니다.

 Note

WinSCP이 SSH 프라이빗 키를 PPK 형식으로 변환하겠다고 제안하는 경우 확인을 선택합니다.

8. OK(확인)을 선택해 Login(로그인) 대화 상자로 돌아간 다음 Save(저장)을 선택합니다.
9. 다음과 같은 Save session as site(세션을 사이트로 저장) 대화 상자에서 OK(확인)을 선택해 연결 설정을 완료합니다.
10. 로그인 대화 상자에서 도구를 선택한 다음 기본 설정을 선택합니다.
11. 환경 설정 대화 상자의 전송에서 Endurance를 선택합니다.

임시 파일 명칭으로 전송 재개/전송 활성화 옵션에 대해 비활성화를 선택합니다.

 Note

이 옵션을 활성화한 상태로 두면 업로드 비용이 증가하여 업로드 성능이 크게 저하됩니다. 또한 대용량 파일 업로드가 실패할 수도 있습니다.

12. 전송의 경우, 배경을 선택하고 단일 전송에 복수 연결 사용 확인란의 선택을 취소합니다.

 Note

이 옵션을 선택한 상태로 두면 대용량 파일 업로드가 예상치 못한 방식으로 실패할 수 있습니다. 예를 들어 Amazon S3 요금이 발생하는 분리된 멀티파트 업로드를 생성할 수 있습니다. 조용한 데이터 손상도 발생할 수 있습니다.

13. 파일 전송을 실행합니다.

메서드를 사용하여 drag-and-drop 대상 창과 소스 창 간에 파일을 복사할 수 있습니다. 도구 모음 아이콘을 사용하여 Win 에서 파일의 속성을 업로드, 다운로드, 삭제, 편집 또는 수정할 수 있습니다 SCP.

Note

Amazon을 스토리지EFS로 사용하는 경우에는 이 참고 사항이 적용되지 않습니다. 타임스탬프를 포함하여 원격 파일의 속성을 변경하려는 명령은 Amazon S3와 같은 객체 스토리지 시스템과 병립되지 않습니다. 따라서 Amazon S3를 스토리지에 사용하는 경우 파일 전송을 수행하기 전에 WinSCP 타임스탬프 설정을 비활성화해야 합니다(또는 에 설명된 SetStatOption 대로 사용 [setstat 오류 방지](#)). 이렇게 하려면 WinSCP Transfer 설정 대화 상자에서 권한 업로드 설정 옵션과 타임스탬프 일반 보존 옵션을 비활성화합니다.

Cyberduck 사용하기

아래의 지침을 이용해 Cyberduck을 이용하는 명령줄로 파일을 전송하세요.

Cyberduck을 AWS Transfer Family 사용하여 파일을 전송하려면

1. [Cyberduck](#) 클라이언트를 엽니다.
2. 연결 열기를 선택합니다.
3. 연결 열기 대화 상자에서 (SFTP 파일 전송 프로토콜), SSHFTP-(SSL명시적 AUTH TLS) 또는 FTP (파일 전송 프로토콜) 프로토콜을 선택합니다.
4. 서버에 서버 엔드포인트를 입력합니다. 서버 엔드포인트는 서버 세부 정보 페이지에 있습니다. 자세한 내용은 [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#) 단원을 참조하십시오.

Note

서버에서 VPC 엔드포인트를 사용하는 경우 섹션을 참조하세요 [Amazon VPC 엔드포인트 찾기](#).

5. 포트 번호에 다음을 입력합니다:
 - SFTP용 **22**
 - **21** FTP/용FTPS
6. 사용자 이름에 [서버 엔드포인트에 대한 사용자 관리](#)에서 생성한 사용자 이름을 입력합니다.
7. SFTP 를 선택한 경우 SSH 프라이빗 키 에서 SSH 프라이빗 키를 선택하거나 입력합니다.
8. 연결을 선택합니다.
9. 파일 전송을 실행합니다.

파일 위치에 따라, 다음 중 하나를 수행하세요.

- 로컬 디렉터리(소스)에서 전송할 파일을 선택하고, Amazon S3 디렉터리(대상)로 끌어다 놓습니다.
- Amazon S3 디렉터리(소스)에서 전송할 파일을 선택하고, 로컬 디렉터리(대상)로 끌어다 놓습니다.

사용 FileZilla

다음 지침에 따라 를 사용하여 파일을 전송합니다 FileZilla.

파일 전송 FileZilla 을 위해 설정하려면

1. FileZilla 클라이언트를 엽니다.
2. 파일을 선택한 다음 사이트 관리자를 선택합니다.
3. 사이트 관리자 대화 상자에서 새 사이트를 선택합니다.
4. 일반 탭의 프로토콜 에서 프로토콜: SFTP 또는 를 선택합니다FTP.

암호화에 대해 FTP를 선택한 경우 다음 중 하나를 선택합니다.

- 일반FTP(비보안)만 사용 - FTP
 - 사용 가능한 TLS 경우 에 명시적 FTP를 사용합니다. FTPS
5. 호스트 명칭에는 사용 중인 프로토콜을 입력한 다음 서버 엔드포인트를 입력합니다. 서버 엔드포인트는 서버 세부 정보 페이지에 있습니다. 자세한 내용은 [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#) 단원을 참조하십시오.

Note

서버에서 VPC 엔드포인트를 사용하는 경우 섹션을 참조하세요 [Amazon VPC 엔드포인트 찾기](#).

- 를 사용하는 경우 다음을 SFTP입력합니다. `sftp://hostname`
- 를 사용하는 경우 다음을 FTPS입력합니다. `ftps://hostname`

교체해야 합니다.`hostname` 실제 서버 엔드포인트를 사용합니다.

6. 포트 번호에 다음을 입력합니다:

- SFTP용 **22**
- **21** FTP/용FTPS

7. SFTP 이 선택된 경우 로그인 유형 에서 키 파일 을 선택합니다.

키 파일 에서 SSH 프라이빗 키를 선택하거나 입력합니다.

8. 사용자 이름에 [서버 엔드포인트에 대한 사용자 관리](#)에서 생성한 사용자 이름을 입력합니다.

9. 연결을 선택합니다.

10. 파일 전송을 실행합니다.

Note

진행 중인 파일 전송을 중단하면 Amazon S3 버킷에 부분 객체를 AWS Transfer Family 쓸 수 있습니다. 업로드를 중단했다면, Amazon S3 버킷의 파일 크기가 소스 개체의 파일 크기와 동일한지 확인한 후 다음 단계로 계속합니다.

Perl 클라이언트 사용

perl 클라이언트를 NET::SFTP::Foreign 사용하는 경우 를 queue_size로 설정해야 합니다1. 예:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

Note

이 해결 방법은 [1.92.02](#) 이전의 Net::SFTP::Foreign을 위해 필요합니다.

업로드 후 처리

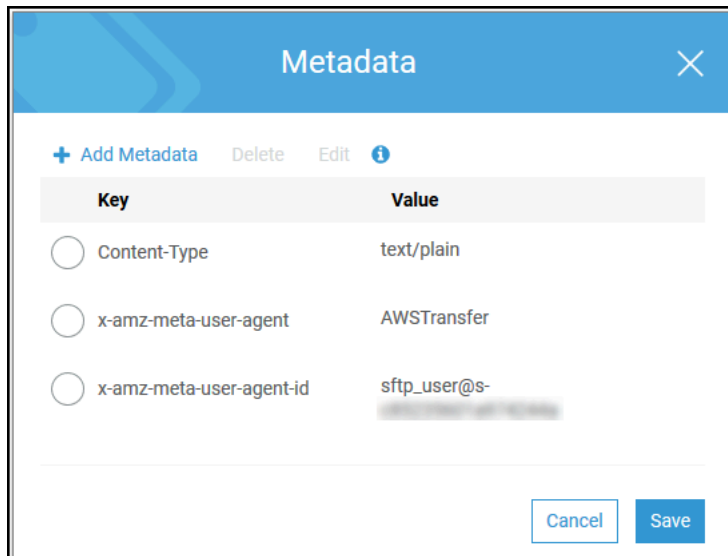
Amazon S3 객체 메타데이터 및 이벤트 알림을 비롯한 업로드 후 처리 정보를 볼 수 있습니다.

주제

- [Amazon S3 객체 메타데이터](#)
- [Amazon S3 이벤트 알림](#)

Amazon S3 객체 메타데이터

객체 메타데이터의 일부로, 'x-amz-meta-user-agent'의 값은 AWSTransfer(이)고 x-amz-meta-user-agent-id의 값은 username@server-id(이)라는 키가 표시됩니다. username은(는) 파일을 업로드한 Transfer Family 사용자이며, server-id은(는) 업로드에 사용되는 서버입니다. 이 정보는 Lambda 함수 내의 S3 객체에 대한 [HeadObject](#) 작업을 사용하여 액세스할 수 있습니다.



The screenshot shows the 'Metadata' window in the AWS console. It has a blue header with a close button. Below the header are buttons for '+ Add Metadata', 'Delete', 'Edit', and an information icon. A table lists metadata items with radio buttons in the first column. The table has two columns: 'Key' and 'Value'.

Key	Value
☐ Content-Type	text/plain
☐ x-amz-meta-user-agent	AWSTransfer
☐ x-amz-meta-user-agent-id	sftp_user@s-

At the bottom right, there are 'Cancel' and 'Save' buttons.

Amazon S3 이벤트 알림

Transfer Family를 사용하여 S3 버킷에 객체를 업로드하면 RoleSessionName이(가) [S3 이벤트 알림 구조](#)의 요청자 필드에 [AWS:Role Unique Identifier]/username.sessionid@server-id와(과) 같이 포함됩니다. 예를 들어, 다음은 S3 버킷으로 복사된 파일에 대한 S3 액세스 로그의 샘플 요청자 필드 콘텐츠입니다.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

위의 요청자 필드에는 라는 IAM 역할이 표시됩니다IamRoleName. S3 이벤트 알림 구성에 대한 자세한 설명은 Amazon Simple Storage Service 개발자 가이드의 [Configuring Amazon S3 이벤트 알림](#)을 참조하세요. AWS Identity and Access Management (IAM) 역할 고유 식별자에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [고유 식별자](#)를 참조하세요.

서버 엔드포인트에 대한 사용자 관리

다음 섹션에서는 AWS Transfer Family또는 사용자 지정 자격 증명 공급자를 사용하여 AWS Directory Service for Microsoft Active Directory 사용자를 추가하는 방법에 대한 정보를 찾을 수 있습니다.

서비스 관리형 자격 증명 타입을 사용한다면, 사용자를 파일 전송 프로토콜 지원 서버에 추가해야 합니다. 이 작업을 할 때 각 사용자 이름은 서버 내에서 고유해야 합니다.

각 사용자의 속성의 일부로 해당 사용자의 Secure Shell(SSH) 퍼블릭 키도 저장합니다. 이는 이 절차에서 사용하는 키 기반 인증에 필요합니다. 프라이빗 키는 사용자의 컴퓨터에 로컬로 저장됩니다. 사용자가 클라이언트를 사용하여 서버에 인증 요청을 보내면 서버는 먼저 사용자가 연결된 SSH 프라이빗 키에 액세스할 수 있는지 확인합니다. 그러면 서버가 사용자를 성공적으로 인증합니다.

또한 사용자의 홈 디렉터리 또는 랜딩 디렉터리를 지정하고 사용자에게 AWS Identity and Access Management (IAM) 역할을 할당합니다. 원한다면 세션 정책을 제공해 사용자 액세스를 Amazon S3 버킷의 홈 디렉터리로 제한할 수도 있습니다.

Important

AWS Transfer Family 는 1자 또는 2자 길이의 사용자 이름이 SFTP 서버에 인증되는 것을 차단합니다. 또한 root 사용자 이름도 차단합니다.
그 이유는 암호 스캐너의 악의적인 로그인 시도가 대량으로 발생하기 때문입니다.

AmazonEFS과 Amazon S3 비교

각 스토리지 옵션의 특징:

- 액세스를 제한하려면: Amazon S3는 세션 정책을 지원하고, Amazon은 POSIX 사용자, 그룹 및 보조 그룹을 EFS 지원합니다. IDs
- 둘 다 퍼블릭/프라이빗 키 지원
- 둘 다 홈 디렉터리 지원
- 둘 다 논리적 디렉터리 지원

Note

Amazon S3의 경우 논리적 디렉터리에 대한 대부분의 지원은 API를 통해 이루어집니다. CLI, 콘솔의 제약 확인란을 사용하여 사용자를 홈 디렉터리에 잠글 수 있지만 가상 디렉터리 구조를 지정할 수는 없습니다.

논리적 디렉터리

사용자의 논리적 디렉터리 값을 지정하는 경우 사용하는 파라미터는 사용자 타입에 따라 달라집니다.

- 서비스 관리 사용자의 경우 HomeDirectoryMappings에서 논리적 디렉터리 값을 제공하세요.
- 사용자 지정 자격 증명 공급자 사용자의 경우 에 논리적 디렉터리 값을 제공합니
다HomeDirectoryDetails.

주제

- [서비스 관리형과 작업](#)
- [AWS 디렉터리 서비스 자격 증명 공급자 사용](#)
- [사용자 지정 자격 증명 공급자와 작업](#)

서비스 관리형과 작업

서버의 도메인 설정에 따라 Amazon S3 또는 Amazon EFS 서비스 관리형 사용자를 서버에 추가할 수 있습니다. 자세한 내용은 [SFTP, FTPS 또는 FTP 서버 엔드포인트 구성](#) 단원을 참조하십시오.

서비스 관리 사용자를 프로그래밍 방식으로 추가하려면 [CreateUser](#)의 [예제](#)를 참조하세요API.

Note

서비스 관리형 사용자의 경우 논리적 디렉터리 항목은 2,000개로 제한됩니다. 논리적 디렉터리 사용에 대한 자세한 내용은 섹션을 참조하세요 [논리적 디렉터리를 사용하여 Transfer Family 디렉터리 구조를 단순화합니다..](#)

주제

- [Amazon S3 서비스 관리 사용자 추가](#)
- [Amazon EFS 서비스 관리형 사용자 추가](#)
- [서비스 관리 사용자 관리](#)

Amazon S3 서비스 관리 사용자 추가

Note

교차 계정 Amazon S3 버킷을 구성하려면 이 지식 센터 문서: [다른 AWS 계정에 있는 Amazon Simple Storage Service 버킷을 사용하도록 AWS Transfer Family 서버를 구성하려면 어떻게 해야 하나요?](#)에 설명된 단계를 따르세요.

Amazon S3 서비스 관리 사용자를 서버에 추가하려면

1. 에서 AWS Transfer Family 콘솔을 연 <https://console.aws.amazon.com/transfer/> 다음 탐색 창에서 서버를 선택합니다.
2. 서버 페이지에서 사용자를 추가할 서버의 확인란을 선택합니다.
3. 사용자 추가를 선택합니다.
4. 사용자 구성 섹션의 사용자 이름에 사용자 이름을 입력합니다. 이 사용자 이름은 3~100자여야 합니다. 사용자 이름에는 a~z, A~Z, 0~9, 밑줄(_)와 하이픈(-), 마침표(.) 및 골뱅이 기호(@) 등의 문자를 사용할 수 있습니다. 사용자 이름은 하이픈 '-', 마침표 '.' 및 "@" 기호로 시작할 수 없습니다.
5. 액세스 에서 Amazon S3 버킷에 대한 액세스를 제공하는 이전에 생성한 IAM 역할을 선택합니다.

의 절차를 사용하여 이 IAM 역할을 생성했습니다 [IAM 역할 및 정책 생성](#). 이 IAM 역할에는 Amazon S3 버킷에 대한 액세스를 제공하는 IAM 정책이 포함됩니다. 또한 다른 IAM 정책에 정의된 AWS Transfer Family 서비스와의 신뢰 관계도 포함됩니다. 사용자를 위한 세분화된 액세스 제어が必要な 경우 [AWS Transfer Family 및 Amazon S3 블로그 게시물을 사용하여 데이터 액세스 제어 강화](#)를 참조하세요.

6. (옵션) 정책에서 다음 중 하나를 선택합니다.
 - None(없음)
 - 기존 정책
 - 에서 정책 선택IAM: 기존 세션 정책을 선택할 수 있습니다. 정책의 세부 정보가 포함된 JSON 객체를 보려면 보기를 선택합니다.
 - 홈 폴더 기반 정책 자동 생성: 세션 정책을 자동으로 생성합니다. 정책의 세부 정보가 포함된 JSON 객체를 보려면 보기를 선택합니다.

Note

홈 폴더를 기반으로 정책 자동 생성을 선택하는 경우 이 사용자에게 대해 제약을 선택하지 마세요.

세션 정책에 대한 자세한 설명은 [IAM 역할 및 정책 생성](#) 섹션을 참조하세요. 세션 정책 생성에 대한 자세한 설명은 [Amazon S3 버킷을 위한 세션 정책 생성](#) 섹션을 참조하세요.

7. 홈 디렉터리 에서 Amazon S3 버킷을 선택하여 를 사용하여 전송할 데이터를 저장합니다 AWS Transfer Family. 사용자가 클라이언트를 이용해 로그인하면 도착하게 되는 home 디렉터리의 경로를 입력합니다.

이 파라미터를 입력하지 않으면 Amazon 버킷의 root 디렉토리를 사용합니다. 이 경우 IAM 역할이 이 root 디렉토리에 대한 액세스 권한을 제공하는지 확인하세요.

Note

사용자의 사용자 이름을 포함하는 디렉토리 경로 선택을 권장합니다. 세션 정책을 효과적으로 사용할 수 있습니다. 세션 정책은 사용자의 home 디렉토리에 대한 Amazon S3 버킷에서의 사용자 액세스를 제한합니다.

8. (옵션) 제약의 경우, 사용자가 해당 폴더 외부에 액세스할 수 없고 Amazon S3 버킷 또는 폴더 이름을 볼 수 없도록 확인란을 선택합니다.

Note

사용자에게 홈 디렉토리를 할당하고 사용자를 해당 홈 디렉터리로 제한하면 지정된 폴더에 대한 사용자 액세스를 차단하기에 충분해야 합니다. 추가 통제를 적용해야 하는 경우 세션 정책을 사용하세요.
이 사용자에게 대해 제약을 선택하면 홈 폴더가 제한된 사용자에게 대해 정의된 값이 아니기 때문에 홈 폴더 기반 정책 자동 생성을 선택할 수 없습니다.

9. SSH 퍼블릭 키의 경우 SSH 키 페어의 퍼블릭 SSH 키 부분을 입력합니다.

서비스에서 사용자의 키를 확인해야 새 사용자를 추가할 수 있습니다.

Note

SSH 키 페어를 생성하는 방법에 대한 지침은 섹션을 참조하세요 [서비스 관리 사용자를 위한 SSH 키 생성](#).

10. (옵션) 키와 값에 하나 이상의 태그를 키-값 쌍으로 입력하고 태그 추가를 선택합니다.
11. 추가를 선택해 새 사용자를 원하는 서버에 추가합니다.

새 사용자는 서버 세부 정보 페이지의 사용자 섹션에 나타납니다.

다음 단계 - 그 다음 단계에서는 [클라이언트를 사용하여 서버 엔드포인트를 통한 파일 전송](#)로 계속 진행하세요.

Amazon EFS 서비스 관리형 사용자 추가

AmazonEFS은 휴대용 운영 체제 인터페이스(POSIX) 파일 권한 모델을 사용하여 파일 소유권을 나타냅니다.

- Amazon EFS 파일 소유권에 대한 자세한 내용은 [Amazon EFS 파일 소유권](#)을 참조하세요.
- EFS 사용자의 디렉터리 설정에 대한 자세한 내용은 섹션을 참조하세요 [Transfer Family용 Amazon EFS 사용자 설정](#).

Amazon EFS 서비스 관리형 사용자를 서버에 추가하려면

1. 에서 AWS Transfer Family 콘솔을 연 <https://console.aws.amazon.com/transfer/> 다음 탐색 창에서 서버를 선택합니다.
2. 서버 페이지에서 사용자를 추가할 Amazon EFS 서버를 선택합니다.
3. 사용자 추가를 선택하여 사용자 추가 페이지를 표시합니다.
4. 사용자 구성 섹션에서 다음 설정을 구성합니다.
 - a. 이 사용자 이름은 최소 3글자에서 최대 100자여야 합니다. 사용자 이름에는 a~z, A~Z, 0~9, 밑줄(_)와 하이픈(-), 마침표(.) 및 골뱅이 기호(@) 등의 문자를 사용할 수 있습니다. 사용자 이름은 하이픈 '-', 마침표 '.' 및 "@" 기호로 시작할 수 없습니다.
 - b. 사용자 ID 및 그룹 ID의 경우, 다음을 참고하세요:
 - 처음 생성하는 사용자의 경우, 그룹 ID와 사용자 ID 모두에 대한 0의 값을 입력하는 것이 좋습니다. 이렇게 하면 Amazon EFS에 대한 사용자 관리자 권한이 부여됩니다.
 - 추가 사용자의 경우 사용자의 POSIX 사용자 ID와 그룹 ID를 입력합니다. 이는 사용자가 수행하는 모든 Amazon Elastic File System 작업에 IDs 사용됩니다.
 - 사용자 ID 및 그룹 ID의 경우 앞에 0을 사용하지 마세요. 예컨대, **12345**는 허용되지만 **012345**는 허용되지 않습니다.
 - c. (선택 사항) 보조 그룹 IDs에 각 사용자에게 IDs 대해 쉼표로 구분된 하나 이상의 추가 POSIX 그룹을 입력합니다.
 - d. 액세스 에서 다음과 같은 IAM 역할을 선택합니다.
 - 사용자에게 액세스하려는 Amazon EFS 리소스(파일 시스템)에만 액세스할 수 있는 권한을 부여합니다.
 - 사용자가 수행할 수 있는 파일 시스템 작업과 수행할 수 없는 파일 시스템 작업을 정의합니다.

탐재 액세스 및 읽기/쓰기 권한과 함께 Amazon EFS 파일 시스템 선택에 IAM 역할을 사용하는 것이 좋습니다. 예를 들어, 다음 두 AWS 관리형 정책의 조합은 매우 허용적이지만 사용자에게 필요한 권한을 부여합니다.

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

자세한 내용은 블로그 게시물 [Amazon Elastic File System을 위한AWS Transfer Family 지원](#)을 참조하세요.

e. 홈 디렉터리의 경우, 다음을 수행합니다.

- 를 사용하여 전송할 데이터를 저장하는 데 사용할 Amazon EFS 파일 시스템을 선택합니다 AWS Transfer Family.
- 홈 디렉터리를 제약으로 설정할지 여부를 결정하세요. 홈 디렉터리를 제약으로 설정하면 다음과 같은 결과가 발생합니다:
 - Amazon EFS 사용자는 해당 폴더 외부의 파일 또는 디렉터리에 액세스할 수 없습니다.
 - Amazon EFS 사용자는 Amazon EFS 파일 시스템 이름(fs-xxxxxxx)을 볼 수 없습니다.

 Note

제한 옵션을 선택하면 Amazon EFS 사용자에게 대한 symlink가 확인되지 않습니다.

- (옵션) 사용자가 클라이언트를 사용하여 로그인할 때 들어갈 홈 디렉터리의 경로를 입력합니다.

홈 디렉터리를 지정하지 않으면 Amazon EFS 파일 시스템의 루트 디렉터리가 사용됩니다. 이 경우 IAM 역할이 이 루트 디렉터리에 대한 액세스를 제공하는지 확인합니다.

5. SSH 퍼블릭 키의 경우 SSH 키 페어의 퍼블릭 SSH 키 부분을 입력합니다.

서비스에서 사용자의 키를 확인해야 새 사용자를 추가할 수 있습니다.

Note

SSH 키 페어를 생성하는 방법에 대한 지침은 섹션을 참조하세요 [서비스 관리 사용자를 위한 SSH 키 생성](#).

6. (옵션) 사용자의 태그를 입력하세요. 키 및 값에 하나 이상의 태그를 키-값 쌍으로 입력하고 태그 추가를 선택합니다.
7. 추가를 선택해 새 사용자를 원하는 서버에 추가합니다.

새 사용자는 서버 세부 정보 페이지의 사용자 섹션에 나타납니다.

SFTP Transfer Family 서버를 처음 사용할 때 발생할 수 있는 문제:

- sftp 명령을 실행해도 프롬프트가 나타나지 않으면 다음 메시지가 표시될 수 있습니다.

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

이 경우 사용자 역할에 대한 정책 권한을 늘려야 합니다. 와 같은 AWS 관리형 정책을 추가할 수 있습니다 AmazonElasticFileSystemClientFullAccess.

- sftp 프롬프트 pwd에 를 입력하여 사용자의 홈 디렉터리를 보는 경우 다음 메시지가 표시될 수 있습니다. **USER-HOME-DIRECTORY** 는 SFTP 사용자의 홈 디렉터리입니다.

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

이 경우 상위 디렉터리(cd ..)로 이동하여 사용자의 홈 디렉터리(mkdir **username**)를 만들 수 있어야 합니다.

다음 단계 - 그 다음 단계에서는 [클라이언트를 사용하여 서버 엔드포인트를 통한 파일 전송](#)로 계속 진행하세요.

서비스 관리 사용자 관리

이 섹션에서는 사용자 목록을 보는 방법, 사용자 세부 정보를 편집하는 방법, SSH 퍼블릭 키를 추가하는 방법에 대한 정보를 찾을 수 있습니다.

- [사용자 목록 보기](#)

- [사용자 세부 정보 보기 또는 편집](#)
- [사용자 삭제](#)
- [SSH 퍼블릭 키 추가](#)
- [SSH 퍼블릭 키 삭제](#)

사용자 목록을 찾으려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택하여 서버 페이지를 표시합니다.
3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자에서 사용자 목록을 확인합니다.

사용자 세부 정보를 보거나 편집하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택하여 서버 페이지를 표시합니다.
3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자에서 사용자 이름을 선택하면 사용자 세부 정보 페이지가 표시됩니다.

편집을 선택하여 이 페이지에서 사용자의 속성을 변경할 수 있습니다.

5. 사용자 세부 정보 페이지에서 사용자 구성 옆의 편집을 선택합니다.

- 구성 편집 페이지의 액세스 에서 Amazon S3 버킷에 대한 액세스를 제공하는 이전에 생성한 IAM 역할을 선택합니다.

의 절차를 사용하여 이 IAM 역할을 생성했습니다 [IAM 역할 및 정책 생성](#). 이 IAM 역할에는 Amazon S3 버킷에 대한 액세스를 제공하는 IAM 정책이 포함됩니다. 또한 다른 IAM 정책에 정의된 AWS Transfer Family 서비스와의 신뢰 관계도 포함됩니다.

- (옵션) 정책에서 다음 중 하나를 선택합니다.

- None(없음)
- 기존 정책
- 에서 정책을 IAM 선택하여 기존 정책을 선택합니다. 정책의 세부 정보가 포함된 JSON 객체를 보려면 보기를 선택합니다.

세션 정책에 대한 자세한 설명은 [IAM 역할 및 정책 생성](#) 섹션을 참조하세요. 세션 정책 생성에 대한 자세한 설명은 [Amazon S3 버킷을 위한 세션 정책 생성](#) 섹션을 참조하세요.

- 홈 디렉터리 에서 Amazon S3 버킷을 선택하여 를 사용하여 전송할 데이터를 저장합니다 AWS Transfer Family. 사용자가 클라이언트를 이용해 로그인하면 도착하게 되는 home 디렉터리의 경로를 입력합니다.

이 파라미터를 입력하지 않으면 Amazon S3 버킷의 root 디렉터리가 사용됩니다. 이 경우 IAM 역할이 이 root 디렉터리에 대한 액세스 권한을 제공하는지 확인하세요.

Note

사용자의 사용자 이름을 포함하는 디렉터리 경로 선택을 권장합니다. 세션 정책을 효과적으로 사용할 수 있습니다. 세션 정책은 사용자의 home 디렉터리에 대한 Amazon S3 버킷에서의 사용자 액세스를 제한합니다.

9. (옵션) 제약의 경우, 사용자가 해당 폴더 외부에 액세스할 수 없고 Amazon S3 버킷 또는 폴더 이름을 볼 수 없도록 확인란을 선택합니다.

Note

사용자에게 홈 디렉터를 할당하고 해당 홈 디렉터리로 사용자를 제한하는 경우 이 정도면 지정된 폴더에 대한 사용자 액세스를 잠그기에 충분합니다. 추가 통제를 적용해야 하는 경우 세션 정책을 사용하세요.

10. 저장을 선택하여 변경 사항을 저장합니다.

사용자 삭제

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택하여 서버 페이지를 표시합니다.
3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자에서 사용자 이름을 선택하면 사용자 세부 정보 페이지가 표시됩니다.
5. 사용자 세부 정보 페이지에서 사용자 이름 오른쪽에 있는 삭제를 선택합니다.
6. 표시되는 확인 대화 상자에서 단어 **delete**를 입력한 다음 삭제를 선택하여 사용자 삭제를 확인합니다.

사용자 목록에서 사용자가 삭제됩니다.

사용자의 SSH 퍼블릭 키를 추가하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.

3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자에서 사용자 이름을 선택하면 사용자 세부 정보 페이지가 표시됩니다.
5. SSH 퍼블릭 키 추가를 선택하여 사용자에게 새 SSH 퍼블릭 키를 추가합니다.

 Note

SSH 키는 Secure Shell(SSH) 파일 전송 프로토콜()에 대해 활성화된 서버에서만 사용됩니다. SFTP. SSH 키 페어를 생성하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [서비스 관리 사용자를 위한 SSH 키 생성](#).

6. SSH 퍼블릭 키의 경우 키 페어의 SSH 퍼블릭 SSH 키 부분을 입력합니다.

서비스에서 사용자의 키를 확인해야 새 사용자를 추가할 수 있습니다. SSH 키의 형식은 `ssh-rsa string`. SSH 키 페어를 생성하려면 섹션을 참조하세요 [서비스 관리 사용자를 위한 SSH 키 생성](#).

7. 키 추가를 선택합니다.

사용자의 SSH 퍼블릭 키를 삭제하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.
3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자에서 사용자 이름을 선택하면 사용자 세부 정보 페이지가 표시됩니다.
5. 퍼블릭 키를 삭제하려면 해당 SSH 키 확인란을 선택하고 삭제를 선택합니다.

AWS 디렉터리 서비스 자격 증명 공급자 사용

이 주제에서는 에 대한 AWS Directory Service 자격 증명 공급자를 사용하는 방법을 설명합니다 AWS Transfer Family.

주제

- [사용 AWS Directory Service for Microsoft Active Directory](#)
- [Azure Active Directory 도메인 서비스에 디렉터리 서비스 사용](#)

사용 AWS Directory Service for Microsoft Active Directory

를 사용하여 AWS Transfer Family 를 사용하여 파일 전송 최종 사용자를 인증할 수 있습니다 AWS Directory Service for Microsoft Active Directory. 최종 사용자의 자격 증명을 변경하거나 사용자 지정 권한 부여자를 사용하지 않고도 Active Directory 인증을 사용하는 파일 전송 워크플로를 원활하게 마 이그레이션할 수 있습니다.

를 사용하면 Amazon Simple Storage Service(Amazon S3)에 저장된 데이터에 FTP 대해 FTPS, 및 SFTP를 통해 AWS Directory Service 사용자 및 그룹에 액세스 권한을 안전하게 제공할 AWS Managed Microsoft AD수 있습니다EFS. Amazon Elastic File System Active Directory를 사용하여 사 용자의 자격 증명을 저장하면 이제 이러한 사용자에게 대한 파일 전송을 더 쉽게 활성화할 수 있습니다.

Active Directory 커넥터를 사용하여 온프레미스 환경 또는 AWS 클라우드에서 의 Active Directory 그 룹에 대한 액세스를 제공할 수 AWS Managed Microsoft AD 있습니다. AWS 클라우드 또는 온프레미 스 네트워크에서 Microsoft Windows 환경에 이미 구성된 사용자에게 를 사용하여 자격 증명에 사용되 는 AWS Transfer Family 서버에 AWS Managed Microsoft AD 대한 액세스 권한을 부여할 수 있습니다.

Note

- AWS Transfer Family 는 Simple AD를 지원하지 않습니다.
- Transfer Family는 리전 간 Active Directory 구성을 지원하지 않습니다. Transfer Family 서버 와 동일한 리전에 있는 Active Directory 통합만 지원합니다.
- Transfer Family는 AWS Managed Microsoft AD 또는 AD Connector를 사용하여 기존 RADIUS기반 MFA 인프라에 대한 다중 인증(MFA)을 활성화하는 것을 지원하지 않습니다.
- AWS Transfer Family 는 Managed Active Directory의 복제된 리전을 지원하지 않습니다.

를 사용하려면 다음 단계를 수행해야 AWS Managed Microsoft AD합니다.

1. AWS Directory Service 콘솔을 사용하여 하나 이상의 AWS Managed Microsoft AD 디렉터리를 생 성합니다.
2. Transfer Family 콘솔을 사용하여 를 자격 증명 공급자 AWS Managed Microsoft AD 로 사용하는 서버를 생성합니다.
3. 하나 이상의 AWS Directory Service 그룹에서 액세스를 추가합니다.
4. 필수 사항은 아니지만 사용자 액세스를 테스트하고 확인하는 것이 좋습니다.

주제

- [사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory](#)
- [액티브 디렉터리 영역 사용](#)
- [자격 증명 공급자 AWS Managed Microsoft AD 로 선택](#)
- [그룹에 액세스 권한 부여](#)
- [테스트 사용자](#)
- [그룹의 서버 액세스 삭제](#)
- [SSH \(Secure Shell\)을 사용하여 서버에 연결](#)
- [포리스트 및 트러스트를 사용하여 자체 관리형 Active Directory AWS Transfer Family 에 연결](#)

사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory

AD 그룹의 고유 식별자를 입력합니다.

를 사용하려면 먼저 Microsoft AD 디렉터리의 각 그룹에 고유한 식별자를 제공해야 AWS Managed Microsoft AD합니다. 각 그룹의 보안 식별자(SID)를 사용하여 이를 수행할 수 있습니다. 연결한 그룹의 사용자는 AWS Transfer Family를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다.

다음 Windows PowerShell 명령을 사용하여 그룹의 SID 를 검색하고 *YourGroupName* 그룹 이름을 사용합니다.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```

Note

를 자격 증명 공급자 AWS Directory Service 로 사용하고 있고 및 값이 다른 경우 userPrincipalNameSamAccountName는 의 값을 AWS Transfer Family 수락합니다 SamAccountName. Transfer Family는 userPrincipalName에 지정된 값을 수락하지 않습니다.

역할에 AWS Directory Service 권한 추가

를 자격 증명 공급자 AWS Directory Service 로 사용하려면 권한도 필요합니다 AWS Directory Service API. 다음 권한이 필요하거나 제안됩니다.

- Transfer Family에서 디렉토리를 조회하려면 `ds:DescribeDirectories`가 필요합니다.
- Transfer Family에 대한 승인을 추가하려면 `ds:AuthorizeApplication`가 필요합니다.
- `ds:UnauthorizeApplication`에서는 서버 생성 프로세스 중에 문제가 발생할 경우를 대비하여 임시로 생성된 모든 리소스를 제거하는 것이 좋습니다.

Transfer Family 서버를 만드는 데 사용하는 역할에 이러한 권한을 추가하세요. 이러한 권한에 대한 자세한 내용은 [AWS Directory Service API 작업, 리소스 및 조건 참조 권한](#)을 참조하세요.

액티브 디렉터리 영역 사용

Active Directory 사용자가 AWS Transfer Family 서버에 액세스하도록 하는 방법을 고려할 때는 사용자의 영역과 해당 그룹의 영역을 염두에 두세요. 가장 바람직한 것은 사용자 영역과 그룹 영역이 일치해야 하는 것입니다. 즉, 사용자와 그룹이 모두 기본 영역에 있거나 둘 다 신뢰할 수 있는 영역에 속해 있다는 뜻입니다. 그렇지 않은 경우 Transfer Family에서 사용자를 인증할 수 없습니다.

사용자를 테스트하여 구성이 올바른지 확인할 수 있습니다. 자세한 내용은 [테스트 사용자](#)를 참조하세요. 사용자/그룹 영역에 문제가 있는 경우 사용자 그룹에 연결된 액세스 권한을 찾을 수 없습니다라는 오류 메시지가 표시됩니다.

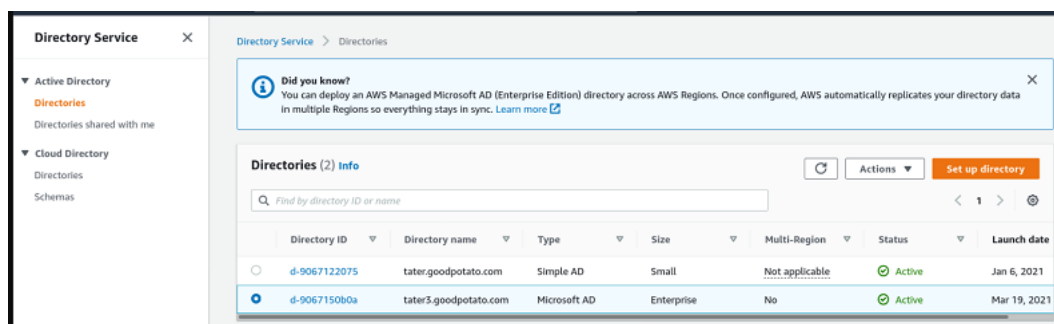
자격 증명 공급자 AWS Managed Microsoft AD 로 선택

이 섹션에서는 클라이언트 서버 AWS Directory Service for Microsoft Active Directory 와 함께 사용하는 방법을 설명합니다.

Transfer Family AWS Managed Microsoft AD 와 함께 사용하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Directory Service 콘솔을 엽니다 <https://console.aws.amazon.com/directoryservicev2/>.

AWS Directory Service 콘솔을 사용하여 하나 이상의 관리형 디렉토리를 구성합니다. 자세한 내용을 알아보려면 AWS Directory Service 관리 안내서의 [AWS Managed Microsoft AD](#) 단원을 참조하세요.



- 에서 AWS Transfer Family 콘솔을 열고 서버 생성 을 <https://console.aws.amazon.com/transfer/> 선택합니다.
- 프로토콜 선택 페이지의 목록에서 하나 이상의 프로토콜을 선택합니다.

Note

를 AWS Certificate Manager 선택한 경우 인증서를 제공해야 FTPS합니다.

- 자격 증명 제공자 선택에서 AWS Directory Service를 선택합니다.

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**

- 디렉터리 목록에는 구성된 모든 관리 디렉터리가 포함됩니다. 목록에서 디렉터리를 선택하고 다음을 선택합니다.

Note

- 크로스 계정 및 공유 디렉터리는 에서 지원되지 않습니다 AWS Managed Microsoft AD.
- Directory Service를 자격 증명 공급자로 사용하여 서버를 설정하려면 몇 가지 AWS Directory Service 권한을 추가해야 합니다. 세부 정보는 [사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory](#)을 참조하세요.

- 서버 생성을 완료하려면 다음 절차 중 하나를 사용합니다.

- [SFTP활성화 서버 생성](#)
- [FTPS활성화 서버 생성](#)
- [FTP활성화 서버 생성](#)

해당 절차에서 ID 제공자 선택 다음 단계를 계속 진행하세요.

⚠ Important

Transfer Family 서버에서 Microsoft AD 디렉터리를 사용한 AWS Directory Service 경우 에서 이를 삭제할 수 없습니다. 먼저 서버를 삭제해야 디렉터리를 삭제할 수 있습니다.

그룹에 액세스 권한 부여

서버를 생성한 후에는 를 사용하여 활성화된 프로토콜을 통해 파일을 업로드하고 다운로드할 수 있는 액세스 권한이 있는 디렉터리의 그룹을 선택해야 합니다 AWS Transfer Family. 액세스 권한을 생성하여 이 작업을 수행할 수 있습니다.

i Note

사용자는 액세스 권한을 부여하는 그룹에 직접 속해야 합니다. 예를 들어 Bob은 사용자이고 그룹 A에 속해 있으며 그룹 A 자체가 그룹 B에 포함되어 있다고 가정해 보겠습니다.

- 그룹 A에 액세스 권한을 부여하면 Bob에게 액세스 권한이 부여됩니다.
- 그룹 A가 아닌 그룹 B에 액세스 권한을 부여하는 경우 Bob은 액세스 권한을 갖지 않습니다.

그룹에 액세스 권한을 부여하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 서버 세부 정보 페이지로 이동합니다.
3. 액세스 섹션에서 액세스 추가를 선택합니다.
4. 이 서버에 액세스할 AWS Managed Microsoft AD 디렉터리SID의 를 입력합니다.

Note

그룹의 SID를 찾는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [the section called “사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory”](#).

5. 액세스에서 그룹의 AWS Identity and Access Management (IAM) 역할을 선택합니다.
6. 정책 섹션에서 정책을 선택합니다. 기본 설정은 없음입니다.
7. 홈 디렉터리의 경우 그룹의 홈 디렉터리에 해당하는 S3 버킷을 선택합니다.

Note

세션 정책을 생성하여 사용자에게 표시되는 버킷 부분을 제한할 수 있습니다. 예를 들어, /filetest 디렉터리 아래에 있는 자신의 폴더로만 사용자를 제한하려면 상자에 다음 텍스트를 입력합니다.

```
/filetest/${transfer:UserName}
```

세션 정책 생성에 대한 자세한 설명은 [Amazon S3 버킷을 위한 세션 정책 생성](#) 섹션을 참조하세요.

8. 추가를 선택하여 연결을 생성합니다.
9. 서버를 선택합니다.
10. 액세스 추가를 선택합니다.
 - 그룹의 SID를 입력합니다.

Note

를 찾는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [the section called “사용을 시작하기 전에 AWS Directory Service for Microsoft Active Directory”](#).

11. 액세스 추가를 선택합니다.

액세스 섹션에는 서버에 대한 액세스가 나열됩니다.

The screenshot displays the AWS Transfer Family console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', 'Subnet ID' as 'subnet-...', and '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 first entry shows 'S...', '/padbucket3', and 'ADGuy_S3_And_EFS'. 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 this section.

테스트 사용자

사용자가 서버의 AWS Managed Microsoft AD 디렉터리에 액세스할 수 있는지 테스트할 수 있습니다.

Note

사용자는 엔드포인트 구성 페이지의 액세스 섹션에 나열된 정확히 하나의 그룹(외부 ID)에 속해야 합니다. 사용자가 그룹에 속하지 않거나 둘 이상의 그룹에 속해 있는 경우 해당 사용자에게 액세스 권한이 부여되지 않습니다.

특정 사용자에게 액세스 권한이 있는지 테스트하려면

1. 서버 세부 정보 페이지에서 작업을 선택한 다음 테스트를 선택합니다.
2. 자격 증명 제공자 테스트의 경우 액세스 권한이 있는 그룹 중 하나에 속하는 사용자의 로그인 자격 증명을 입력합니다.
3. 테스트를 선택합니다.

ID 제공자 테스트에 성공하면 선택한 사용자에게 서버 액세스 권한이 부여되었음을 알 수 있습니다.

Identity provider testing

User configuration [Info](#)

Username

transferuser1

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

사용자가 액세스 권한이 있는 두 개 이상의 그룹에 속해 있는 경우 다음과 같은 응답을 받게 됩니다.

```
"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."
```

그룹의 서버 액세스 삭제

그룹의 서버 액세스 삭제

1. 서버 세부 정보 페이지에서 작업을 선택한 다음 액세스 삭제를 선택합니다.
2. 대화 상자에서 이 그룹에 대한 액세스 권한을 제거합니다.

서버 세부 정보 페이지로 돌아가면 이 그룹에 대한 액세스 권한이 더 이상 나열되지 않는 것을 볼 수 있습니다.

SSH (Secure Shell)을 사용하여 서버에 연결

서버와 사용자를 구성한 후 를 사용하여 서버에 연결하고 액세스 권한이 있는 사용자의 정규화된 사용자 이름을 SSH 사용할 수 있습니다.

```
sftp user@active-directory-domain@vpc-endpoint
```

예: `transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`.

이 형식은 페더레이션 검색을 대상으로 하므로 크기가 클 수 있는 Active Directory의 검색을 제한합니다.

Note

간단한 사용자 이름을 지정할 수 있습니다. 하지만 이 경우 Active Directory 코드가 페더레이션의 모든 디렉터리를 검색해야 합니다. 이로 인해 검색이 제한될 수 있으며 사용자에게 액세스 권한이 있어야 하는 경우에도 인증이 실패할 수 있습니다.

인증이 완료되면 사용자는 사용자를 구성할 때 지정한 홈 디렉터리에 위치해 있습니다.

포리스트 및 트러스트를 사용하여 자체 관리형 Active Directory AWS Transfer Family 에 연결

자체 관리형 Active Directory(AD)의 사용자는 AWS 계정 및 Transfer Family 서버에 AWS IAM Identity Center 대한 Single Sign-On 액세스에도 를 사용할 수 있습니다. 이렇게 하려면 AWS Directory Service 다음 옵션을 사용할 수 있습니다.

- 단방향 포리스트 신뢰(온프레미스 Active Directory에서 발신 AWS Managed Microsoft AD 및 수신)는 루트 도메인에서만 작동합니다.
- 하위 도메인의 경우 다음 중 하나를 사용할 수 있습니다.
 - AWS Managed Microsoft AD 및 온프레미스 Active Directory 간에 양방향 신뢰 사용
 - 각 하위 도메인에는 단방향 외부 트러스트를 사용합니다.

예를 들어 `transferuserexample@mycompany.com` 신뢰할 수 있는 도메인을 사용하여 서버에 연결하는 경우 사용자는 신뢰할 수 있는 도메인을 지정해야 합니다.

Azure Active AWS Directory 도메인 서비스에 디렉터리 서비스 사용

- SFTP 전송 요구 사항에 맞게 기존 Active Directory 포리스트를 활용하려면 [Active Directory Connector](#)를 사용할 수 있습니다.
- 완전 관리형 서비스에서 Active Directory의 이점과 고가용성을 활용하려면 AWS Directory Service for Microsoft Active Directory를 사용할 수 있습니다. 세부 정보는 [AWS 디렉터리 서비스 자격 증명 공급자 사용](#)을 참조하세요.

이 주제에서는 Active Directory 커넥터 및 [Azure Active Directory 도메인 서비스\(Azure ADDS\)](#)를 사용하여 [Azure Active Directory](#)로 SFTP Transfer 사용자를 인증하는 방법을 설명합니다.

주제

- [Azure Active AWS Directory Domain Services용 Directory Service를 사용하기 전에](#)
- [1단계: Azure Active Directory 도메인 서비스 추가](#)
- [2단계: 서비스 계정 생성](#)
- [3단계: AD Connector를 사용하여 AWS 디렉터리 설정](#)
- [4단계: AWS Transfer Family 서버 설정](#)
- [5단계: 그룹에 액세스 권한 부여](#)
- [6단계: 사용자 테스트](#)

Azure Active AWS Directory Domain Services용 Directory Service를 사용하기 전에

의 경우 다음이 AWS필요합니다.

- Transfer Family 서버를 사용하는 AWS 리전의 가상 프라이빗 클라우드(VPC)
- 예서 최소 2개의 프라이빗 서브넷 VPC
- 예 인터넷 연결이 있어야 VPC 합니다.
- Microsoft Azure와의 VPN 연결을 위한 site-to-site 고객 게이트웨이 및 가상 프라이빗 게이트웨이

Microsoft Azure의 경우 다음이 필요합니다.

- Azure Active Directory 및 Active Directory 도메인 서비스(AzureADDS)
- Azure 리소스 그룹
- Azure 가상 네트워크

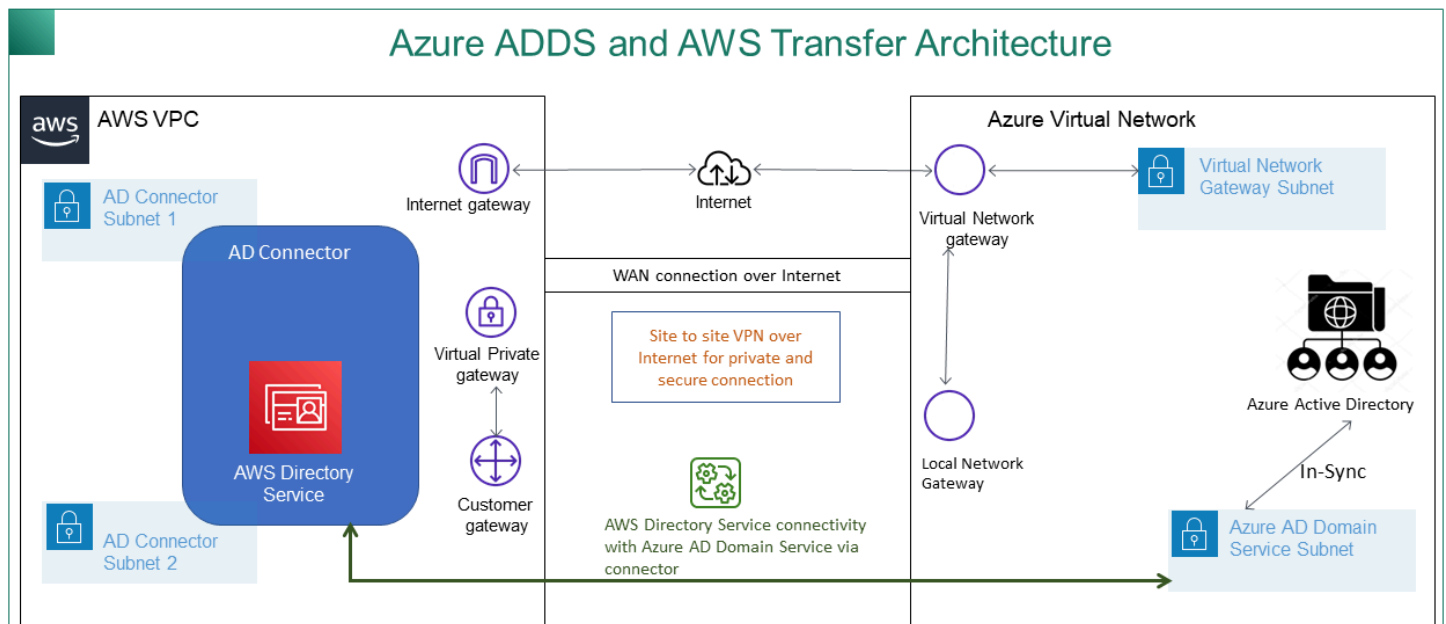
- VPN AmazonVPC과 Azure 리소스 그룹 간의 연결

Note

이는 네이티브 IPSEC 터널을 통하거나 VPN 어플라이언스를 사용하는 것일 수 있습니다. 이 주제에서는 Azure Virtual 네트워크 게이트웨이와 로컬 네트워크 게이트웨이 간의 IPSEC 터널을 사용합니다. 터널은 Azure ADDS 엔드포인트와 를 수용하는 서브넷 간의 트래픽을 허용하도록 구성되어야 합니다 AWS VPC.

- Microsoft Azure와의 VPN 연결을 위한 site-to-site 고객 게이트웨이 및 가상 프라이빗 게이트웨이

다음 다이어그램은 시작하기 전에 필요한 구성을 보여줍니다.



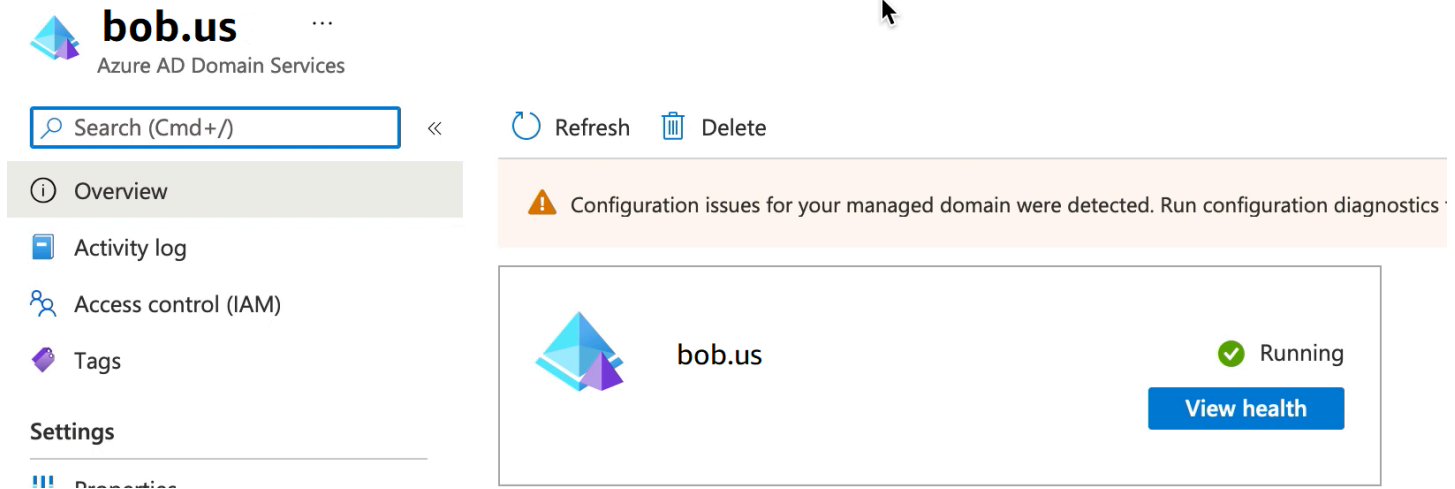
1단계: Azure Active Directory 도메인 서비스 추가

Azure AD는 기본적으로 도메인 가입 인스턴스를 지원하지 않습니다. 도메인 가입과 같은 작업을 수행하고 그룹 정책과 같은 도구를 사용하려면 관리자가 Azure Active Directory 도메인 서비스를 사용하도록 설정해야 합니다. Azure AD DS를 아직 추가하지 않았거나 기존 구현이 SFTP Transfer 서버가 사용할 도메인과 연결되어 있지 않은 경우 새 인스턴스를 추가해야 합니다.

Azure Active Directory 도메인 서비스(Azure ADDS) 활성화에 대한 자세한 내용은 [자습서: Azure Active Directory 도메인 서비스 관리형 도메인 생성 및 구성을 참조하세요](#).

Note

Azure 를 활성화할 때 SFTP Transfer 서버를 연결할 리소스 그룹과 Azure AD 도메인에 대해 구성되었는지 ADDS확인합니다.



The screenshot shows the Azure AD Domain Services interface for the domain **bob.us**. The left sidebar contains navigation links: Overview (selected), Activity log, Access control (IAM), Tags, Settings, and Properties. The main content area features a search bar, Refresh and Delete buttons, and a warning message: "Configuration issues for your managed domain were detected. Run configuration diagnostics". Below this, a card displays the domain **bob.us** with a green checkmark and the status **Running**, accompanied by a **View health** button.

2단계: 서비스 계정 생성

Azure AD에는 Azure 의 관리자 그룹에 속하는 서비스 계정이 하나 있어야 합니다ADDS. 이 계정은 AWS Active Directory 커넥터와 함께 사용됩니다. 이 계정이 Azure 와 동기화되어 있는지 확인합니다ADDS.

Home > Default Directory > Users > bobatusa



bobatusa | Profile

User


[Edit](#)
[Reset password](#)
[Revoke sessions](#)
[Delete](#)
[Refresh](#)
[Got feedback?](#)
[Diagnose and solve problems](#)

Manage

- [Profile](#)
- [Assigned roles](#)
- [Administrative units](#)
- [Groups](#)
- [Applications](#)
- [Licenses](#)
- [Devices](#)
- [Azure role assignments](#)
- [Authentication methods](#)

Activity

- [Sign-in logs](#)
- [Audit logs](#)

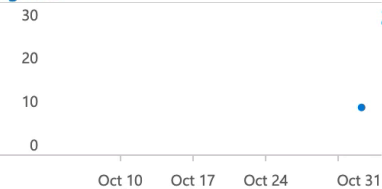
bobatusa

bobsmith@xyz.com



Creation time
10/6/2021, 1:32:27 AM

User Sign-ins



Group memberships

2

Identity

Name	First name	Last name
bobatusa	Bob	Smith
User Principal Name	User type	
bobsmith@xyz.com	Member	

Tip

Azure Active Directory에 대한 다중 인증은 SFTP 프로토콜을 사용하는 Transfer Family 서버에서 지원되지 않습니다. 사용자가 에 인증한 후에는 Transfer Family 서버가 MFA 토큰을 제공할 수 없습니다. SFTP 연결을 시도하기 전에 MFA 전에 를 비활성화해야 합니다.

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](#)

3단계: AD Connector를 사용하여 AWS 디렉터리 설정

Azure 를 구성ADDS하고 및 Azure Virtual 네트워크 간에 IPSEC VPN AWS VPC 터널이 있는 서비스 계정을 생성한 후에는 모든 AWS EC2 인스턴스에서 Azure ADDS DNS IP 주소를 ping하여 연결을 테스트할 수 있습니다.

연결이 활성화되었는지 확인한 후 아래에서 계속할 수 있습니다.

AD Connector를 사용하여 AWS 디렉터리를 설정하려면

1. [디렉터리 서비스](#) 콘솔을 열고 디렉터리를 선택합니다.
2. 디렉터리 설정을 선택합니다.
3. 디렉터리 타입으로는 AD Connector를 선택합니다.
4. 디렉터리 크기를 선택하고 다음 을 선택한 다음 VPC 및 서브넷을 선택합니다.
5. 다음을 선택하고 다음과 같이 필드를 채웁니다.
 - 디렉터리 DNS 이름: Azure 에 사용 중인 도메인 이름을 입력합니다ADDS.
 - DNS IP 주소: Azure ADDS IP 주소를 입력합니다.
 - 서버 계정 사용자 이름 및 암호: 2단계: 서비스 계정 생성에서 만든 서비스 계정의 세부 정보를 입력합니다.
6. 화면을 완료하여 디렉터리 서비스를 생성합니다.

이제 디렉터리 상태가 활성 이어야 하며 SFTP Transfer 서버와 함께 사용할 준비가 되었습니다.

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](#)



Actions ▾

Set up directory

< 1 >
 

	Directory ID ▾	Directory name ▾	Type ▾	Size ▾	Multi-Region ▾	Status ▾	Launch date ▾
☐	d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

4단계: AWS Transfer Family 서버 설정

SFTP 프로토콜과 AWS Directory Service 의 자격 증명 공급자 유형을 사용하여 Transfer Family 서버를 생성합니다. 디렉터리 드롭다운 목록에서 3단계: AD Connector를 사용한 디렉터리 설정 에서 추가한 AWS 디렉터리를 선택합니다.

Note

Transfer Family 서버에서 Microsoft AD 디렉터리를 사용한 경우 AWS Directory Service에서 이를 삭제할 수 없습니다. 먼저 서버를 삭제해야 디렉터리를 삭제할 수 있습니다.

5단계: 그룹에 액세스 권한 부여

서버를 생성한 후에는 를 사용하여 활성화된 프로토콜을 통해 파일을 업로드하고 다운로드할 수 있는 액세스 권한이 있는 디렉터리의 그룹을 선택해야 합니다 AWS Transfer Family. 액세스 권한을 생성하여 이 작업을 수행할 수 있습니다.

Note

사용자는 액세스 권한을 부여하는 그룹에 직접 속해야 합니다. 예를 들어 Bob은 사용자이고 그룹 A에 속해 있으며 그룹 A 자체가 그룹 B에 포함되어 있다고 가정해 보겠습니다.

- 그룹 A에 액세스 권한을 부여하면 Bob에게 액세스 권한이 부여됩니다.
- 그룹 A가 아닌 그룹 B에 액세스 권한을 부여하는 경우 Bob은 액세스 권한을 갖지 않습니다.

액세스 권한을 부여하려면 그룹의 SID 를 검색해야 합니다.

다음 Windows PowerShell 명령을 사용하여 그룹의 SID 를 검색하고 *YourGroupName* 그룹 이름을 사용합니다.

```
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 Administrat
mAccountName,ObjectSid

SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104

```

그룹에 액세스 권한을 부여하려면

1. 를 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 서버 세부 정보 페이지로 이동한 다음 액세스 섹션에서 액세스 추가를 선택합니다.
3. 이전 절차의 출력에서 SID 받은 를 입력합니다.
4. 액세스 에서 그룹의 AWS Identity and Access Management 역할을 선택합니다.
5. 정책 섹션에서 정책을 선택합니다. 기본값은 없음입니다.
6. 홈 디렉터리의 경우 그룹의 홈 디렉터리에 해당하는 S3 버킷을 선택합니다.
7. 추가를 선택하여 연결을 생성합니다.

전송 서버의 세부 정보는 다음과 유사해야 합니다.

Protocols
Edit

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider
Edit

Identity provider type
AWS Directory Service

Directory ID
d-123456789a

Accesses (1)

Actions
Add access

< 1 >

☐	External Id	Home directory	Role
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/s3/transfer	sftp-user-role

6단계: 사용자 테스트

사용자가 서버의 AWS Managed Microsoft AD 디렉터리에 액세스할 수 있는지 테스트([테스트 사용자](#))할 수 있습니다. 사용자는 엔드포인트 구성 페이지의 액세스 섹션에 나열된 정확히 하나의 그룹(외부 ID)에 속해야 합니다. 사용자가 그룹에 속하지 않거나 둘 이상의 그룹에 속해 있는 경우 해당 사용자에게 액세스 권한이 부여되지 않습니다.

사용자 지정 자격 증명 공급자와 작업

사용자를 인증하려면 에서 기존 자격 증명 공급자를 사용할 수 있습니다 AWS Transfer Family. 사용자가 Amazon S3 또는 Amazon Elastic File System(Amazon)에 액세스할 수 있도록 인증하고 권한을 부여하는 AWS Lambda 함수를 사용하여 자격 증명 공급자를 통합합니다EFS. 세부 정보는 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#)을 참조하세요. 또한 AWS Transfer Family 관리 콘솔에서 전송된 파일 수 및 바이트와 같은 지표에 대한 그래프에 액세스 CloudWatch 하여 중앙 집중식 대시보드를 사용하여 파일 전송을 모니터링할 수 있는 단일 창을 제공할 수 있습니다.

또는 단일 Amazon API Gateway 메서드가 있는 RESTful 인터페이스를 제공할 수 있습니다. Transfer Family는 이 메서드를 호출하여 자격 증명 공급자에 연결합니다. 자격 증명 공급자는 사용자에게 Amazon S3 또는 Amazon 에 대한 액세스 권한을 인증하고 부여합니다EFS. 를 사용하여 자격 증명 공급자RESTfulAPI를 통합해야 하거나 를 사용하여 지리 차단 또는 속도 제한 요청을 위한 기능을 AWS WAF 활용하려는 경우 이 옵션을 사용합니다. 세부 정보는 [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#)을 참조하세요.

어느 경우든 [AWS Transfer Family 콘솔](#) 또는 [CreateServer](#) API 작업.

Note

참석할 수 있는 워크숍이 있어 File Transfer 솔루션을 구축할 수 있습니다. 이 솔루션은 관리형 SFTP/FTPS 엔드포인트 AWS Transfer Family 에 를 활용하고 사용자 관리를 위해 Amazon Cognito 및 DynamoDB를 활용합니다. 이 워크숍의 세부 정보는 [여기](#)에서 확인할 수 있습니다.

AWS Transfer Family 는 사용자 지정 자격 증명 공급자를 사용하기 위한 다음 옵션을 제공합니다.

- AWS Lambda 를 사용하여 자격 증명 공급자 연결 - Lambda 함수가 지원하는 기존 자격 증명 공급자를 사용할 수 있습니다. 귀하는 Lambda 함수의 명칭을 제공합니다. 자세한 내용은 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.
- Amazon API Gateway를 사용하여 자격 증명 공급자 연결 - 자격 증명 공급자로 사용하기 위해 Lambda 함수가 지원하는 API 게이트웨이 메서드를 생성할 수 있습니다. Amazon API GatewayURL

와 호출 역할을 제공합니다. 자세한 내용은 [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#) 단원을 참조하십시오.

어느 옵션이든 귀하가 인증 방법도 지정할 수 있습니다.

- 암호 또는 키 - 사용자는 암호 또는 키로 인증할 수 있습니다. 이것이 기본값입니다.
- 암호 ONLY - 사용자가 연결할 암호를 제공해야 합니다.
- 키 ONLY - 사용자가 연결할 프라이빗 키를 제공해야 합니다.
- 암호 AND 키 - 사용자는 연결할 프라이빗 키와 암호를 모두 제공해야 합니다. 서버가 먼저 키를 확인한 다음 키가 유효하면 암호를 입력하라는 메시지가 표시됩니다. 제공된 프라이빗 키가 저장된 퍼블릭 키와 일치하지 않는 경우 인증이 실패합니다.

여러 인증 방법을 사용하여 사용자 지정 자격 증명 공급자로 인증

Transfer Family 서버는 여러 인증 방법을 사용할 때 AND 로직을 제어합니다. Transfer Family는 이를 사용자 지정 자격 증명 공급자에 대한 두 개의 별도 요청으로 취급하지만, 그 효과가 결합됩니다.

인증을 완료하려면 두 요청 모두 올바른 응답으로 성공적으로 반환되어야 합니다. Transfer Family는 두 개의 응답을 완료해야 합니다. 즉, Amazon을 스토리지EFS로 사용하는 경우 필요한 모든 요소(역할, 홈 디렉터리, 정책 및 POSIX 프로파일)가 포함되어 있습니다. 또한 Transfer Family는 암호 응답에 퍼블릭 키를 포함하지 않아야 합니다.

퍼블릭 키 요청은 자격 증명 공급자와 별도의 응답이 있어야 합니다. 암호 OR 키 또는 암호 키 AND 를 사용할 때는 이 동작이 변경되지 않습니다.

SSH/SFTP 프로토콜은 먼저 퍼블릭 키 인증으로 소프트웨어 클라이언트에 문제를 제기한 다음 암호 인증을 요청합니다. 이 작업은 사용자가 인증을 완료하기 전에 모두 성공하도록 요구합니다.

주제

- [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#)
- [Amazon API Gateway를 사용하여 자격 증명 공급자 통합](#)

AWS Lambda 를 사용하여 자격 증명 공급자 통합

사용자 지정 자격 증명 공급자에 연결하는 AWS Lambda 함수를 생성합니다. Okta, Secrets Manager, OneLogin 또는 권한 부여 및 인증 로직이 포함된 사용자 지정 데이터 스토어와 같은 사용자 지정 자격 증명 공급자를 사용할 수 있습니다.

 Note

Lambda를 ID 공급자로 사용하는 Transfer Family 서버를 생성하기 전에 함수를 생성해야 합니다. Lambda 함수의 예는 [예 Lambda 함수](#)를 참조하세요. 또는 중 하나를 사용하는 CloudFormation 스택을 배포할 수 있습니다 [Lambda 함수 템플릿](#). 또한 Lambda 함수가 Transfer Family를 신뢰하는 리소스 기반 정책을 사용하는지 확인하세요. 정책 예제는 [Lambda 리소스 기반 정책](#)을 참조하세요.

1. [AWS Transfer Family 콘솔](#)을 엽니다.
2. 서버 생성을 선택하여 서버 생성 페이지를 엽니다. ID 제공자 선택을 위해 다음 스크린샷과 같이 사용자 지정 ID 공급자를 선택합니다.

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](#) Either a valid password or valid private key will be required during user authentication

Cancel Previous **Next**

[i](#) Note

인증 방법 선택은 Transfer Family 서버의 프로토콜 중 SFTP 하나로 를 활성화한 경우에만 사용할 수 있습니다.

- 기본값인 자격 증명 공급자 연결 AWS Lambda 에 사용 가 선택되어 있는지 확인합니다.
- AWS Lambda 함수에서 Lambda 함수의 이름을 선택합니다.
- 나머지 상자를 채운 다음 서버 만들기를 선택합니다. 서버를 만들기 위한 나머지 단계에 대한 자세한 내용은 [SFTP, FTPS 또는 FTP 서버 엔드포인트 구성](#)을 참조하세요.

Lambda 리소스 기반 정책

Transfer Family 서버 및 Lambda를 참조하는 정책이 있어야 합니다ARNs. 예를 들어 ID 공급자에 연결되는 Lambda 함수와 함께 다음 정책을 사용할 수 있습니다. 정책은 문자열JSON로 이스케이프됩니다.

```
"Policy":
"{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "AllowTransferInvocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:transfer:region:account-id:function:my-lambda-auth-function",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:transfer:region:account-id:server/server-id"
        }
      }
    }
  ]
}"
```

Note

위의 예제 정책에서 각각을 바꿉니다.*user input placeholder* 자신의 정보를 사용합니다.

이벤트 메시지 구조

사용자 지정에 대해 권한 부여자 Lambda 함수로 전송된 SFTP 서버의 이벤트 메시지 구조IDP는 다음과 같습니다.

```
{
  'username': 'value',
  'password': 'value',
```

```
{
  'protocol': 'SFTP',
  'serverId': 's-abcd123456',
  'sourceIp': '192.168.0.100'
}
```

서버로 전송되는 로그인 자격 증명의 값인 username과 password의 위치는 어디입니까?

예를 들어, 다음 명령을 입력해서 연결합니다.

```
sftp bobusa@server_hostname
```

새 암호를 두 번 입력하라는 메시지가 나타납니다.

```
Enter password:
mysecretpassword
```

Lambda 함수 내에서 전달된 이벤트를 인쇄하여 Lambda 함수에서 이를 확인할 수 있습니다. 그것은 다음 텍스트 블록과 비슷하게 보여야 합니다.

```
{
  'username': 'bobusa',
  'password': 'mysecretpassword',
  'protocol': 'SFTP',
  'serverId': 's-abcd123456',
  'sourceIp': '192.168.0.100'
}
```

이벤트 구조는 FTP 및 에 대해 유사합니다FTPS. 유일한 차이점은 값이 보다는 protocol 파라미터에 사용된다는 것입니다SFTP.

인증을 위한 Lambda 함수

다양한 인증 전략을 구현하려면 Lambda 함수를 편집하세요. 애플리케이션의 요구 사항을 충족하기 위해 CloudFormation 스택을 배포할 수 있습니다. 자세한 내용은 [개발자 안내서](#)나 [AWS Lambda Node.js로 Lambda 함수 구축](#)을 참조하세요.

주제

- [Lambda 함수 템플릿](#)
- [유효 Lambda 값](#)
- [예 Lambda 함수](#)

• [구성 테스트](#)

Lambda 함수 템플릿

인증에 Lambda 함수를 사용하는 AWS CloudFormation 스택을 배포할 수 있습니다. 로그인 자격 증명을 사용하여 사용자를 인증하고 권한을 부여하는 여러 템플릿을 제공합니다. 이러한 템플릿 또는 AWS Lambda 코드를 수정하여 사용자 액세스를 추가로 사용자 지정할 수 있습니다.

Note

템플릿에 FIPS활성화된 보안 정책을 지정 AWS CloudFormation 하여 를 통해 FIPS활성화된 AWS Transfer Family 서버를 생성할 수 있습니다. 사용 가능한 보안 정책은 [에 대한 보안 정책 AWS Transfer Family](#)에 설명되어 있습니다.

인증에 사용할 AWS CloudFormation 스택을 생성하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. AWS CloudFormation 사용 설명서의 AWS CloudFormation 스택 템플릿 [선택 의 기존 템플릿에서 스택을 배포하는](#) 방법에 대한 지침을 따릅니다.
3. 다음 템플릿 중 하나를 사용하여 Transfer Family의 인증에 사용할 Lambda 함수를 생성합니다.

- [클래식 \(Amazon Cognito\) 스택 템플릿](#)

에서 사용자 지정 자격 증명 공급자로 사용할 를 생성하기 AWS Lambda 위한 기본 템플릿입니다 AWS Transfer Family. 암호 기반 인증을 위해 Amazon Cognito에 대해 인증하며, 퍼블릭 키 기반 인증을 사용하는 경우 Amazon S3 버킷에서 퍼블릭 키가 반환됩니다. 배포 후에는 Lambda 함수 코드를 수정하여 다른 작업을 수행할 수 있습니다.

- [AWS Secrets Manager 스택 템플릿](#)

가 AWS Transfer Family 서버 AWS Lambda 와 함께 사용하여 Secrets Manager를 자격 증명 공급자로 통합하는 기본 템플릿입니다. 형식 AWS Secrets Manager 의 에 있는 항목에 대해 인증합니다 `aws/transfer/server-id/username`. 또한 암호에는 Transfer Family에 반환된 모든 사용자 속성에 대한 키값 쌍이 들어 있어야 합니다. 배포 후에는 Lambda 함수 코드를 수정하여 다른 작업을 수행할 수 있습니다.

- [Okta 스택 템플릿](#) : AWS Transfer Family 서버 AWS Lambda 와 함께 를 사용하여 Okta를 사용자 지정 자격 증명 공급자로 통합하는 기본 템플릿입니다.

- [Okta-mfa 스택 템플릿](#) : AWS Transfer Family 서버 AWS Lambda 와 함께 를 사용하여 Okta를 사용자 지정 자격 증명 공급자로 MultiFactor 인증과 통합하는 기본 템플릿입니다.
- [Azure Active Directory 템플릿](#): 이 스택에 대한 세부 정보는 [Azure Active Directory 및 를 AWS Transfer Family 사용하여 인증 AWS Lambda](#)블로그 게시물에 설명되어 있습니다.

스택이 배포된 후 CloudFormation 콘솔의 출력 탭에서 스택에 대한 세부 정보를 볼 수 있습니다.

사용자 지정 ID 공급자를 Transfer Family 워크플로에 통합하는 가장 쉬운 방법은 이러한 스택 중 하나를 배포하는 것입니다.

유효 Lambda 값

다음 표에는 사용자 지정 ID 공급자에 사용되는 Lambda 함수에 대해 Transfer Family가 허용하는 값에 대한 세부 정보가 설명되어 있습니다.

값	설명	필수
Role	Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 IAM 역할의 Amazon 리소스 이름 (ARN)을 지정합니다. 이 역할에 연결된 정책은 Amazon S3 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계도 포함되어야 합니다. 신뢰 관계 설정에 대한 자세한 내용은 신뢰 관계를 구축하기 위해를 참조하세요.	필수

값	설명	필수
PosixProfile	Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹 IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.	Amazon EFS 백업 스토리지에 필요
PublicKeys	이 사용자에게 유효한 SSH 퍼블릭 키 값 목록입니다. 목록이 비어 있으면 유효한 로그인이 아님을 의미합니다. 암호 인증 중에는 반환할 수 없습니다.	선택 사항
Policy	여러 사용자 간에 동일한 IAM 역할을 사용할 수 있도록 사용자를 위한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자 액세스의 범위를 축소합니다.	선택 사항

값	설명	필수
HomeDirectoryType	사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. - 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. - 로 설정한 경우 사용자가 Amazon S3 또는 Amazon EFS 경로를 볼 수 있도록 HomeDirectoryDetails 파라미터에 매핑을 제공해야 LOGICAL합니다.	선택 사항
HomeDirectoryDetails	사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 는 경로가 어떻게 표시되는Entry지, 는 실제 Amazon S3 또는 Amazon EFS 경로Target입니다.	HomeDirectoryType 이 LOGICAL의 값을 가진 경우 필요
HomeDirectory	클라이언트를 사용하여 서버에 로그인하는 경우 랜딩 디렉터리(폴더)입니다.	선택 사항

Note

HomeDirectoryDetails 는 JSON 맵의 문자열 표현입니다. 이는 실제 JSON 맵 객체이고 문자열 JSON 배열PosixProfile인 PublicKeys 와는 대조적입니다. 언어별 세부 정보는 코드 예를 참조하세요.

예 Lambda 함수

이 섹션에서는 NodeJS와 Python 모두에서 사용할 수 있는 Lambda 함수 몇 가지를 소개합니다.

Note

이 예제에서는 사용자, 역할, POSIX 프로파일, 암호 및 홈 디렉터리 세부 정보가 모두 예제이므로 실제 값으로 교체해야 합니다.

Logical home directory, NodeJS

다음 NodeJS 예 함수는 [논리적 홈 디렉터리](#)가 있는 사용자에 대한 세부 정보를 제공합니다.

```
// 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 abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // 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

다음 NodeJS 예 함수는 경로 기반의 홈 디렉터리가 있는 사용자에 대한 세부 정보를 제공합니다.

```

// 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: '/fs-faa1a123' // Not required, defaults to '/'
    };
  }
};

```

```

// Check if password is provided
if (!event.password) {
    // If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // 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

다음 Python 예 함수는 [논리적 홈 디렉터리](#)가 있는 사용자에 대한 세부 정보를 제공합니다.

```

# 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

다음 Python 예 함수는 경로 기반 홈 디렉터리가 있는 사용자에 대한 세부 정보를 제공합니다.

```

# 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': '/fs-fs-faa1a123',
    '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

```

구성 테스트

사용자 지정 ID 공급자를 만든 후에는 구성을 테스트해야 합니다.

Console

AWS Transfer Family 콘솔을 사용하여 구성을 테스트하려면

1. [AWS Transfer Family 콘솔](#)을 엽니다.
2. 서버 페이지에서 새 서버를 선택하고 작업을 선택한 다음 테스트를 선택합니다.
3. AWS CloudFormation 스택을 배포할 때 설정한 사용자 이름 및 암호의 텍스트를 입력합니다. 기본 옵션을 유지한 경우 사용자 이름은 myuser 이고 암호는 MySuperSecretPassword입니다.
4. 서버 프로토콜을 선택하고 AWS CloudFormation 스택을 배포할 때 설정한 경우 원본 IP 의 IP 주소를 입력합니다.

CLI

를 사용하여 구성을 테스트하려면 AWS CLI

1. [test-identity-provider](#) 명령을 실행합니다. 다음 단계에서 설명하는 대로 *user input placeholder* 각각을 사용자 고유의 정보로 바꾸세요.

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-name myuser --user-password MySuperSecretPassword --server-protocol FTP --source-ip 127.0.0.1
```

2. 서버 ID를 입력합니다.
3. AWS CloudFormation 스택을 배포할 때 설정한 사용자 이름과 암호를 입력합니다. 기본 옵션을 유지한 경우 사용자 이름은 myuser 이고 암호는 MySuperSecretPassword입니다.
4. AWS CloudFormation 스택을 배포할 때 설정한 경우 서버 프로토콜과 소스 IP 주소를 입력합니다.

사용자 인증에 성공하면 테스트는 StatusCode: 200 HTTP 응답, 빈 문자열Message: ""(그렇지 않으면 실패 이유 포함) 및 Response 필드를 반환합니다.

Note

아래 응답 예제에서 Response 필드는 '문자열화'(프로그램 내에서 사용할 수 있는 플랫폼 JSON 문자열로 변환됨)된 JSON 객체이며 사용자의 역할 및 권한에 대한 세부 정보를 포함합니다.

```
{
  "Response": "{\\\"Policy\\\":\\\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":[\\\"{\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\\":[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",\\\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"],\\\"Resource\\\":\\\"*\\\"}]}\\\",\\\"Role\\\":\\\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\\",\\\"HomeDirectory\\\":\\\"/\\\"}\\\"\",
  \"StatusCode\": 200,
  \"Message\": \"\"
}
```


Amazon API Gateway를 사용하여 자격 증명 공급자 통합

이 주제에서는 AWS Lambda 함수를 사용하여 API Gateway 메서드를 백업하는 방법을 설명합니다. 를 사용하여 자격 증명 공급자 RESTful API를 통합해야 하거나 를 사용하여 지리 차단 또는 속도 제한 요청을 위한 기능을 AWS WAF 활용하려는 경우 이 옵션을 사용합니다.

API Gateway를 사용하여 자격 증명 공급자를 통합하는 경우의 제한 사항

- 이 구성은 사용자 지정 도메인을 지원하지 않습니다.
- 이 구성은 프라이빗 API 게이트웨이 를 지원하지 않습니다 URL.

이 중 하나가 필요한 경우 API Gateway 없이 Lambda를 자격 증명 공급자로 사용할 수 있습니다. 세부 정보는 [AWS Lambda 를 사용하여 자격 증명 공급자 통합](#)을 참조하세요.

API Gateway 메서드를 사용하여 인증

Transfer Family의 자격 증명 공급자로 사용할 API Gateway 메서드를 생성할 수 있습니다. 이 접근 방식은 를 생성하고 제공할 수 있는 매우 안전한 방법을 제공합니다 APIs. API Gateway를 사용하면 HTTPS 엔드포인트를 생성하여 모든 수신 API 통화가 더 높은 보안으로 전송되도록 할 수 있습니다. API Gateway 서비스에 대한 자세한 내용은 [API Gateway 개발자 안내서](#)를 참조하세요.

API Gateway는 라는 권한 부여 방법을 제공합니다. AWS_IAM이 권한 부여 방법은 가 내부적으로 AWS 사용하는 AWS Identity and Access Management (IAM)를 기반으로 동일한 인증을 제공합니다. 를 사용하여 인증을 활성화하면 AWS_IAM를 호출할 명시적 권한이 있는 호출자만 해당 게이트웨이 API API 메서드에 연결할 API 수 있습니다.

API Gateway 메서드를 Transfer Family의 사용자 지정 자격 증명 공급자로 사용하려면 API 를 Gateway 메서드 IAM에 대해 활성화합니다. 이 프로세스의 일환으로 Transfer Family가 게이트웨이를 사용할 수 있는 권한을 IAM 역할에 제공합니다.

Note

보안을 개선하기 위해 웹 애플리케이션 방화벽을 구성할 수 있습니다. AWS WAF 는 Amazon API Gateway로 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽입니다. 세부 정보는 [웹 애플리케이션 방화벽 추가](#)을 참조하세요.

Transfer Family를 사용한 사용자 지정 인증에 API Gateway 메서드를 사용하려면

1. AWS CloudFormation 스택을 생성합니다. 방법:

Note

스택 템플릿이 BASE64인코딩된 암호를 사용하도록 업데이트되었습니다. 자세한 내용은 섹션을 참조하세요 [AWS CloudFormation 템플릿 개선 사항](#).

- <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
- AWS CloudFormation 사용 설명서의 AWS CloudFormation 스택 템플릿 [선택의 기존 템플릿에서 스택을 배포하는](#) 방법에 대한 지침을 따릅니다.
- 다음 기본 템플릿 중 하나를 사용하여 Transfer Family에서 사용자 지정 자격 증명 공급자로 사용할 AWS Lambda지원 API Gateway 메서드를 생성합니다.

- [기본 스택 템플릿](#)

기본적으로 API Gateway 메서드는 하드 코딩된SSH(Secure Shell) 키 또는 암호를 사용하여 단일 서버의 단일 사용자를 인증하는 사용자 지정 자격 증명 공급자로 사용됩니다. 배포 후에는 Lambda 함수 코드를 수정하여 다른 작업을 수행할 수 있습니다.

- [AWS Secrets Manager 스택 템플릿](#)

기본적으로 API Gateway 메서드는 Secrets Manager의 형식 항목에 대해 인증합니다aws/transfer/*server-id/username*. 또한 암호에는 Transfer Family에 반환된 모든 사용자 속성에 대한 키값 쌍이 들어 있어야 합니다. 배포 후에는 Lambda 함수 코드를 수정하여 다른 작업을 수행할 수 있습니다. 자세한 내용은 블로그 게시물 [AWS Transfer Family 사용 시 암호 인증 활성화를 참조하세요 AWS Secrets Manager](#).

- [Okta 스택 템플릿](#)

API Gateway 메서드는 Transfer Family의 사용자 지정 자격 증명 공급자로 Okta와 통합됩니다. 자세한 내용은 블로그 게시물 [Okta를 AWS Transfer Family를 사용한 ID 공급자로서 사용](#)을 참조하세요.

사용자 지정 ID 공급자를 Transfer Family 워크플로에 통합하는 가장 쉬운 방법은 이러한 스택 중 하나를 배포하는 것입니다. 각 스택은 Lambda 함수를 사용하여 API Gateway 기반 API 메서드를 지원합니다. 그런 다음 Transfer Family에서 사용자 지정 자격 증명 공급자로 API 메서드를 사용할 수 있습니다. 기본적으로 Lambda 함수는 암호로 myuser 호출된 단일 사용자를 인증합니다.MySuperSecretPassword 배포 후에는보안 인증 정보를 편집하거나 Lambda 함수 코드를 업데이트하여 다른 작업을 수행할 수 있습니다.

⚠ Important

기본 사용자 및 암호 보안 인증 정보를 편집하는 것이 좋습니다.

스택이 배포된 후 CloudFormation 콘솔의 출력 탭에서 스택에 대한 세부 정보를 볼 수 있습니다. 이러한 세부 정보에는 스택의 Amazon 리소스 이름(ARN), 스택이 생성한 IAM 역할ARN의 , 새 게이트웨이의 URL가 포함됩니다.

i Note

사용자 지정 자격 증명 공급자 옵션을 사용하여 사용자의 암호 기반 인증을 활성화하고 API Gateway에서 제공하는 요청 및 응답 로깅을 활성화하는 경우 API Gateway는 사용자의 암호를 Amazon CloudWatch Logs에 기록합니다. 프로덕션 환경에서는 이 로깅을 사용하지 않는 것이 좋습니다. 자세한 내용은 [API Gateway 개발자 안내서의 Gateway에서 CloudWatch API 로깅 설정을](#) 참조하세요. API

2. 서버의 API 게이트웨이 메서드 구성을 확인합니다. 방법:
 - a. 에서 API 게이트웨이 콘솔을 엽니다<https://console.aws.amazon.com/apigateway/>.
 - b. 템플릿이 생성한 사용자 지정 자격 증명 공급자 기본 템플릿 전송API을 선택합니다. AWS CloudFormation 게이트웨이를 보려면 리전을 선택해야 할 수 있습니다.
 - c. 리소스 창에서 를 선택합니다GET. 다음 스크린샷은 올바른 방법 설정을 보여줍니다.

Method request settings

Authorization: AWS_IAM
API key required: False
Request validator: None
SDK operation name: Generated based on method and path

Request paths (0)

Name	Caching
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)

Content type	Name
No request body defined.	

이제 API 게이트웨이를 배포할 준비가 되었습니다.

- 작업 에서 배포를 API선택합니다. 배포 단계에서 prod를 선택한 다음 배포를 선택합니다.

API Gateway 메시드가 성공적으로 배포되면 다음 스크린샷과 같이 스테이지 > 스테이지 세부 정보 에서 성능을 확인합니다.

Note

화면 상단에 나타나는 호출 URL 주소를 복사합니다. 다음 단계에 필요할 수 있습니다.

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: t8aqrm 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 | Deployment history | Documentation history | Canary | Tags

Stage variables (0/0)

Find resources

Name	Value
No variables	

No variables associated with the stage.

Manage variables

4. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
5. 스택을 생성할 때 Transfer Family가 생성되었어야 합니다. 그렇지 않은 경우 다음 단계를 사용하여 서버를 구성합니다.
 - a. 서버 생성을 선택하여 서버 생성 페이지를 엽니다. 자격 증명 공급자 선택 에서 사용자 지정 을 선택한 다음 다음 다음 스크린샷과 같이 Amazon API Gateway를 사용하여 자격 증명 공급자 에 연결을 선택합니다.

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. Amazon API Gateway 텍스트 제공 URL 상자에 이 절차의 3단계에서 생성한 API Gateway 엔드포인트의 호출 URL 주소를 붙여넣습니다.
- c. 역할 에서 AWS CloudFormation 템플릿에서 생성한 IAM 역할을 선택합니다. 이 역할을 통해 Transfer Family는 API 게이트웨이 메서드를 호출할 수 있습니다.

호출 역할에는 1단계에서 생성한 AWS CloudFormation 스택에 대해 선택한 스택 이름이 포함됩니다. 형식은 다음과 같습니다. **CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI**

- d. 나머지 상자를 채운 다음 서버 만들기를 선택합니다. 서버를 만들기 위한 나머지 단계에 대한 자세한 내용은 [SFTP, FTPS 또는 FTP 서버 엔드포인트 구성](#)을 참조하세요.

API Gateway 메서드 구현

Transfer Family에 대한 사용자 지정 자격 증명 공급자를 생성하려면 API Gateway 메서드에서 리소스 경로가 인 단일 메서드를 구현해야 합니다/servers/**serverId**/users/**username**/config.

serverId 및 **username** 값은 RESTful 리소스 경로에서 가져옵니다. 또한 다음 이미지와 같이 메서드 요청에 **sourceIp** 및 **protocol** URL 쿼리 문자열 파라미터로 추가합니다.

The screenshot displays the AWS Transfer Family console interface for configuring a GET method execution. The left sidebar shows the resource path: `/servers/{serverId}/users/{username}/config`. The main panel shows the method request settings, including authorization (AWS_IAM), request validator (None), API key required (False), and SDK operation name (Generated based on method and path). The request paths section is empty, and the URL query string parameters section shows `protocol` and `sourceIp` as optional parameters.

Note

이 사용자 이름은 최소 3글자에서 최대 100자여야 합니다. 사용자 이름에는 다음 글자를 사용할 수 있습니다. a~z, A~Z, 0~9, 밑줄(_)과 하이픈(-), 마침표(.)과 골뱅이 사인(@)입니다. 그러나 사용자 이름은 하이픈, 마침표 및 @ 기호로 시작할 수 없습니다.

Transfer Family가 사용자를 대신해 암호 인증을 시도하면, 서비스는 `Password:` 헤더 필드를 공급합니다. `Password:` 헤더가 없는 경우, Transfer Family는 퍼블릭 키 인증을 시도하여 사용자를 인증합니다.

ID 공급자를 사용하여 최종 사용자를 인증하고 권한을 부여하는 경우 자격 증명을 검증하는 것 외에도 최종 사용자가 사용하는 클라이언트의 IP 주소를 기반으로 액세스 요청을 허용하거나 거부할 수 있습니다. 이 기능을 사용하면 S3 버킷 또는 Amazon EFS 파일 시스템에 저장된 데이터에 신뢰할 수 있는

것으로 지정한 IP 주소에서만 지원되는 프로토콜을 통해 액세스할 수 있습니다. 이 기능을 활성화하려면 `sourceIp`를 쿼리 문자열에 포함해야 합니다.

서버에 여러 프로토콜을 사용하도록 설정한 상태에서 여러 프로토콜에서 동일한 사용자 이름을 사용하여 액세스를 제공하려는 경우 ID 공급자에 각 프로토콜별 자격 증명이 설정되어 있으면 그렇게 할 수 있습니다. 이 기능을 활성화하려면 RESTful 리소스 경로에 `protocol` 값을 포함해야 합니다.

API Gateway 메서드는 항상 HTTP 상태 코드 200을 반환해야 합니다. 다른 HTTP 상태 코드는 액세스하는 동안 오류가 발생했음을 의미합니다.

Amazon S3 응답 예

예제 응답 본문은 Amazon S3에 대한 다음 양식의 JSON 문서입니다.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/bucketName/path/to/home/directory"
}
```

Note

정책은 문자열 JSON로 이스케이프됩니다. 예:

```
"Policy":
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
  [
    {\"Condition\":
      {\"StringLike\":
        {\"s3:prefix\":
          [\"user/*\", \"user/\"]}},
      \"Resource\": \"arn:aws:s3:::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\"}]
  }"

```

다음 예 응답은 사용자의 홈 디렉터리 타입이 논리적임을 보여줍니다.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\"/\\\"\", \"Target\": \"\\\"/MY-HOME-BUCKET\\\"}]\"",
  "PublicKeys": [""],
}

```

Amazon EFS 예제 응답

예제 응답 본문은 Amazon EFS에 대한 다음 양식의 JSON 문서입니다.

```

{
  "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"
}

```

Role 필드는 인증에 성공했음을 나타냅니다. 암호 인증을 수행할 때(Password: 헤더를 제공할 때) SSH 퍼블릭 키를 제공할 필요가 없습니다. 사용자를 인증할 수 없는 경우(예: 암호가 잘못된 경우) 메시지는 Role 설정되지 않은 응답을 반환해야 합니다. 이러한 응답의 예는 빈 JSON 객체입니다.

다음 예 응답은 사용자가 논리적인 홈 디렉터리 타입을 가졌다는 것을 보여줍니다.

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\\\", \"Target\": \"\\\\/faa1a123\"}]",
  "PublicKeys": [""],
  "PosixProfile": { "Uid": 65534, "Gid": 65534 }
}
```

Lambda 함수에 JSON 형식의 사용자 정책을 포함할 수 있습니다. Transfer Family의 사용자 정책 구성에 대한 자세한 내용은 단원을 참조하세요 [액세스 통제 관리](#).

기본 Lambda 함수

다양한 인증 전략을 구현하려면, 사용자의 게이트웨이 사용하는 Lambda 함수를 편집하세요. 애플리케이션의 요구 사항을 충족하는 데 도움이 되려면 Node.js에서 다음 예 Lambda 함수를 사용할 수 있습니다. 자세한 내용은 [개발자 안내서](#)나 [AWS Lambda Node.js로 Lambda 함수 구축](#)을 참조하세요.

다음 예 Lambda 함수는 사용자 이름, 암호 (암호 인증을 수행하는 경우), 서버 ID, 프로토콜 및 클라이언트 IP 주소를 가져옵니다. 이러한 입력을 조합하여 ID 공급자를 조회하고 로그인을 허용할지 여부를 결정할 수 있습니다.

 Note

서버에 여러 프로토콜을 사용하도록 설정한 상태에서 여러 프로토콜에서 동일한 사용자 이름을 사용하여 액세스를 제공하려는 경우 ID 공급자에 각 프로토콜별 보안 인증이 설정되어 있으면 그렇게 할 수 있습니다.

파일 전송 프로토콜(FTP)의 경우 Secure Shell() 파일 전송 프로토콜(SSH) 및 파일 전송 프로토콜 overSSL(SFTP)와 별도의 보안 인증을 유지하는 것이 좋습니다. FTPS, SFTP 및 와 달리는 보안 인증 정보를 일반 텍스트로 FTPS FTP 전송FTP하므로 에 대한 별도의 보안 인증 정보를 유지하는 것이 좋습니다. SFTP 또는 에서 FTP 보안 인증을 격리하면 FTP 보안 인증 정보가 공유되거나 노출FTP되면 워크로드가 SFTP 또는 를 사용하여 보안이 FTPS 유지됩니다.

이에 함수는 퍼블릭 키 인증을 수행하는 경우 퍼블릭 키와 함께 역할 및 논리적 홈 디렉터리 세부 정보를 반환합니다.

서비스 관리 사용자를 생성할 때는 해당 사용자의 홈 디렉터리를 논리적 또는 물리적 디렉터리로 설정합니다. 마찬가지로 원하는 사용자의 물리적 또는 논리적 디렉터리 구조를 전달하려면 Lambda 함수 결과가 필요합니다. 설정한 파라미터는 의 값에 따라 달라집니다. [HomeDirectoryType](#) 필드.

- HomeDirectoryType 로 설정 PATH- HomeDirectory 필드는 사용자가 볼 수 있는 절대 Amazon S3 버킷 접두사 또는 Amazon EFS 절대 경로여야 합니다.
- HomeDirectoryType을 LOGICAL로 설정 — HomeDirectory 필드를 설정하지 마세요. 대신 의 설명된 값과 마찬가지로 원하는 항목/대상 매핑을 제공하는 HomeDirectoryDetails 필드를 설정합니다. [HomeDirectoryDetails](#) 서비스 관리 사용자를 위한 파라미터입니다.

예 함수는 [예 Lambda 함수](#)에 나열되어 있습니다.

와 함께 사용하기 위한 Lambda 함수 AWS Secrets Manager

를 자격 증명 공급자 AWS Secrets Manager 로 사용하려면 샘플 AWS CloudFormation 템플릿에서 Lambda 함수로 작업할 수 있습니다. Lambda 함수는 사용자 자격 증명으로 Secrets Manager 서비스를 쿼리하고, 성공하면 지정된 시크릿을 반환합니다. Secrets Manager 사용에 대한 자세한 내용은 [AWS Secrets Manager 사용 설명서](#)를 참조하세요.

이 Lambda 함수를 사용하는 샘플 AWS CloudFormation 템플릿을 다운로드하려면 [에서 제공하는 Amazon S3 버킷으로 AWS Transfer Family](#) 이동합니다.

AWS CloudFormation 템플릿 개선 사항

API 게이트웨이 인터페이스가 게시된 CloudFormation 템플릿에 개선되었습니다. 이제 템플릿은 API Gateway에서 BASE64인코딩된 암호를 사용합니다. 기존 배포는 이 개선 사항 없이 계속 작동하지만 기본 미국ASCII 문자 세트 외부의 문자가 있는 암호는 허용하지 않습니다.

이 기능을 활성화하는 템플릿의 변경 사항은 다음과 같습니다.

- GetUserConfigRequest AWS::ApiGateway::Method 리소스에는 이 RequestTemplates 코드가 있어야 합니다(기울임꼴로 표시된 줄은 업데이트된 줄임).

```
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')"
```

- PasswordBase64 헤더를 사용하려면 GetUserConfig 리소스RequestParameters의 를 변경해야 합니다(기울임꼴로 표시된 줄은 업데이트된 줄임).

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
  method.request.querystring.sourceIp: false
```

스택의 템플릿이 최신 버전인지 확인하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 스택 목록에서 스택을 선택합니다.
3. 세부 정보 패널에서 템플릿 탭을 선택합니다.
4. 다음을 찾습니다.

- 를 검색RequestTemplates하고 다음 줄이 있는지 확인합니다.

```
"password":
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
    \',\'','\"')",
```

- 를 검색RequestParameters하고 다음 줄이 있는지 확인합니다.

```
method.request.header.PasswordBase64: false
```

업데이트된 줄이 표시되지 않으면 스택을 편집합니다. AWS CloudFormation 스택을 업데이트하는 방법에 대한 자세한 내용은 AWS CloudFormation, 사용 설명서의 [스택 템플릿 수정](#)을 참조하세요.

논리적 디렉터리를 사용하여 Transfer Family 디렉터리 구조를 단순화합니다.

AWS Transfer Family 서버 디렉터리 구조를 단순화하기 위해 논리적 디렉터리를 사용할 수 있습니다. 논리적 디렉터리를 사용하면 사용자가 Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 연결할 때

탐색하는 사용자 친화적 이름을 사용하는 가상 디렉터리 구조를 구성할 수 있습니다. 논리적 디렉터리를 사용하면 최종 사용자에게 절대 디렉터리 경로, Amazon S3 버킷 이름 및 EFS 파일 시스템 이름을 공개하지 않아도 됩니다.

Note

세션 정책 및 기타 내부 요구 사항의 사용에 따라 다르지만 일반적으로 사용자가 의도한 파일만 액세스하도록 하기 위해 세션 정책과 논리적 디렉터리가 모두 필요하지는 않습니다. 논리적 디렉터리를 설정하는 경우 세션 정책도 생성하지 마세요. 둘 다 있으면 권한 거부 오류가 발생할 수 있습니다.

논리적 디렉터를 사용하여 chroot 작업을 수행하여 스토리지 계층 내에서 사용자의 루트 디렉터를 원하는 위치로 설정할 수 있습니다. 이 모드에서는 사용자가 구성한 홈 또는 루트 디렉터리 외부의 디렉터를 탐색할 수 없습니다.

예를 들어 Amazon S3 사용자는 `/mybucket/home/${transfer:UserName}`까지만 액세스하도록 제한되었지만 일부 클라이언트는 사용자가 폴더를 `/mybucket/home`로 이동할 수 있도록 허용합니다. 이 경우 사용자는 Transfer Family 서버에서 로그아웃했다가 다시 로그인한 후에야 의도한 홈 디렉터리로 돌아갑니다. chroot 작업을 수행하면 이러한 상황이 발생하는 것을 방지할 수 있습니다.

버킷 및 접두사 전체에 고유한 디렉터리 구조를 만들 수 있습니다. 이 기능은 버킷 접두사를 통해 복제할 수 없는 특정 디렉터리 구조가 필요한 워크플로가 있는 경우에 유용합니다. 디렉터리 경로가 파일 시스템의 다른 위치를 참조하는 Linux 파일 시스템에 심볼릭 링크를 생성하는 것과 비슷하게 Amazon S3 내의 여러 비연속 위치에 연결할 수도 있습니다.

논리적 디렉터리 FILE 매핑

이제 HomeDirectoryMapEntry 데이터 유형에 Type 파라미터가 포함됩니다. 이 파라미터가 존재하기 전에 대상이 파일인 논리적 디렉터리 매핑을 만들 수 있었습니다. 이전에 이러한 종류의 논리적 디렉터리 매핑을 생성한 경우 를 Type로 명시적으로 설정해야 합니다. FILE 그렇지 않으면 이러한 매핑이 제대로 작동하지 않습니다.

이렇게 하는 한 가지 방법은 UpdateUser 를 호출API하고 기존 매핑을 FILE 위해 를 Type 로 설정하는 것입니다.

논리적 디렉터리 사용 규칙

논리적 디렉터리 매핑을 구축하기 전에 다음 규칙을 이해해야 합니다.

- Entry이(가) "/"인 경우 경로가 겹칠 수 없으므로 매핑을 하나만 사용할 수 있습니다.
- 논리적 디렉터리는 최대 2.1MB의 매핑을 지원합니다(서비스 관리형 사용자의 경우 이 제한은 2,000개 항목임). 즉, 매핑이 포함된 데이터 구조는 최대 크기가 2.1MB입니다. 매핑이 많은 경우 다음과 같이 매핑 크기를 계산할 수 있습니다.
 1. 일반적인 매핑을 형식으로 작성합니다. {"Entry":"/*entry-path*", "Target":"/*target-path*"}여기서 *entry-path* 및 *target-path*는 사용할 실제 값입니다.
 2. 해당 문자열의 문자 수를 계산한 다음 하나(1)를 추가합니다.
 3. 해당 수에 서버에 대해 가지고 있는 대략적인 매핑 수를 곱합니다.

3단계에서 추정된 수가 2.1MB 미만인 경우 매핑이 허용 한도 내에 있는 것입니다.
- 버킷 또는 파일 시스템 경로가 사용자 이름을 기반으로 파라미터화된 경우 타겟은 \${transfer:UserName} 변수를 사용할 수 있습니다.
- 대상은 서로 다른 버킷 또는 파일 시스템의 경로일 수 있지만 매핑된 AWS Identity and Access Management (IAM) 역할(응답의 Role 파라미터)이 이러한 버킷 또는 파일 시스템에 대한 액세스를 제공하는지 확인해야 합니다.
- HomeDirectory 파라미터 값을 사용할 때 Entry Target 페어에서 이 값을 암시하므로 LOGICAL HomeDirectoryType 파라미터를 지정하지 마세요.
- 대상은 순방향 슬래시(/) 문자로 시작해야 하지만 를 지정할 때는 후행 슬래시(/)를 사용하지 마세요Target. 예를 들어 /*DOC-EXAMPLE-BUCKET*/images는 허용되지만 *DOC-EXAMPLE-BUCKET*/images /*DOC-EXAMPLE-BUCKET*/images/는 허용되지 않습니다.
- Amazon S3는 객체 스토어입니다. 즉, 폴더가 가상 개념이고 실제 디렉터리 계층 구조가 없습니다. 애플리케이션에서 클라이언트의 stat 작업을 발급하는 경우 Amazon S3를 스토리지로 사용할 때 모든 항목이 파일로 분류됩니다. 이 동작은 [Amazon Simple Storage Service 사용 설명서의 폴더를 사용하여 Amazon S3 콘솔에서 객체 구성](#)에 설명되어 있습니다. 애플리케이션에 파일 또는 폴더가 있는지 stat 정확하게 표시해야 하는 경우 Transfer Family 서버의 스토리지 옵션으로 Amazon Elastic File System(AmazonEFS)을 사용할 수 있습니다.
- 사용자의 논리적 디렉터리 값을 지정하는 경우 사용하는 파라미터는 사용자 유형에 따라 달라집니다.
 - 서비스 관리 사용자의 경우 HomeDirectoryMappings에서 논리적 디렉터리 값을 제공하세요.
 - 사용자 지정 자격 증명 공급자 사용자의 경우 에 논리적 디렉터리 값을 제공합니다HomeDirectoryDetails.

⚠ Important

Amazon S3 디렉터리(서버를 생성하거나 업데이트할 때)의 성능을 최적화하도록 선택하지 않는 한 루트 디렉터리는 시작 시 존재해야 합니다. Amazon S3의 경우 루트 폴더를 생성하려면 슬래시(/)로 끝나는 0바이트 객체를 이미 생성했어야 합니다. 이 문제를 피하는 것은 Amazon S3 성능 최적화를 고려해야 하는 이유입니다.

논리적 디렉터리 구현 및 chroot

논리적 디렉터리와 chroot 기능을 사용하려면 다음을 수행해야 합니다:

각 사용자에게 논리적 디렉터를 활성화하세요. 사용자를 만들거나 업데이트할 때 HomeDirectoryType 파라미터를 LOGICAL로 설정하면 됩니다.

```
"HomeDirectoryType": "LOGICAL"
```

chroot

chroot의 경우, 각 사용자에게 대한 단일 Entry 및 Target 쌍으로 구성된 디렉터리 구조를 만드세요. 루트 폴더는 Entry 지점이고 매핑할 버킷 또는 파일 시스템의 Target 위치입니다.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

이전 예와 같이 절대 경로를 사용하거나, 다음 예와 같이 사용자 이름을 동적으로 \${transfer:UserName}로 대체할 수 있습니다.

```
[{"Entry": "/", "Target":  
"/mybucket/${transfer:UserName}"}]
```

위 예에서 사용자는 루트 디렉터리에 잠겨 있어 계층 구조에서 상위 위치로 이동할 수 없습니다.

가상 디렉터리 구조

가상 디렉터리 구조의 경우 사용자의 IAM 역할 매핑에 액세스할 수 있는 권한이 있는 한 여러 버킷 또는 EFS 파일 시스템을 포함하여 S3 버킷 또는 파일 시스템의 모든 위치에 대상으로 여러 Entry Target 페어링을 생성할 수 있습니다.

다음 가상 구조 예제에서는 사용자가 에 로그인하면 AWS SFTP, , 및 하위 디렉터리가 있는 루트 디렉터리에 있습니다/pics/doc/reporting/anotherpath/subpath/financials.

Note

Amazon S3 디렉터리의 성능을 최적화하기로 선택하지 않는 한(서버를 생성하거나 업데이트 할 때) 사용자 또는 관리자가 디렉터리가 아직 없는 경우 디렉터리를 생성해야 합니다. 이 문제를 피하는 것은 Amazon S3 성능 최적화를 고려해야 하는 이유입니다.

Amazon 의 EFS경우 관리자가 논리적 매핑 또는 / 디렉터리를 생성해야 합니다.

```
[
{"Entry": "/pics", "Target": "/bucket1/pics"},
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/financials"}]
```

Note

매핑한 특정 폴더에만 파일을 업로드할 수 있습니다. 즉, 이전 예에서는 /anotherpath 또는 anotherpath/subpath 디렉터리에는 업로드할 수 없고; anotherpath/subpath/financials에만 업로드할 수 있습니다. 또한 경로가 겹칠 수 없으므로 이러한 경로에 직접 매핑할 수 없습니다.

예를 들어, 다음 매핑을 형성한다고 가정하겠습니다:

```
{
  "Entry": "/pics",
  "Target": "/mybucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/mybucket/mydocs"
```



```

},
{
  "Entry": "/temp",
  "Target": "/mybucket"
}

```

해당 버킷에만 파일을 업로드할 수 있습니다. sftp를 통해 처음 연결하면 루트 디렉터리인 /(으)로 이동됩니다. 해당 디렉터리에 파일을 업로드하려고 하면 업로드가 실패합니다. 다음 명령은 예 순서를 나타냅니다:

```

sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory

```

임의의 directory/sub-directory 위치에 업로드하려면 경로를 sub-directory에 명시적으로 매핑해야 합니다.

다운로드하여 사용할 수 있는 AWS CloudFormation 템플릿을 포함하여 사용자를 chroot 위한 논리적 디렉터리 구성에 대한 자세한 내용은 AWS 스토리지 블로그의 [chroot 및 논리적 디렉터리를 사용하여 구조 단순화를 참조하세요 AWS SFTP](#).

논리적 디렉터리 구성 예

이 예에서는 사용자를 생성하고 두 개의 논리적 디렉터를 할당합니다. 다음 명령을 실행하면 (기존 Transfer Family 서버의 경우) 논리적 디렉터리 pics 및 doc 를 사용하여 새 사용자가 만들어집니다.

```

aws transfer create-user --user-name marymajor-logical --server-id s-11112222333344445
--role arn:aws:iam::1234abcd5678:role/marymajor-role --home-directory-type LOGICAL \
--home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/DOC-EXAMPLE-BUCKET1/
pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]" \
--ssh-public-key-body file://~/.ssh/id_rsa.pub

```

marymajor가 기존 사용자이고 홈 디렉터리 타입이 PATH인 경우 이전 사용자와 비슷한 명령을 사용하여 그것을 LOGICAL로 변경할 수 있습니다.

```

aws transfer update-user --user-name marymajor-logical \

```

```
--server-id s-11112222333344445 --role arn:aws:iam::1234abcd5678:role/marymajor-role \
--home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/pics\",
\"Target\":\"/DOC-EXAMPLE-BUCKET1/pics\"}, \
{\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]"]
```

유념할 사항:

- 디렉터리 `/DOC-EXAMPLE-BUCKET1/pics` 및 `/DOC-EXAMPLE-BUCKET2/test/mydocs` 없는 경우 사용자 (또는 관리자) 가 해당 디렉터리를 만들어야 합니다.
- **marymajor**이 서버에 연결되어 `ls -l` 명령을 실행하면 다음과 같은 내용이 표시됩니다:

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor**은(는) 이 수준에서는 파일이나 디렉터리를 만들 수 없습니다. 하지만 `pics` 및 `doc` 내에서 하위 디렉토리를 추가할 수는 있습니다.
- `pics` 및 `doc`에 추가되는 파일은 각각 Amazon S3 경로 `/DOC-EXAMPLE-BUCKET1/pics` 및 `/DOC-EXAMPLE-BUCKET2/test/mydocs`에 추가됩니다.
- 이 예에서는 이러한 가능성을 설명하기 위해 서로 다른 두 개의 버킷을 지정합니다. 하지만 사용자에게 대해 지정한 여러 논리 디렉터리 또는 모든 논리적 디렉터리에 동일한 버킷을 사용할 수 있습니다.

Amazon용 논리적 디렉터리 구성 EFS

Transfer Family 서버가 Amazon EFS를 사용하는 경우 사용자가 논리적 EFS 홈 디렉터리에서 작업하기 전에 읽기 및 쓰기 액세스 권한으로 사용자의 홈 디렉터리를 생성해야 합니다. 사용자는 논리적 홈 디렉터리 상의 `mkdir`에 대한 권한이 없기 때문에 이 디렉터리를 직접 만들 수는 없습니다.

사용자의 홈 디렉터리가 존재하지 않고 사용자가 `ls` 명령을 실행하면 시스템은 다음과 같이 응답합니다:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

상위 디렉터리에 대한 관리 액세스 권한이 있는 사용자는 사용자의 논리적 홈 디렉터리를 생성해야 합니다.

사용자 지정 AWS Lambda 응답

맞춤 ID 공급자에 연결하는 Lambda 함수와 함께 논리적 디렉터리를 사용할 수 있습니다. 이렇게 하려면 Lambda 함수에서 HomeDirectoryType를 **LOGICAL**(으)로 지정하고, HomeDirectoryDetails 파라미터에 Entry와(과) Target를 추가합니다. 예:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{"Entry": "\\", "Target": "\/DOC-EXAMPLE-BUCKET/
theRealFolder"}]"
```

다음 코드는 맞춤 Lambda 인증 호출로부터의 응답 성공의 예입니다.

```
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\\\": \\\"/DOC-EXAMPLE-BUCKET/theRealFolder\\\"}]\\\", \"PublicKeys\":
\\\"[ssh-rsa myrsapubkey]\\\"\",
  \"StatusCode\": 200
}
```

Note

Gateway API 메서드를 사용자 지정 자격 증명 공급자로 사용하는 경우에만 "Url": 라인이 반환됩니다.

AWS Transfer Family SFTP 커넥터

AWS Transfer Family SFTP 커넥터는 SFTP 프로토콜을 사용하여 Amazon 스토리지와 외부 파트너 간에 파일 및 메시지를 보내기 위한 관계를 설정합니다. Amazon S3에서 파트너 소유의 외부 대상으로 파일을 보낼 수 있습니다. SFTP 커넥터를 사용하여 파트너의 SFTP 서버에서 파일을 검색할 수도 있습니다.

Note

현재 SFTP 커넥터는 인터넷에 액세스할 수 있는 엔드포인트를 제공하는 원격 SFTP 서버에 연결하는 데만 사용할 수 있습니다.

Transfer Family [AWS Transfer Family SFTP 커넥터](#)에 대한 간략한 소개는 SFTP 커넥터를 참조하세요.

주제

- [SFTP 커넥터 구성](#)
- [SFTP 커넥터를 사용하여 파일 전송 및 검색](#)
- [SFTP 커넥터 관리](#)

SFTP 커넥터 구성

이 주제에서는 SFTP 커넥터를 생성하는 방법, 커넥터와 연결된 보안 알고리즘, 보안 인증 정보를 보관할 보안 암호를 저장하는 방법, 프라이빗 키 형식 지정에 대한 세부 정보 및 커넥터 테스트 지침을 설명합니다.

주제

- [SFTP 커넥터 생성](#)
- [SFTP 커넥터 알고리즘](#)
- [SFTP 커넥터와 함께 사용할 보안 암호 저장](#)
- [SFTP 커넥터 프라이빗 키 생성 및 형식 지정](#)
- [SFTP 커넥터 테스트](#)

SFTP 커넥터 생성

이 절차에서는 AWS Transfer Family 콘솔 또는 CLI를 사용하여 SFTP 커넥터를 생성하는 방법을 설명합니다.

Console

SFTP 커넥터를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택한 다음 커넥터 생성을 선택합니다.
3. 커넥터 유형을 SFTP 선택하여 SFTP 커넥터를 생성한 다음 다음을 선택합니다.

Transfer Family > Connectors > Create connector

Create connector Info

Create a connector that will be used to connect to your trading partner's server

Choose the connector type
Choose the protocol of the remote server to create a connector

☒ **SFTP**
Create a connector to connect to remote SFTP server

☐ **AS2**
Create a connector to connect to your trading partner's AS2 server

Cancel **Next**

4. 커넥터 구성 섹션에서 다음 정보를 제공합니다:
 - 에 원격 SFTP 서버의 URL을 URL입력합니다. 예를 들어 와 `sftp://partner-SFTP-server-url` 같이 형식이 여야 URL 합니다 `sftp://AnyCompany.com`.

Note

선택적으로 에 포트 번호를 제공할 수 있습니다URL. 형식은 `sftp://partner-SFTP-server-url:port-number`입니다. 기본 포트 번호(지정된 포트가 없는 경우)는 포트 22입니다.

- 액세스 역할 에서 사용할 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)을 선택합니다.
- 이 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 이 역할이 제공하는지 확인하세요.
- 이 역할이 secretsmanager:GetSecretValue에 대해 암호에 액세스할 수 있는 권한을 제공하는지 확인하세요.

 Note

정책에서 보안 암호에 ARN 대해 를 지정해야 합니다. 예는 보안 암호 이름이 ARN 포함되어 있지만 이름에 6자의 임의의 영숫자를 추가합니다. 암호ARN의 는 다음 형식을 갖습니다.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- 사용자의 이전 요청을 처리할 때 커넥터가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 이 역할에 포함되어 있는지 확인하세요. 신뢰 관계 설정에 대한 자세한 내용은 [신뢰 관계를 구축하기 위해](#)을 참조하세요.

다음 예제에서는 예 액세스하는 데 필요한 권한을 부여합니다.*DOC-EXAMPLE-BUCKET* Amazon S3 Secrets Manager에 저장된 지정된 보안 암호.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
```

```

    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters"
}
]
}

```

Note

액세스 역할의 경우, 예는 단일 암호에 대한 액세스 권한을 부여합니다. 그러나 와 일드카드 문자를 사용하면 여러 사용자 및 보안 암호에 동일한 IAM 역할을 재사용하려는 경우 작업을 저장할 수 있습니다. 예컨대, 다음 리소스 명령문은 `aws/transfer`으로 시작하는 이름을 가진 모든 암호에 대한 권한을 부여합니다.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

SFTP 자격 증명이 포함된 보안 암호를 다른 에 저장할 수도 있습니다 AWS 계정. 교차 계정 보안 암호 액세스를 활성화하는 방법에 대한 자세한 내용은 [다른 계정의 사용자 보안 AWS Secrets Manager 암호에 대한 권한 섹션을 참조하세요](#).

- (선택 사항) 로깅 역할 에서 이벤트를 CloudWatch 로그로 푸시하는 데 사용할 커넥터의 IAM 역할을 선택합니다. 다음 예제 정책은 SFTP 커넥터에 대한 이벤트를 로깅하는 데 필요한 권한을 나열합니다.

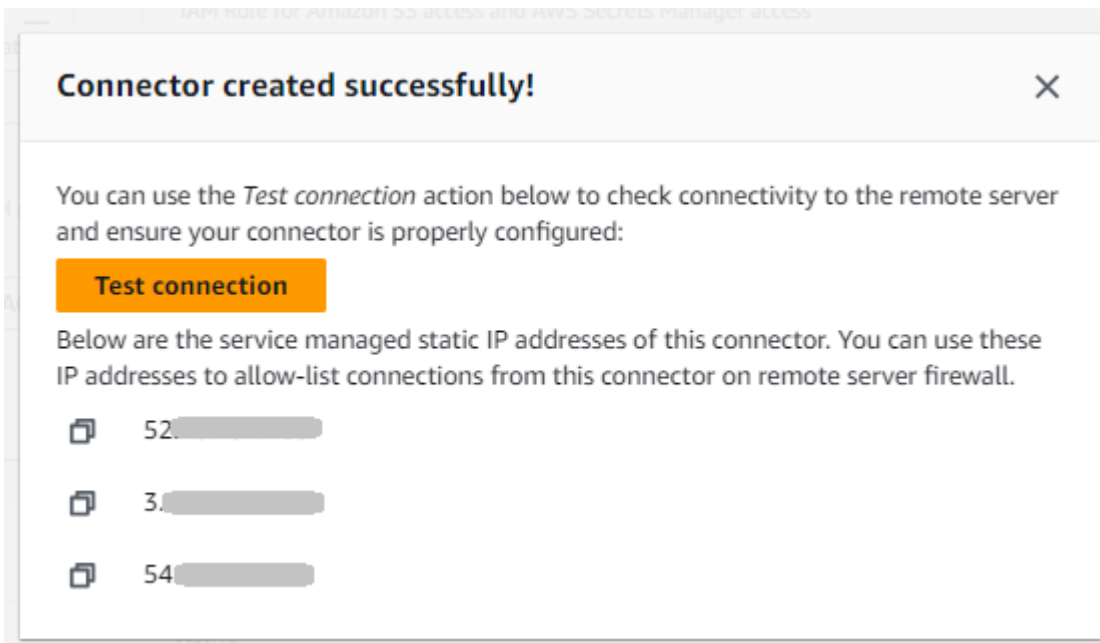
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "SFTPConnectorPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    ]
  }]
}
```

5. SFTP 구성 섹션에서 다음 정보를 제공합니다.

- 커넥터 보안 인증 정보의 드롭다운 목록에서 SFTP 사용자의 프라이빗 키 또는 암호 AWS Secrets Manager가 포함된 보안 암호 이름을 선택합니다. 암호를 생성하여 특정 방식으로 저장해야 합니다. 자세한 내용은 [SFTP 커넥터와 함께 사용할 보안 암호 저장](#)을 참조하세요.
- 신뢰 호스트 키 - 외부 서버를 식별하는 데 사용되는 호스트 키의 공개 부분에 붙여 넣습니다. 신뢰 호스트 키 추가를 선택하여 키를 더 추가하면 키를 두 개 이상 추가할 수 있습니다. SFTP 서버에 대한 ssh-keyscan 명령을 사용하여 필요한 키를 검색할 수 있습니다. Transfer Family가 지원하는 신뢰할 수 있는 호스트 키의 형식 및 유형에 대한 자세한 내용은 섹션을 참조하세요. [SFTPConnectorConfig](#).

6. (옵션) 태그 섹션에서 키 및 값에 하나 이상의 태그를 키-값 쌍을 입력합니다.

7. 모든 설정을 확인한 후 커넥터 생성을 선택하여 SFTP 커넥터를 생성합니다. 커넥터가 성공적으로 생성되면 할당된 정적 IP 주소 목록과 연결 테스트 버튼이 포함된 화면이 나타납니다. 버튼을 사용하여 새 커넥터의 구성을 테스트합니다.



새 커넥터의 ID가 목록에 추가된 SFTP 커넥터 페이지가 나타납니다. 커넥터에 대한 세부 정보를 보려면 [SFTP 커넥터 세부 정보 보기](#) 섹션을 참조하세요.

CLI

를 사용합니다. [create-connector](#) 명령을 사용하여 커넥터를 생성합니다. 이 명령을 사용하여 SFTP 커넥터를 생성하려면 다음 정보를 제공해야 합니다.

- 원격 SFTP 서버의 URL . 예를 들어 와 `sftp://partner-SFTP-server-url` 같이 형식이 여야 URL 합니다 `sftp://AnyCompany.com`.
- 액세스 역할입니다. 사용할 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)을 선택합니다.
- 이 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 이 역할이 제공하는지 확인하세요.
- 이 역할이 `secretsmanager:GetSecretValue`에 대해 암호에 액세스할 수 있는 권한을 제공하는지 확인하세요.

Note

정책에서 보안 암호에 ARN 대해 를 지정해야 합니다. 예는 보안 암호 이름이 ARN 포함되어 있지만 이름에 6자의 임의의 영숫자를 추가합니다. 암호ARN의 는 다음 형식을 갖습니다.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- 사용자의 이전 요청을 처리할 때 커넥터가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 이 역할에 포함되어 있는지 확인하세요. 신뢰 관계 설정에 대한 자세한 내용은 [신뢰 관계를 구축하기 위해](#)를 참조하세요.

다음 예제에서는 이 액세스하는 데 필요한 권한을 부여합니다.*DOC-EXAMPLE-BUCKET* Amazon S3 Secrets Manager에 저장된 지정된 보안 암호.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
```

```

    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

액세스 역할의 경우, 예는 단일 암호에 대한 액세스 권한을 부여합니다. 그러나 와일드카드 문자를 사용하면 여러 사용자 및 보안 암호에 동일한 IAM 역할을 재사용하려는 경우 작업을 저장할 수 있습니다. 예컨대, 다음 리소스 명령문은 aws/transfer으로 시작하는 이름을 가진 모든 암호에 대한 권한을 부여합니다.

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"

```

SFTP 자격 증명이 포함된 보안 암호를 다른 계정에 저장할 수도 있습니다 AWS 계정. 교차 계정 보안 암호 액세스를 활성화하는 방법에 대한 자세한 내용은 [다른 계정의 사용자 보안 AWS Secrets Manager 암호에 대한 권한 섹션을 참조하세요](#).

- (선택 사항) CloudWatch 로그에 이벤트를 푸시하는 데 사용할 커넥터의 IAM 역할을 선택합니다. 다음 예제 정책은 SFTP 커넥터에 대한 이벤트를 로깅하는 데 필요한 권한을 나열합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "SFTPConnectorPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    ]
  }]
}

```

```
}
```

- 다음 SFTP 구성 정보를 제공합니다.
 - SFTP 사용자의 프라이빗 키 또는 암호 AWS Secrets Manager 가 포함된 의 ARN 보안 암호.
 - 외부 서버를 식별하는 데 사용되는 호스트 키의 공개 부분입니다. 원하는 경우 신뢰 호스트 키를 여러 개 제공할 수 있습니다.

SFTP 정보를 제공하는 가장 쉬운 방법은 파일에 저장하는 것입니다. 예컨대, 다음 예 텍스트를 testSFTPConfig.json이라는 파일에 복사합니다.

```
// 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="
  ]
}
```

Note

는 보안 암호SecretId의 전체 ARN 또는 이름(*example-username-key* 이전 목록에서 참조).

이제 다음 명령을 실행하여 커넥터를 생성합니다.

```
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
```

SFTP 커넥터 알고리즘

SFTP 커넥터를 생성하면 다음 보안 알고리즘이 커넥터에 연결됩니다.

유형	알고리즘
SSH 암호	aes256-gcm@openssh.com aes128-gcm@openssh.com aes256-ctr aes192-ctr
SSH 키 교환 메서드(KEX)	curve25519-sha256 curve25519-sha256@libssh.org diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256
SSH MAC	hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-256
SSH 호스트 키	ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 rsa-sha2-512 rsa-sha2-256

SFTP 커넥터와 함께 사용할 보안 암호 저장

Secrets Manager를 사용하여 SFTP 커넥터에 대한 사용자 보안 인증을 저장할 수 있습니다. 암호를 생성할 때 사용자 이름을 입력해야 합니다. 또한 암호, 프라이빗 키 또는 둘 다 제공할 수 있습니다. 세부 정보는 [SFTP 커넥터 할당량](#)을 참조하세요.

Note

Secrets Manager에 암호를 저장하면 AWS 계정 에 요금이 발생합니다. 요금에 대한 자세한 내용은 [AWS Secrets Manager 요금](#)을 참조하세요.

SFTP 커넥터의 Secrets Manager에 사용자 자격 증명을 저장하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Secrets Manager 콘솔을 엽니다 <https://console.aws.amazon.com/secretsmanager/>.
2. 왼쪽 탐색 창에서 암호를 선택합니다.
3. 암호 페이지에서 새 암호 저장을 선택합니다.
4. 암호 선택 페이지의 암호 타입에서 다른 타입의 암호를 선택합니다.
5. 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

- 키 - **Username**를 입력합니다.
- 값 - 파트너 서버에 연결할 권한이 있는 사용자의 이름을 입력합니다.

6. 암호를 제공하려면 행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

- 키 - **Password**를 입력합니다.
- 값 - 사용자의 암호를 입력합니다.

7. 프라이빗 키를 제공하려면 프라이빗 키 데이터를 입력하는 방법에 대해 설명하는 [SFTP 커넥터 프라이빗 키 생성 및 형식 지정](#) 섹션을 참조하세요.

Note

입력한 프라이빗 키 데이터는 원격 SFTP 서버에 이 사용자에게 저장된 퍼블릭 키와 일치해야 합니다.

8. Next(다음)를 선택합니다.
9. 암호 구성 페이지에 암호를 위한 명칭과 설명을 입력합니다. 이름에 **aws/transfer/**이라는 접두사를 사용하는 것이 좋습니다. 예컨대, 암호 **aws/transfer/connector-1**을 지정할 수 있습니다.
10. 다음을 선택한 후 교체 구성 페이지의 기본값을 그대로 사용합니다. 그 다음 다음을 선택합니다.
11. 검토 페이지에서 저장을 선택하여 암호를 만들고 저장합니다.

SFTP 커넥터 프라이빗 키 생성 및 형식 지정

퍼블릭/프라이빗 키 페어를 생성하기 위한 전체 세부 정보는 [여기](#)에 설명되어 있습니다. [macOS, Linux 또는 Unix에서 SSH 키 생성](#).

예를 들어 SFTP 커넥터와 함께 사용할 프라이빗 키를 생성하려면 다음 샘플 명령이 올바른 유형의 키를 생성합니다(교체 **key_name** 키 페어의 실제 파일 이름과 함께):

```
ssh-keygen -t rsa -b 4096 -m PEM -f key_name -N ""
```

Note

SFTP 커넥터와 함께 사용할 키 페어를 생성할 때는 암호문을 사용하지 마세요. SFTP 구성이 올바르게 작동하려면 빈 암호가 필요합니다.

이 명령은 RSA 키 크기가 4096비트인 키 페어를 생성합니다. 키는 SFTP 커넥터 보안 암호와 함께 사용하기 위해 Transfer Family에서 요구하는 레거시 PEM 형식으로 생성됩니다. 키는 현재 디렉터리, 즉 `ssh-keygen` 명령을 실행하는 디렉터리의 **key_name** (프라이빗 키) 및 **key_name.pub** (퍼블릭 키)에 저장됩니다.

Note

Transfer Family는 SFTP 커넥터에 사용되는 키에 대해 OpenSSH 형식(-----BEGIN OPENSSH PRIVATE KEY-----)을 지원하지 않습니다. 키는 레거시 PEM 형식(-----BEGIN RSA PRIVATE KEY----- 또는 -----BEGIN EC PRIVATE KEY-----)이어야 합니다. `ssh-keygen` 도구를 사용하여 명령을 실행할 때 `-m PEM` 옵션을 제공하여 키를 변환할 수 있습니다.

키를 생성한 후 프라이빗 키의 형식이 포함된 새 줄 문자('\n')로 JSON 지정되어 있는지 확인해야 합니다.

명령을 사용하여 기존 프라이빗 키를 올바른 형식, 즉JSON 새 줄 문자가 포함된 형식으로 변환합니다. 여기에서jq는 및 Powershell에 대한 예를 제공합니다. 프라이빗 키를 새 줄 문자가 포함된 JSON 형식으로 변환하려는 모든 도구 또는 명령을 사용할 수 있습니다.

jq command

이 예제에서는 [Download jq](#) 에서 다운로드할 수 있는 jq 명령을 사용합니다.

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

예를 들어 프라이빗 키 파일이 에 있는 경우 ~/.ssh/my_private_key명령은 다음과 같습니다.

```
jq -sR . ~/.ssh/my_private_key
```

이렇게 하면 키를 올바른 형식(새 줄 문자가 포함된)으로 표준 출력으로 출력합니다.

PowerShell

Windows를 사용하는 경우 PowerShell 를 사용하여 키를 올바른 형식으로 변환할 수 있습니다. 다음 Powershell 명령은 프라이빗 키를 올바른 형식으로 변환합니다.

```
Get-Content -Raw path-to-private-key-file | ConvertTo-Json
```

SFTP 커넥터와 함께 사용할 프라이빗 키 데이터를 보안 암호에 추가하려면

1. Secrets Manager 콘솔에서 기타 타입의 암호를 저장할 때 일반 텍스트 탭을 선택합니다. 텍스트는 비어 있어야 하며 여는 중괄호와 닫는 중괄호({})만 있어야 합니다.
2. 다음 형식을 사용하여 사용자 이름, 프라이빗 키 데이터 및/또는 암호를 붙여 넣습니다. 프라이빗 키 데이터의 경우 1단계에서 실행한 명령의 출력을 붙여 넣습니다.

```
{"Username": "SFTP-USER", "Password": "SFTP-USER-PASSWORD", "PrivateKey": "PASTE-PRIVATE-KEY-DATA-HERE"}
```




프라이빗 키 데이터를 올바르게 붙여 넣으면 키/값 탭을 선택할 때 다음과 같은 내용이 표시됩니다. 프라이빗 키 데이터는 연속 텍스트 문자열 line-by-line이 아닌 로 표시됩니다.

Secret value [Info](#)
Retrieve and view the secret value.

Key/value | Plaintext

Secret key	Secret value
Username	SFTP-USER
Password	SFTP-USER-PASSWORD
PrivateKey	-----BEGIN RSA PRIVATE KEY----- MITMw... g... a... U... G... g... T... a... I... W... I... A... e... 5... 7... H... i... By...

3. 8단계의 [SFTP 커넥터와 함께 사용할 보안 암호 저장](#)의 절차를 계속하고 끝까지 해당 절차를 따르세요.

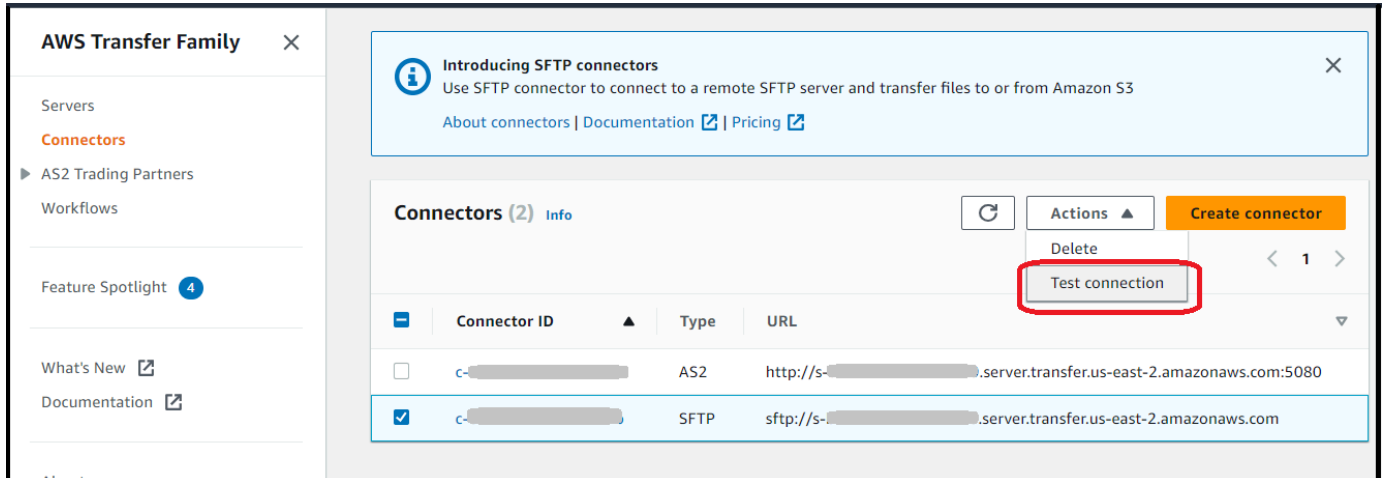
SFTP 커넥터 테스트

SFTP 커넥터를 생성한 후에는 새 커넥터를 사용하여 파일을 전송하기 전에 테스트하는 것이 좋습니다.

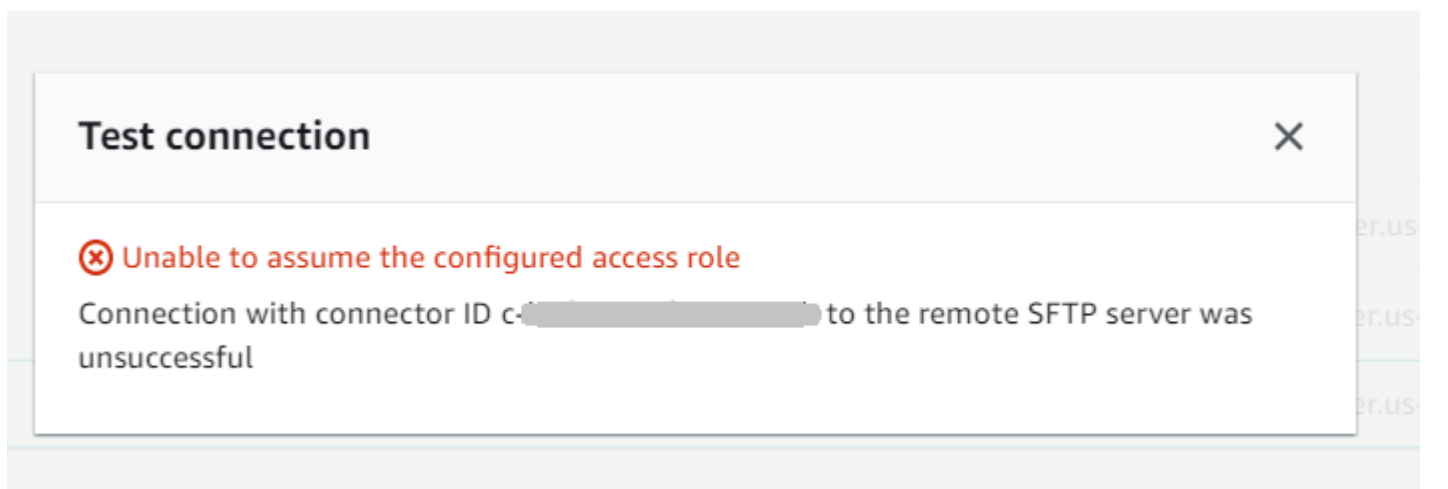
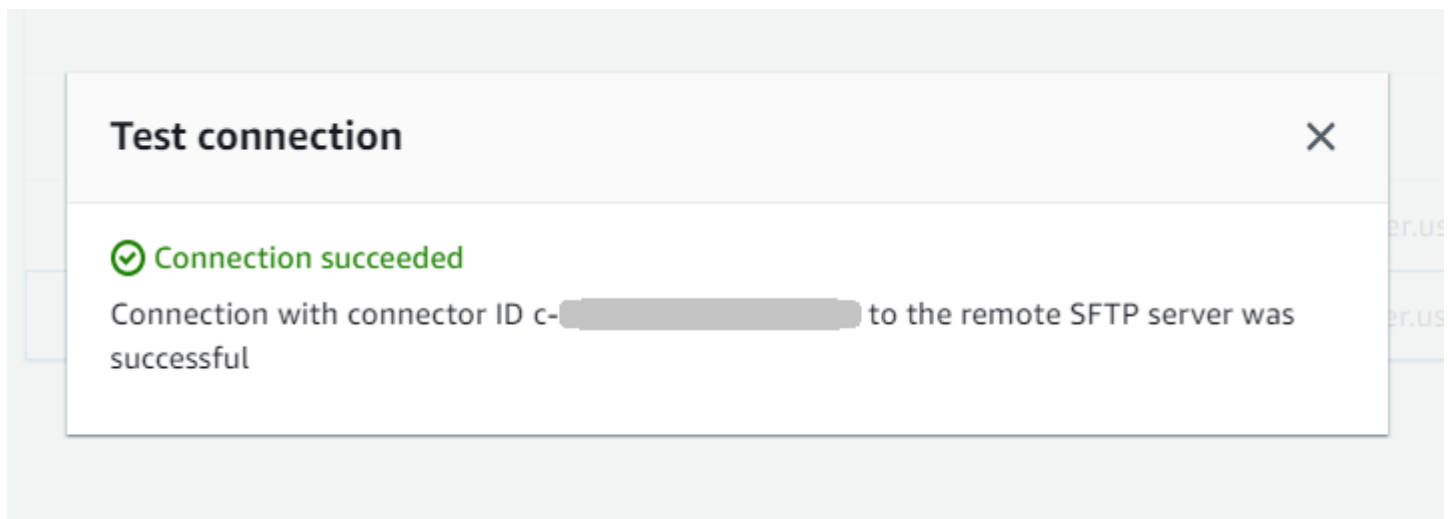
SFTP 커넥터를 테스트하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택하고 커넥터를 선택합니다.

3. 작업 메뉴에서 테스트 연거을 선택합니다.



시스템은 테스트의 통과 또는 실패 여부를 나타내는 메시지를 반환합니다. 테스트가 실패하면 시스템은 테스트 실패 이유를 기반으로 오류 메시지를 제공합니다.



Note

API 를 사용하여 커넥터를 테스트하려면 [TestConnection](#) API 설명서.

SFTP 커넥터를 사용하여 파일 전송 및 검색

SFTP 커넥터는 의 기능을 확장 AWS Transfer Family 하여 클라우드 및 온프레미스 모두에서 원격 서버와 통신합니다. 원격 소스에서 생성 및 저장된 데이터를 분석, 비즈니스 애플리케이션, 보고 및 감사를 위해 AWS 호스팅된 데이터 웨어하우스와 통합할 수 있습니다. 원격 SFTP 서버로 파일 전송을 시작하려면 [StartFileTransfer](#) API SFTP 커넥터를 사용하여 전송을 수행하는 작업입니다. 각 StartFileTransfer 요청에는 10개의 고유한 경로가 포함될 수 있습니다.

서버 로그를 확인하여 파일 전송을 모니터링할 수 있습니다. 커넥터 활동은 `aws/transfer/connector-id` 형식(예: `aws/transfer/c-1234567890abcdef0`)의 로그 스트림에 기록됩니다. 커넥터에 대한 로그가 표시되지 않는 경우 커넥터에 대한 올바른 권한을 가진 로깅 역할을 지정했는지 확인하세요.

커넥터 생성에 대한 자세한 설명은 [SFTP 커넥터 구성](#) 섹션을 참조하세요.

SFTP 커넥터를 사용하여 파일을 전송하고 검색하려면 `start-file-transfer` AWS Command Line Interface (AWS CLI) 명령을 사용합니다. 파일 전송(아웃바운드 전송) 또는 파일 수신(인바운드 전송) 여부에 따라 다음 매개 변수를 지정합니다.

- 아웃바운드 전송
 - `send-file-paths`에는 파트너의 SFTP 서버로 파일을 전송할 수 있는 소스 파일 경로가 1~10 개 있습니다.
 - `remote-directory-path`는 고객 SFTP 서버의 에 파일을 보내는 원격 경로입니다.
- 인바운드 전송
 - `retrieve-file-paths`에는 1~10개의 원격 경로가 포함됩니다. 각 경로는 파트너의 서버에서 Transfer Family SFTP 서버로 파일을 전송할 위치를 지정합니다.
 - `local-directory-path`는 파일이 저장되는 Amazon S3 위치 (버킷 및 선택적 접두사) 입니다.

파일을 보내려면 `send-file-paths` 및 `remote-directory-path` 파라미터를 지정합니다. 최대 10개의 파일을 `send-file-paths` 파라미터에 지정할 수 있습니다. 다음 예제 명령은 Amazon S3 스토리지에 `/DOC-EXAMPLE-SOURCE-BUCKET/file2.txt` 있는 `/DOC-EXAMPLE-SOURCE-BUCKET/`

file1.txt 및 이라는 파일을 파트너 SFTP 서버의 /tmp 디렉터리로 보냅니다. 이 예 명령을 사용하려면 *DOC-EXAMPLE-SOURCE-BUCKET*를 실제 버킷으로 대체하세요.

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/
file1.txt /DOC-EXAMPLE-SOURCE-BUCKET/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

파일을 수신하려면 retrieve-file-paths 및 local-directory-path 파라미터를 지정합니다. 다음 예제에서는 파트너의 SFTP 서버에서 /my/remote/file1.txt 및 파일을 검색하여 Amazon S3 위치 //my/remote/file2.txt에 배치합니다. *DOC-EXAMPLE-BUCKET/prefix*. 이 예제 명령을 사용하려면 *user input placeholders*를 자체 정보로 바꿉니다.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/
remote/file2.txt \
  --local-directory-path /DOC-EXAMPLE-BUCKET/prefix --connector-id c-2222BBBB3333CCCC4
--region us-east-2
```

이전 예제에서는 SFTP 서버의 절대 경로를 지정합니다. 상대 경로, 즉 SFTP 사용자의 홈 디렉터리에 상대적인 경로를 사용할 수도 있습니다. 예를 들어, SFTP 사용자가 marymajor 이고 SFTP 서버의 홈 디렉터리가 인 경우 /users/marymajor/다음 명령은 */DOC-EXAMPLE-SOURCE-BUCKET/file1.txt*로 전송합니다. /users/marymajor/test-connectors/file1.txt

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/file1.txt
\
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

SFTP 커넥터 관리

이 주제에서는 SFTP 커넥터를 보고 업데이트하는 방법을 설명하고 SFTP 커넥터와 관련된 할당량을 나열합니다.

주제

- [SFTP 커넥터 업데이트](#)
- [SFTP 커넥터 세부 정보 보기](#)
- [SFTP 커넥터 할당량](#)

SFTP 커넥터 업데이트

커넥터의 기존 파라미터 값을 변경하려면 `update-connector` 명령을 실행하면 됩니다. 다음 명령은 지역의 커넥터 `connector-id`의 암호를 `region-id`에서 `secret-ARN`로 업데이트합니다. 이 예 명령을 사용하려면 `user input placeholders`를 실제 정보로 대체하세요.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
--connector-id connector-id --region region-id
```

SFTP 커넥터 세부 정보 보기

AWS Transfer Family 콘솔에서 SFTP 커넥터에 대한 세부 정보 및 속성 목록을 찾을 수 있습니다.

커넥터 세부 정보를 보려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택합니다.
3. 커넥터 ID 옆에서 식별자를 선택하면 선택한 커넥터의 세부 정보 페이지가 표시됩니다.

SFTP 커넥터 세부 정보 페이지에서 편집을 선택하여 커넥터의 속성을 변경할 수 있습니다.

[Transfer Family](#) > [Connectors](#) > c-

C-
Delete

Connector configuration Info

Edit

URL 📄 sftp:// 	Access role transfer-s3 🔗	Logging role role 🔗

SFTP configuration

Edit

Connector credentials 📄 arn:aws:secretsmanager:us- 🔗	Trusted host keys 1. SHA256

Egress IP details Info

Service managed static IP addresses of this connector

📄	52.
📄	3.
📄	54.

Tags (0)

Manage tags

🔍

<
1
>

Key	Value

i Note

다음 AWS Command Line Interface (AWS CLI) 명령을 실행하면 다른 형식이지만 이 정보의 대부분을 얻을 수 있습니다. 이 예 명령을 사용하려면 *user input placeholders*를 실제 정보로 대체하세요.

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

자세한 내용은 [단원을 참조하세요.DescribeConnector](#) API 참조에 있습니다.

SFTP 커넥터 할당량

SFTP 커넥터에는 다음 할당량이 적용됩니다. AS2 커넥터의 할당량은 [여기](#)에 설명되어 있습니다. [AS2 할당량 및 제한](#). 조정 가능한 할당량 증가를 요청하려면 AWS 일반 참조의 [AWS 서비스 할당량](#)을 참조하세요.

SFTP 커넥터 할당량

명칭	기본값	조정 가능
초당 최대 테스트 연결 트랜잭션(TPS)	계정 한 개에 대해 초당 1개의 요청	아니요
최대 StartFileTransfer TPS	계정 한 개에 대해 초당 3개의 요청	예
보류 중인 파일 전송의 최대 대기열 크기	1000	아니요
최대 파일 크기	50기가바이트 (GiB)	아니요
파일당 최대 전송 시간	6시간	아니요
파일당 최대 요청 대기 시간	6시간	아니요
최소 AccessRole 또는 LoggingRole 세션 지속 시간	60분	아니요
최대 동시 파일 전송	커넥터당 동시 파일 전송 1회	아니요
계정 한 개에 대한 초당 최대 File Transfer 요청 수	3	예
계정당 최대 커넥터 수(SFTP 및 AS2 커넥터 모두 이 수에 기여)	100	예

명칭	기본값	조정 가능
계정당 커넥터의 최대 대역폭 (SFTP 및 AS2 커넥터 모두 이 값에 기여)	50 MBps	아니요

SFTP 커넥터의 보안 인증 정보를 저장하기 위해 각 Secrets Manager 보안 암호와 연결된 할당량이 있습니다. 동일한 보안 암호를 사용하여 여러 유형의 키를 저장하는 경우 여러 용도로 이러한 할당량이 발생할 수 있습니다.

- 단일 암호의 총 길이: 12,000자
- **Password** 문자열의 최대 길이: 1,024자
- **PrivateKey** 문자열의 최대 길이: 8,192자
- **Username** 문자열의 최대 길이: 100자

AWS Transfer Family 에 대한 AS2

적용성 선언문 2(AS2)는 강력한 메시지 보호 및 확인 메커니즘을 포함하는 RFC정의된 파일 전송 사양입니다. AS2 프로토콜은 프로토콜에 데이터 보호 및 보안 기능이 내장되어 있어야 하는 규정 준수 요구 사항이 있는 워크플로에 매우 중요합니다.

Note

AS2 용 Transfer Family는 [Drummond 인증을 받았습니다](#).

공급망, 물류 및 결제 워크플로AS2에 의존하는 소매, 생명 과학, 제조, 금융 서비스 및 유틸리티와 같은 산업의 고객은 AWS Transfer Family AS2 엔드포인트를 사용하여 비즈니스 파트너와 안전하게 거래할 수 있습니다. 트랜잭션된 데이터는 처리, 분석 및 기계 학습을 AWS 위해 에서 기본적으로 액세스할 수 있습니다. 이 데이터는 에서 실행되는 엔터프라이즈 리소스 계획(ERP) 및 고객 관계 관리(CRM) 시스템과의 통합에도 사용할 수 있습니다 AWS. AS2를 사용하면 고객은 기존 비즈니스 파트너 통합 및 규정 준수를 AWS 유지하면서 규모에 맞게 business-to-business (B2B) 트랜잭션을 실행할 수 있습니다.

구성된 AS2활성화 서버가 있는 파트너와 파일을 교환하려는 Transfer Family 고객인 경우 설정에는 암호화를 위한 퍼블릭-프라이빗 키 페어 하나와 파트너와 퍼블릭 키에 서명하고 교환하기 위한 퍼블릭-프라이빗 키 페어 하나를 생성하는 것이 포함됩니다.

전송 중 AS2페이로드를 보호하려면 일반적으로 암호화 메시지 구문(CMS)을 사용해야 하며 일반적으로 암호화와 디지털 서명을 사용하여 데이터 보호와 피어 인증을 제공합니다. 서명된 메시지 처리 알림(MDN) 응답 페이로드는 메시지가 수신되었고 성공적으로 복호화되었다는 확인(미거부)을 제공합니다.

이러한 CMS페이로드 및 MDN 응답의 전송은 를 통해 이루어집니다HTTP.

Note

HTTPS AS2 서버 엔드포인트는 현재 지원되지 않습니다. TLS 종료는 현재 고객의 책임입니다.

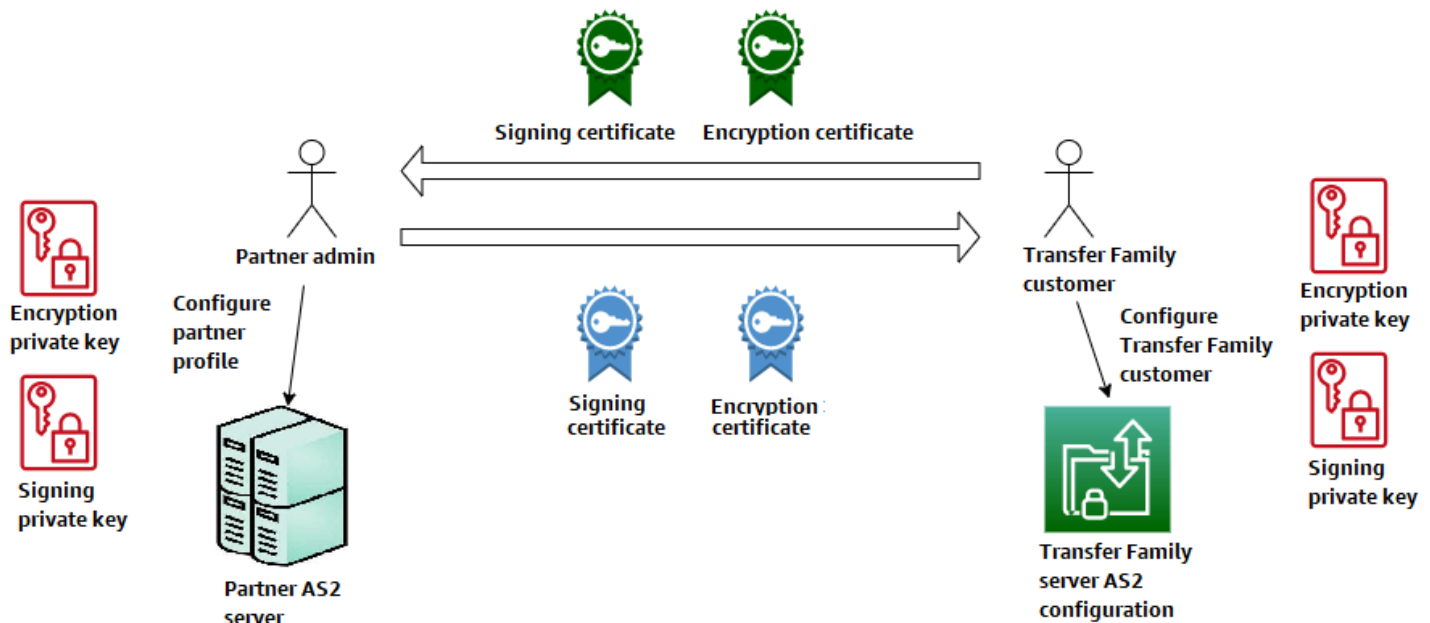
적용성 명령문 2(AS2) 구성 설정에 대한 자세한 step-by-step 내용은 자습서 를 참조하세요[AS2 구성 설정](#).

주제

- [AS2 사용 사례](#)
- [구성 AS2](#)
- [AS2 커넥터 구성](#)
- [AS2 파트너 관리](#)
- [AS2 메시지 전송 및 수신](#)
- [AS2 사용량 모니터링](#)

AS2 사용 사례

구성된 AS2 서버가 있는 파트너와 파일을 교환하려는 AWS Transfer Family 고객인 경우 설정의 가장 복잡한 부분에는 암호화를 위한 퍼블릭-프라이빗 키 페어 하나와 파트너와 퍼블릭 키를 서명하고 교환하기 위한 다른 페어가 포함됩니다.



와 AWS Transfer Family 함께 를 사용하려면 다음 변형을 고려하세요AS2.

Note

거래 파트너는 해당 파트너 프로필과 연결된 파트너입니다.
다음 표MDN의 모든 언급은 서명된 를 가정합니다MDNs.

AS2 사용 사례

인바운드 전용 사용 사례

- 거래 파트너에서 Transfer Family 서버로 암호화된 AS2 메시지를 전송합니다.

이 경우 다음과 같이 합니다:

1. 거래 파트너와 자신을 위한 프로필을 생성합니다.
2. AS2 프로토콜을 사용하는 Transfer Family 서버를 생성합니다.
3. 계약서를 작성하여 서버에 추가합니다.
4. 프라이빗 키로 인증서를 가져와 프로필에 추가한 다음 암호화를 위해 파트너 프로필로 퍼블릭 키를 가져옵니다.
5. 이러한 항목을 확보한 후에는 인증서용 퍼블릭 키를 거래 파트너에게 보내세요.

이제 파트너가 암호화된 메시지를 보내고 사용자는 이를 복호화하여 Amazon S3 버킷에 저장할 수 있습니다.

- 거래 파트너에서 Transfer Family 서버로 암호화된 AS2 메시지를 전송하고 서명을 추가합니다.

이 시나리오에서는 여전히 인바운드 전송만 하고 있지만, 이제는 파트너가 보내는 메시지에 서명하도록 하는 것이 좋습니다. 이 경우 거래 파트너의 서명 퍼블릭 키(파트너 프로필에 추가된 서명 인증서)를 가져옵니다.

- 트레이딩 파트너에서 Transfer Family 서버로 암호화된 AS2 메시지를 전송하고 서명 및 MDN 응답 전송을 추가합니다.

이 시나리오에서는 아직 인바운드 전송만 수행하지만 이제는 서명된 페이로드를 수신하는 것 외에도 거래 파트너가 서명된 MDN 응답을 받고 싶어합니다.

1. 공개 및 비공개 서명 키(프로필의 서명 인증서로 사용)를 가져오세요.
2. 퍼블릭 서명 키를 거래 파트너에게 보냅니다.

아웃바운드 전용 사용 사례

- Transfer Family 서버에서 거래 파트너로 암호화된 AS2 메시지를 전송합니다.

이 사례는 AS2 서버에 계약을 추가하는 대신 커넥터를 생성하는 것을 제외하고 인바운드 전용 전송 사용 사례와 유사합니다. 이 경우 거래 파트너의 퍼블릭 키를 프로필로 가져옵니다.

- Transfer Family 서버에서 거래 파트너로 암호화된 AS2 메시지를 전송하고 서명을 추가합니다.

아직 아웃바운드 전송만 수행 중이지만 이제 거래 파트너는 전송한 메시지에 서명하기를 원합니다.

1. 서명 프라이빗 키(프로필에 추가된 서명 인증서)를 가져오세요.
 2. 거래 파트너에게 퍼블릭 키를 보냅니다.
- Transfer Family 서버에서 거래 파트너로 암호화된 AS2 메시지를 전송하고 서명을 추가하고 MDN 응답을 전송합니다.

아직 아웃바운드 전송만 수행 중이지만 이제 서명된 페이로드를 보내는 것 외에도 거래 파트너로부터 서명된 MDN 응답을 받으려고 합니다.

1. 거래 파트너가 퍼블릭 서명 키를 보냅니다.
2. 거래 파트너의 퍼블릭 키를 가져옵니다(파트너 프로필에 추가된 서명 인증서로).

인바운드 및 아웃바운드 사용 사례

- Transfer Family 서버와 거래 파트너 간에 암호화된 AS2 메시지를 양방향으로 전송합니다.

이 경우 다음과 같이 합니다:

1. 거래 파트너와 자신을 위한 프로필을 생성합니다.
2. AS2 프로토콜을 사용하는 Transfer Family 서버를 생성합니다.
3. 계약서를 작성하여 서버에 추가합니다.
4. 커넥터를 생성합니다.
5. 프라이빗 키로 인증서를 가져와 프로필에 추가한 다음 암호화를 위해 파트너 프로필로 퍼블릭 키를 가져옵니다.
6. 거래 파트너로부터 퍼블릭 키를 받아 암호화를 위해 프로파일에 추가합니다.
7. 이러한 항목을 확보한 후에는 인증서용 퍼블릭 키를 거래 파트너에게 보내세요.

이제 거래 파트너와 암호화된 메시지를 교환할 수 있으며 둘 다 암호를 복호화할 수 있습니다. 사용자는 Amazon S3 버킷에 수신한 메시지를 저장할 수 있으며, 파트너는 사용자가 전송한 메시지를 복호화하여 저장할 수 있습니다.

- Transfer Family 서버와 거래 파트너 간에 암호화된 AS2 메시지를 양방향으로 전송하고 서명을 추가합니다.

이제 당신과 당신의 파트너는 서명된 메시지를 원합니다.

1. 서명 프라이빗 키(프로필에 추가된 서명 인증서)를 가져오세요.
 2. 거래 파트너에게 퍼블릭 키를 보냅니다.
 3. 거래 파트너의 서명 퍼블릭 키를 가져와 프로필에 추가합니다.
- Transfer Family 서버와 거래 파트너 간에 암호화된 AS2 메시지를 양방향으로 전송하고 서명을 추가하고 MDN 응답을 전송합니다.

이제 서명된 페이로드를 교환하고 귀하와 거래 파트너 모두 MDN 응답을 원합니다.

1. 거래 파트너가 퍼블릭 서명 키를 보냅니다.
2. 거래 파트너의 퍼블릭 키를 가져옵니다(파트너 프로필에 대한 서명 인증서로).
3. 퍼블릭 키를 거래 파트너에게 보냅니다.

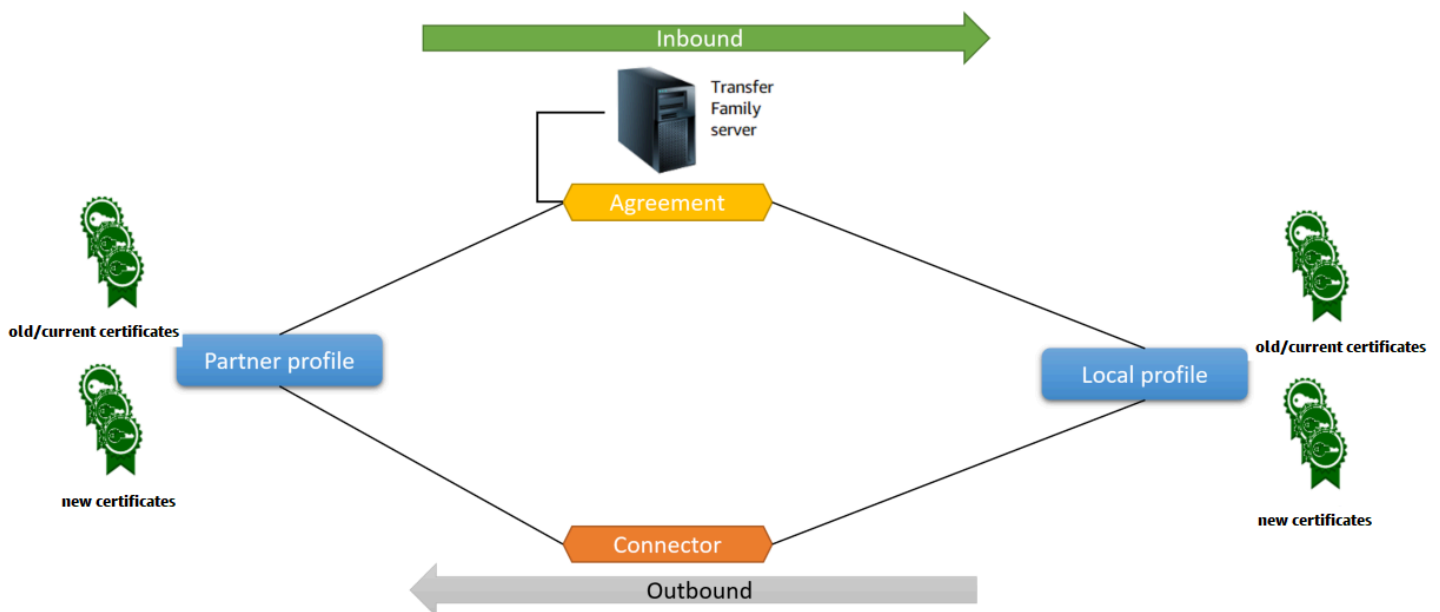
구성 AS2

AS2활성화된 서버를 생성하려면 다음 구성 요소도 지정해야 합니다.

- 계약 - 양자간 거래 파트너 계약 또는 파트너십, 메시지(파일)를 교환하는 두 당사자들 사이의 관계를 정의함. 계약을 정의하기 위해 Transfer Family는 서버, 로컬 프로파일, 파트너 프로파일, 인증서 정보를 결합합니다. Transfer Family AS2- 인바운드 프로세스는 계약을 사용합니다.
- 인증서 - 퍼블릭 키(X.509) 인증서는 메시지 암호화 및 확인을 위해 AS2 통신에 사용됩니다. 인증서는 커넥터 엔드포인트에도 사용됩니다.
- 로컬 프로파일 및 파트너 프로파일 AS2- 로컬 프로파일은 로컬(활성화된 Transfer Family 서버) 조직 또는 “당사자”를 정의합니다. 마찬가지로 파트너 프로파일은 Transfer Family 외부의 원격 파트너 조직을 정의합니다.

모든 AS2지원 서버에 필요한 것은 아니지만 아웃바운드 전송에는 커넥터가 필요합니다. 커넥터는 아웃바운드 연결에 대한 파라미터를 캡처합니다. 커넥터는 고객의 외부 비 AWS 서버로 파일을 전송하는데 필요합니다.

다음 다이어그램은 인바운드 및 아웃바운드 프로세스에 관련된 AS2 객체 간의 관계를 보여줍니다.



예제 AS2 구성은 end-to-end 섹션을 참조하세요 [AS2 구성 설정](#).

주제

- [Transfer Family 콘솔을 사용하여 AS2 서버 생성](#)

- [템플릿을 사용하여 Transfer Family AS2 스택 데모 생성](#)
- [AS2 구성 및 제한](#)
- [AS2 특징 및 기능](#)

Transfer Family 콘솔을 사용하여 AS2 서버 생성

이 절차에서는 Transfer Family 콘솔을 사용하여 AS2활성화된 서버를 생성하는 방법을 설명합니다. AWS CLI 대신 를 사용하려면 섹션을 참조하세요 [the section called “2단계: AS2 프로토콜을 사용하는 Transfer Family 서버 생성”](#).

AS2활성화된 서버를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택한 다음 서버 생성을 선택합니다.
3. 프로토콜 선택 페이지에서 AS2 (적용 가능성 설명 2)를 선택한 다음 다음을 선택합니다.

Choose 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 Next

4. 자격 증명 제공자 선택 페이지에서 다음을 선택합니다.

Note

의 경우 AS2 프로토콜에 기본 인증이 지원되지 않으므로 자격 증명 공급자를 선택할 AS2 수 없습니다. 대신 가상 프라이빗 클라우드(VPC) 보안 그룹을 통해 액세스를 제어합니다.

5. 엔드포인트 선택 페이지에서 다음을 수행합니다.

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

- a. 엔드포인트 유형 에서 VPC 호스팅을 선택하여 서버의 엔드포인트를 호스팅합니다. VPC 호스팅 엔드포인트 설정에 대한 자세한 내용은 섹션을 참조하세요 [Virtual Private Cloud\(VPC\)에 서버 생성](#).

Note

공개적으로 액세스할 수 있는 엔드포인트는 AS2 프로토콜에 지원되지 않습니다. 인터넷을 통해 VPC 엔드포인트에 액세스할 수 있도록 하려면 액세스 아래에서 인터넷 연결을 선택한 다음 탄력적 IP 주소를 제공합니다.

- b. 액세스에서 다음 옵션 중 하나를 선택합니다.

- 내부 VPC- 또는 를 통한 AWS Direct Connect 온프레미스 데이터 센터와 같이 VPC 및 연결된 환경 내에서 액세스를 제공하려면 이 옵션을 선택합니다VPN.
- 인터넷 연결 VPC- 인터넷을 통해 액세스를 제공하고 AWS Direct Connect 또는 를 통한 온프레미스 데이터 센터와 같이 VPC 및 연결된 환경 내에서 액세스를 제공하려면 이 옵션을 선택합니다VPN.

인터넷 연결을 선택하는 경우 메시지가 표시되면 탄력적 IP 주소를 제공하세요.

- c. 에서 기존 를 VPC선택하거나 생성을 VPC VPC 선택하여 새 를 생성합니다VPC.
- d. FIPS 활성화된 의 경우 FIPS 활성화된 엔드포인트 확인란을 선택 취소합니다.

 Note

FIPS-enabled 엔드포인트는 AS2 프로토콜에서 지원되지 않습니다.

- e. Next(다음)를 선택합니다.
6. 도메인 선택 페이지에서 선택한 프로토콜을 사용하여 파일을 객체로 저장하고 액세스하려면 Amazon S3를 선택합니다.

Next(다음)를 선택합니다.

7. 추가 세부 정보 구성 페이지에서 필요한 설정을 선택합니다.

 Note

와 함께 다른 프로토콜을 구성하는 경우 추가 세부 정보 설정이 AS2모두 적용됩니다. 그러나 AS2 프로토콜의 경우 적용되는 유일한 설정은 CloudWatch 로깅 및 태그 섹션의 설정입니다.

CloudWatch 로깅 역할 설정은 선택 사항이지만 메시지 상태를 확인하고 구성 문제를 해결할 수 있도록 설정하는 것이 좋습니다.

8. 검토 및 생성 페이지에서 옵션을 검토하여 올바른지 확인하세요.
 - 설정을 편집하려면 변경하려는 단계 옆의 편집을 선택합니다.

Note

단계를 편집하는 경우 편집하기로 선택한 단계 이후의 각 단계를 검토하는 것이 좋습니다.

- 변경 사항이 없는 경우 서버 생성을 선택하여 서버를 생성하세요. 서버 페이지로 이동하고, 새 서버가 나열되는 다음 화면이 표시됩니다.

Servers (1)							Actions	Add user	Create server
	Hostname	Server ID	State	Service managed users	Endpoint type	Domain			
☐	-	s-	Starting	-	VPC	Amazon S3			

새 서버 상태가 온라인으로 변경되기까지 몇 분 정도 걸릴 수 있습니다. 이때부터 서버는 사용자의 파일 작업을 수행할 수 있습니다.

템플릿을 사용하여 Transfer Family AS2 스택 데모 생성

를 AS2활성화한 Transfer Family 서버를 빠르게 생성할 수 있는 독립형 AWS CloudFormation 템플릿이 제공됩니다. 템플릿은 퍼블릭 Amazon VPC 엔드포인트, 인증서, 로컬 및 파트너 프로필, 계약 및 커넥터로 서버를 구성합니다.

이 템플릿을 사용하기 전에 다음 사항에 유의하세요.

- 이 템플릿에서 스택을 생성할 경우, 사용한 AWS 리소스에 대한 요금이 청구됩니다.
- 템플릿은 여러 인증서를 생성하고 안전하게 저장 AWS Secrets Manager 하기 위해 배치합니다. 이 서비스를 사용하면 요금이 부과되므로 원하는 경우 Secrets Manager에서 이러한 인증서를 삭제할 수 있습니다. Secrets Manager에서 이러한 인증서를 삭제해도 Transfer Family 서버에서는 삭제되지 않습니다. 따라서 데모 스택의 기능은 영향을 받지 않습니다. 그러나 프로덕션 AS2 서버에 사용할 인증서의 경우 Secrets Manager를 사용하여 저장된 인증서를 관리하고 주기적으로 교체하는 것이 좋습니다.
- 템플릿은 기본 용도로만 사용하고 주로 데모 용도로만 사용하는 것이 좋습니다. 프로덕션에서 이 데모 스택을 사용하려면 템플릿의 YAML 코드를 수정하여 더 강력한 스택을 생성하는 것이 좋습니다. 예를 들어 프로덕션 수준의 인증서를 만들고 프로덕션에서 사용할 수 있는 AWS Lambda 함수를 만들어 보세요.

CloudFormation 템플릿에서 AS2활성화된 Transfer Family 서버를 생성하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 스택을 선택합니다.
3. 스택 생성을 선택한 다음 새 리소스 사용(표준)을 선택합니다.
4. 사전 조건 - 템플릿 준비섹션에서 템플릿 준비 완료를 선택합니다.
5. 이 링크, [AS2 데모 템플릿](#) 을 복사하여 Amazon S3 URL 필드에 붙여 넣습니다.
6. Next(다음)를 선택합니다.
7. 스택 세부 정보 지정 페이지에서 스택의 이름을 지정한 다음 파라미터를 지정합니다.
 - 에서 로컬 AS2 ID 및 파트너 AS2 ID 값을 AS2입력하거나 각각 기본값인 local 및 를 수락합니다partner.
 - 네트워크 에서 보안 그룹 수신 CIDR IP 의 값을 입력하거나 기본값인 를 수락합니다0.0.0.0/0.

 Note

이 값은 CIDR 형식으로 AS2 서버로 들어오는 트래픽에 허용되는 IP 주소를 지정합니다. 기본값인 0.0.0.0/0은 모든 IP 주소를 허용합니다.

- 일반에서 접두사에 값을 입력하거나 기본값인 transfer-as2을 그대로 사용합니다. 이 접두사는 스택에서 생성되는 모든 리소스 이름 앞에 위치합니다. 예를 들어, 기본 접두사를 사용하는 경우 Amazon S3 버킷의 transfer-as2-*TransferS3BucketName*라는 이름이 지정됩니다.
8. Next(다음)를 선택합니다. 스택 옵션 구성페이지에서 다음을 다시 선택합니다.
 9. 생성 중인 스택의 세부 정보를 검토한 다음 스택 생성을 선택합니다.

 Note

페이지 하단의 기능 아래에서 가 AWS Identity and Access Management (IAM) 리소스를 생성할 AWS CloudFormation 수 있음을 확인해야 합니다.

스택이 생성된 후 AWS Command Line Interface ()를 사용하여 파트너 서버에서 로컬 Transfer Family 서버로 테스트 AS2 메시지를 보낼 수 있습니다AWS CLI. 테스트 메시지를 보내기 위한 샘플 AWS CLI 명령이 스택의 다른 모든 리소스와 함께 생성됩니다.

이 샘플 명령을 사용하려면 스택의 출력 탭으로 이동하여 `TransferExampleAs2Command` 를 복사합니다. 그런 다음 AWS CLI를 사용하여 명령을 실행할 수 있습니다. 아직 를 설치하지 않은 경우 AWS Command Line Interface 사용 설명서의 [의 최신 버전 설치 또는 업데이트를 AWS CLI](#) AWS CLI참조하세요.

샘플 명령의 형식은 다음과 같습니다.

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt && aws transfer
start-file-transfer --region aws-region --connector-id TransferConnectorId --send-
file-paths /TransferS3BucketName/test.txt
```

Note

이 명령의 버전에는 스택에 있는 *TransferS3BucketName* 및 *TransferConnectorId* 리소스의 실제 값이 포함되어 있습니다.

이 샘플 명령은 && 문자열을 사용하여 서로 연결된 두 개의 개별 명령으로 구성되어 있습니다.

첫 번째 명령은 버킷에 비어 있는 새 텍스트 파일을 만듭니다.

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt
```

그런 다음 두 번째 명령은 커넥터를 사용하여 파트너 프로파일에서 로컬 프로파일로 파일을 보냅니다. Transfer Family 서버에는 로컬 프로파일의 파트너 프로파일의 메시지를 수락하도록 허용하는 계약이 설정되어 있습니다.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
--send-file-paths /TransferS3BucketName/test.txt
```

명령을 실행한 후 Amazon S3 버킷(*TransferS3BucketName*)으로 이동하여 콘텐츠를 볼 수 있습니다. 명령이 제대로 실행되면 버킷에 다음과 같은 객체가 표시되어야 합니다.

- `processed/` - 이 폴더에는 전송된 JSON 파일과 MDN 응답을 설명하는 파일이 포함되어 있습니다.
- `processing/`— 이 폴더에는 처리 중인 파일이 일시적으로 포함되지만 전송이 완료된 후에는 이 폴더가 비어 있어야 합니다.
- `server-id/`— 이 폴더의 이름은 Transfer Family 서버 ID에 따라 붙여집니다. 여기에는 `from-partner` (이 폴더는 파트너의 AS2 ID를 기반으로 동적으로 명명됨)이 포함되며, 그 자체에

는 failed/, processed/및 processing/ 폴더가 포함됩니다. /*server-id*/from-*partner*/processed/ 폴더에는 전송된 텍스트 파일의 복사본과 해당 JSON 및 MDN 파일이 포함되어 있습니다.

- test.txt— 이 객체는 전송된 (빈) 파일입니다.

AS2 구성 및 제한

이 주제에서는 허용되는 암호 및 다이제스트를 포함하여 적용성 선언문 2(AS2) 프로토콜을 사용하는 전송에 지원되는 구성, 기능 및 기능에 대해 설명합니다. 이 섹션에서는 AS2 전송의 제한 및 알려진 문제도 설명합니다.

주제

- [AS2 지원되는 구성](#)
- [AS2 할당량 및 제한](#)

AS2 지원되는 구성

서명, 암호화, 압축, MDN

인바운드 전송과 아웃바운드 전송 모두에서 다음 항목은 필수 또는 옵션입니다.

- 암호화 - 필수(HTTP현재 지원되는 유일한 전송 방법인 전송의 경우). 암호화되지 않은 메시지는 Application Load Balancer(ALB)와 같은 TLS종료 프록시에서 전달되고 X-Forwarded-Proto: https 헤더가 있는 경우에만 허용됩니다.
- 서명 — 옵션
- 압축 - 선택 사항(현재 지원되는 유일한 압축 알고리즘은 ZLIB)
- 메시지 처리 알림(MDN) - 선택 사항

암호(Ciphers)

다음 암호는 인바운드 및 아웃바운드 전송 모두에 지원됩니다.

- AES128_CBC
- AES192_CBC
- AES256_CBC

- 3DES(이전 버전과의 호환성에만 해당)

Digests

다음 데이터 유형이 지원됩니다.

- 인바운드 서명 및 MDN – SHA1, SHA256, SHA384, SHA512
- 아웃바운드 서명 및 MDN – SHA1, SHA256, SHA384, SHA512

MDN

MDN 응답의 경우 다음과 같이 특정 유형이 지원됩니다.

- 인바운드 전송 — 동기 및 비동기
- 아웃바운드 전송— 동기식 전송 전용
- Simple Mail Transfer Protocol(SMTP)(이메일 MDN) - 지원되지 않음

Transports

- 인바운드 전송 - 현재 지원되는 HTTP 유일한 전송이며 명시적으로 지정해야 합니다.

Note

인바운드 전송 HTTPS에 를 사용해야 하는 경우 Application Load Balancer 또는 Network Load Balancer TLS에서 를 종료할 수 있습니다. 이에 대한 설명은 [를 통해 AS2 메시지 수신 HTTPS](#)에 나와 있습니다.

- 아웃바운드 전송 - HTTP 를 제공하는 경우 암호화 알고리즘도 지정URL해야 합니다. 를 제공하는 경우 암호화 알고리즘 HTTPSURL에 NONE 를 지정할 수 있습니다.

AS2 할당량 및 제한

이 섹션에서는 에 대한 할당량 및 제한 사항에 대해 설명합니다. AS2

주제

- [AS2 할당량](#)
- [비밀 처리를 위한 할당량](#)

- [알려진 제한 사항](#)

AS2 할당량

AS2 파일 전송에는 다음 할당량이 적용됩니다. 조정 가능한 할당량 증가를 요청하려면 AWS 일반 참조의 [AWS 서비스 할당량](#)을 참조하세요.

AS2 할당량

명칭	기본값	조정 가능
서버당 인바운드 AS2 요청 수	25개/초	아니요
서버당 진행 중인 인바운드 AS2 요청	100	아니요
File Transfer 요청당 최대 파일 수	10	아니요
커넥터당 진행 중인 아웃바운드 AS2 요청	100	아니요
최대 파일 크기 (압축 또는 비압축)	50 MiB	예
비활성 제한 시간	350초	아니요
계정당 최대 파트너 프로필 개수	1000 (파트너 프로필당 인증서 최대 10개: 조정 불가)	예
계정당 최대 인증서 수	1000	예
계정 한 개에 대한 초당 최대 File Transfer 요청 수	3	예
계정당 최대 커넥터 수(SFTP 및 AS2 커넥터 모두 이 수에 기여)	100	예

명칭	기본값	조정 가능
계정당 커넥터의 최대 대역폭 (SFTP 및 AS2 커넥터 모두 이 값에 기여)	50 MBps	아니요
서버당 최대 계약 수	100	예

비밀 처리를 위한 할당량

AWS Transfer Family 는 기본 인증을 사용하는 AS2 고객을 AWS Secrets Manager 대신하여 에 전화를 겁니다. 또한 Secrets Manager는 에 전화를 겁니다 AWS KMS.

Note

이 할당량은 Transfer Family의 비밀 사용에만 국한되지 않으며, 귀하의 모든 서비스에서 공유됩니다. AWS 계정

Secrets Manager GetSecretValue의 경우 할당량 에 설명된 대로 적용되는 할당량은 DescribeSecret 및 GetSecretValue API 요청의 결합 비율입니다. [AWS Secrets Manager](#)

Secrets Manager GetSecretValue

이름	값	설명
DescribeSecret 및 GetSecret Value API 요청의 통합 속도	지원되는 각 리전: 초당 10,000 개	DescribeSecret 및 GetSecret Value API 요청을 합한 초당 최대 트랜잭션 수입니다.

AWS KMS의 경우 다음 할당량이 에 적용됩니다Decrypt. 자세한 내용은 [각 AWS KMS API 작업에 대한 할당량 요청을 참조하세요.](#)

AWS KMS Decrypt

할당량 이름	기본값(초당 요청 수)
암호화 작업(대칭) 요청 빈도	이러한 공유 할당량은 AWS 리전 및 요청에 사용되는 AWS KMS 키 유형에 따라 달라집니다. 각 할당량은 별도로 계산됩니다. • 5500(공유) • 다음 리전에서는 10000(공유): • 미국 동부(오하이오) us-east-2 • 아시아 태평양(싱가포르) ap-southeast-1 • 아시아 태평양(시드니) ap-southeast-2 • 아시아 태평양(도쿄) ap-northeast-1 • EU(프랑크푸르트) eu-central-1 • EU(런던) eu-west-2 • 다음 리전에서는 50000(공유): • 미국 동부(버지니아 북부), us-east-1 • 미국 서부(오리건), us-west-2 • 유럽(아일랜드) eu-west-1
사용자 지정 키 스토어 요청 할당량  Note 이 할당량은 외부 키 저장소를 사용하는 경우에만 적용됩니다.	사용자 지정 키 저장소 요청 할당량은 각 사용자 지정 키 저장소에 대해 별도로 계산됩니다. • AWS CloudHSM 키 스토어당 1,800개(공유) • 각 외부 키 저장소에 대해 1800회(공유)

알려진 제한 사항

- 서버 측 TCP 연결 유지는 지원되지 않습니다. 클라이언트가 keep-alive 패킷을 전송하지 않는 한 350초 동안 사용하지 않으면 연결 제한 시간이 초과됩니다.
- 서비스에서 활성 계약을 수락하고 Amazon CloudWatch 로그에 표시하려면 메시지에 유효한 AS2 헤더가 포함되어야 합니다.

- AWS Transfer Family 에서 메시지를 수신하는 서버는 [RFC6211](#)에 정의된 대로 메시지 서명을 검증하기 위한 암호화 메시지 구문(CMS) 알고리즘 보호 속성을 지원AS2해야 합니다. 일부 이전 IBM Sterling 제품에서는 이 속성이 지원되지 않습니다.
- 중복 메시지로 IDs 인해 처리됨/경고: 중복 문서 메시지가 발생합니다.
- AS2 인증서의 키 길이는 최소 2048비트에서 최대 4096비트여야 합니다.
- 거래 파트너의 HTTPS 엔드포인트MDNs에 AS2 메시지를 보내거나 비동기적으로 보낼 때 또는 메시지는 공개적으로 신뢰할 수 있는 SSL 인증 기관(CA)이 서명한 유효한 인증서를 사용해야 MDNs 합니다. 자체 서명된 인증서는 현재 지원되지 않습니다.
- 엔드포인트는 TLS 버전 1.2 프로토콜과 보안 정책에서 허용하는 암호화 알고리즘(에 설명된 대로)을 지원해야 합니다 [에 대한 보안 정책 AWS Transfer Family](#).
- 상호TLS(mTLS)는 현재 지원되지 않습니다.
- AS2 버전 1.2의 여러 첨부 파일 및 인증서 교환 메시징(CEM)은 현재 지원되지 않습니다.
- 기본 인증은 현재 아웃바운드 메시지에만 지원됩니다.

AS2 특징 및 기능

다음 표에는 를 사용하는 Transfer Family 리소스에 사용할 수 있는 기능과 기능이 나열되어 있습니다 AS2.

AS2 기능

Transfer Family는 에 대해 다음과 같은 기능을 제공합니다AS2.

기능	에서 지원 AWS Transfer Family
Drummond 인증	예
AWS CloudFormation 지원	예
Amazon CloudWatch 지표	예
SHA-2 암호화 알고리즘	예
Amazon S3 지원	예
Amazon 지원 EFS	아니요

기능	에서 지원 AWS Transfer Family
예약된 메시지	예 ¹
AWS Transfer Family 관리형 워크플로	아니요
Certificate Exchange 메시징(CEM)	아니요
상호TLS(mTLS)	아니요

1. [Amazon을 사용하여 AWS Lambda 함수를 예약 EventBridge](#)하여 사용할 수 있는 아웃바운드 예약 메시지

AS2 송수신 기능

다음 표에는 전송 및 수신 기능 목록이 AWS Transfer Family AS2 나와 있습니다.

기능	인바운드: 서버로 수신	아웃바운드: 커넥터로 전송
TLS 암호화된 전송(HTTPS)	예 ¹	예
비TLS운송(HTTP)	예	예 ²
동기식 MDN	예	예
메시지 압축	예	예
비동기식 MDN	예	아니요
정적 IP 주소	예	예
자체 IP 주소 가져오기	예	아니요
여러 파일 첨부 파일	아니요	아니요
기본 인증	아니요	예
AS2 다시 시작	해당 사항 없음	아니요
메시지당 사용자 지정 제목	해당 사항 없음	아니요

1. Network Load Balancer에서 사용 가능한 인바운드 TLS 암호화된 전송(NLB)
2. 아웃바운드 비TLS전송은 암호화가 활성화된 경우에만 사용 가능

AS2 커넥터 구성

커넥터의 목적은 아웃바운드 전송을 위해 거래 파트너 간에 관계를 수립하여 Transfer Family 서버에서 파트너 소유의 외부 대상으로 AS2 파일을 보내는 것입니다. 커넥터의 경우 로컬 및 파트너 프로필을 생성하여 로컬 당사자, 원격 파트너 및 인증서를 지정합니다. 커넥터를 설치한 후에는 거래 파트너에게 정보를 전송할 수 있습니다.

Note

거래 파트너가 수신한 메시지 크기는 Amazon S3의 객체 크기와 일치하지 않습니다. 이러한 불일치는 AS2 메시지가 전송 전에 파일을 봉투에 래핑하기 때문에 발생합니다. 따라서 파일을 압축하여 전송하더라도 파일 크기가 커질 수 있습니다. 따라서 거래 파트너의 최대 파일 크기가 보내는 파일 크기보다 커야 합니다.

적용성 선언문 2(AS2) 커넥터는 아웃바운드 전송을 위한 거래 파트너 간의 관계를 설정합니다. AS2 커넥터에 대한 자세한 내용은 섹션을 참조하세요 [AS2 커넥터 구성](#).

AS2 커넥터 생성

이 절차에서는 AWS Transfer Family 콘솔을 사용하여 AS2 커넥터를 생성하는 방법을 설명합니다. AWS CLI 대신 를 사용하려면 섹션을 참조하세요 [the section called “6단계: 사용자와 사용자의 거래 파트너 간의 커넥터를 생성합니다.”](#).

AS2 커넥터를 생성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택한 다음 커넥터 생성을 선택합니다.
3. 커넥터 구성 섹션에서 다음 정보를 지정합니다:
 - URL - 아웃바운드 연결URL용 를 입력합니다.
 - 액세스 역할 - 사용할 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)을 선택합니다. 이 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 그 역할이

StartFileTransfer와 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는 지 확인하세요.

Note

커넥터에 기본 인증을 사용하는 경우 액세스 역할에는 암호에 대한 `secretsmanager:GetSecretValue` 권한이 필요합니다. 보안 암호가 AWS 관리형 키의 대신 고객 관리형 키를 사용하여 암호화되는 경우 AWS Secrets Manager 역할에도 해당 키에 대한 `kms:Decrypt` 권한이 필요합니다. 접두어 `aws/transfer/`를 사용하여 암호의 명칭을 지정하는 경우 [암호 생성 권한 예](#)에 나와 있는 것처럼 와일드카드 문자(*)를 사용하여 필요한 권한을 추가할 수 있습니다.

- 로깅 역할(선택 사항) - 이벤트를 CloudWatch 로그로 푸시하는 데 사용할 커넥터의 IAM 역할을 선택합니다.
4. AS2 구성 섹션에서 로컬 및 파트너 프로파일, 암호화 및 서명 알고리즘, 전송된 정보를 압축할지 여부를 선택합니다. 유의할 사항:
 - 암호화 알고리즘의 경우 필요한 레거시 클라이언트를 지원해야 하는 DES_EDE3_CBC 경우가 아니면 를 선택하지 마세요. 암호화 알고리즘이 약하기 때문입니다.
 - 제목은 커넥터와 함께 전송되는 AS2 메시지의 subject HTTP 헤더 속성으로 사용됩니다.
 - 암호화 알고리즘 없이 커넥터를 생성하도록 선택한 경우 를 프로토콜HTTPS로 지정해야 합니다.
 5. MDN 구성 섹션에서 다음 정보를 지정합니다.
 - 요청 MDN - 거래 파트너가 를 통해 메시지를 성공적으로 수신한 MDN 후 를 보내도록 요구할 수 있습니다AS2.
 - 서명된 MDN - 에 서명을 요구할 수 있는 옵션이 MDNs 있습니다. 이 옵션은 요청을 MDN선택한 경우에만 사용할 수 있습니다.
 6. 기본 인증 섹션에서 다음 정보를 지정합니다.
 - 아웃바운드 메시지와 함께 로그인 자격 증명을 보내려면 기본 인증 활성화를 선택합니다. 아웃바운드 메시지와 함께 자격 증명을 보내지 않으려면 기본 인증 활성화를 선택 취소하세요.
 - 인증을 사용하는 경우 암호를 선택하거나 생성하세요.
 - 새 암호를 만들려면 새 암호 생성을 선택한 다음 사용자 이름과 암호를 입력합니다. 이러한 자격 증명은 파트너의 엔드포인트에 연결하는 사용자와 일치해야 합니다.

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

ⓘ Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- 암호를 사용하려면 기존 암호 선택을 선택한 후 드롭다운 메뉴에서 암호를 선택합니다. Secrets Manager에서 올바른 형식의 암호를 만드는 방법에 대한 자세한 설명은 [AS2 커넥터에 대한 기본 인증 활성화](#) 섹션을 참조하세요.

[illegible]

7. 모든 설정을 확인한 후 커넥터 생성을 선택하여 커넥터를 생성합니다.

새 커넥터의 ID가 목록에 추가된 커넥터 페이지가 나타납니다. 커넥터에 대한 세부 정보를 보려면 [AS2 커넥터 세부 정보 보기](#) 섹션을 참조하세요.

AS2 커넥터 알고리즘

AS2 커넥터를 생성하면 다음 보안 알고리즘이 커넥터에 연결됩니다.

유형	알고리즘
TLS 암호화	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

유형	알고리즘
	TLS_ECDHE_RSAWITH_AES__128_GCM_SHA256
	TLS_ECDHE_ECDSAWITH_AES__128_CBC_SHA256
	TLS_ECDHE_RSAWITH_AES__128_CBC_SHA256
	TLS_ECDHE_ECDSAWITH_AES__256_GCM_SHA384
	TLS_ECDHE_RSAWITH_AES__256_GCM_SHA384
	TLS_ECDHE_ECDSAWITH_AES__256_CBC_SHA384
	TLS_ECDHE_RSAWITH_AES__256_CBC_SHA384

AS2 커넥터에 대한 기본 인증

AS2 프로토콜을 사용하는 Transfer Family 서버를 생성하거나 업데이트할 때 아웃바운드 메시지에 대한 기본 인증을 추가할 수 있습니다. 커넥터에 인증 정보를 추가하여 이 작업을 수행합니다.

Note

기본 인증은 를 사용하는 경우에만 사용할 수 있습니다HTTPS.

커넥터에 인증을 사용하려면 기본 인증 섹션에서 기본 인증 활성화를 선택합니다. 기본 인증을 활성화한 후 새 비밀을 생성하거나 기존 비밀을 사용할 수 있습니다. 어느 경우든 비밀의 자격 증명은 이 커넥터를 사용하는 아웃바운드 메시지와 함께 전송됩니다. 자격 증명은 거래 파트너의 원격 엔드포인트에 연결하려는 사용자와 일치해야 합니다.

다음 스크린샷은 기본 인증 활성화를 선택하고 새 비밀번호를 선택한 것을 보여줍니다. 이러한 선택을 한 후 비밀번호에 대한 사용자 이름과 암호를 입력할 수 있습니다.

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.

다음 스크린샷은 기본 인증 활성화를 선택하고 기존 비밀번호를 선택한 것을 보여줍니다. 비밀번호는 [AS2 커넥터에 대한 기본 인증 활성화](#)에 설명된 대로 올바른 형식이어야 합니다.

[illegible]

AS2 커넥터에 대한 기본 인증 활성화

AS2 커넥터에 대한 기본 인증을 활성화하면 Transfer Family 콘솔에서 새 보안 암호를 생성하거나에서 생성한 보안 암호를 사용할 수 있습니다 AWS Secrets Manager. 어느 경우든 암호는 Secrets Manager에 저장됩니다.

주제

- 콘솔을 사용하여 새 암호 생성
- 기존 암호 사용
- 에서 보안 암호 생성 AWS Secrets Manager

콘솔을 사용하여 새 암호 생성

콘솔에서 커넥터를 만들 때 새 암호를 생성할 수 있습니다.

새 암호를 만들려면 새 암호 생성을 선택한 다음 사용자 이름과 암호를 입력합니다. 이러한 자격 증명은 파트너의 엔드포인트에 연결하는 사용자와 일치해야 합니다.

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.

i Note

콘솔에서 새 보안 암호를 생성할 때 보안 암호의 이름은 다음과 같은 명명 규칙을 따릅니다. **/aws/transfer/*connector-id* *connector-id*** 는 생성하려는 커넥터의 ID입니다. AWS Secrets Manager에서 암호를 찾으려고 할 때는 이 점을 고려하세요.

기존 암호 사용

콘솔에서 커넥터를 만들 때 기존 암호를 지정할 수 있습니다.

암호를 사용하려면 기존 암호 선택을 선택한 후 드롭다운 메뉴에서 암호를 선택합니다. Secrets Manager에서 올바른 형식의 암호를 만드는 방법에 대한 자세한 설명은 [에서 보안 암호 생성 AWS Secrets Manager](#) 섹션을 참조하세요.

[illegible]

에서 보안 암호 생성 AWS Secrets Manager

다음 절차에서는 AS2 커넥터와 함께 사용할 적절한 보안 암호를 생성하는 방법을 설명합니다.

 Note

기본 인증은 를 사용하는 경우에만 사용할 수 있습니다HTTPS.

AS2 기본 인증을 위해 Secrets Manager에 사용자 자격 증명을 저장하려면

1. 에 로그인 AWS Management Console 하고 에서 AWS Secrets Manager 콘솔을 엽니다 <https://console.aws.amazon.com/secretsmanager/>.
2. 왼쪽 탐색 창에서 암호를 선택합니다.
3. 암호 페이지에서 새 암호 저장을 선택합니다.
4. 암호 선택 페이지의 암호 타입에서 다른 타입의 암호를 선택합니다.
5. 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 - **Username**를 입력합니다.
 - 값 - 파트너 서버에 연결할 권한이 있는 사용자의 이름을 입력합니다.
6. 암호를 제공하려면 행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

 - 키 - **Password**를 입력합니다.
 - 값 - 사용자의 암호를 입력합니다.
7. 프라이빗 키를 제공하려면 행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 - **PrivateKey**를 입력합니다.
 - 값 - 사용자의 프라이빗 키를 입력합니다. 이 값은 OpenSSH 형식으로 저장해야 하며 원격 서버에 이 사용자에게 대해 저장된 퍼블릭 키와 일치해야 합니다.
8. Next(다음)를 선택합니다.
9. 암호 구성 페이지에 암호를 위한 명칭과 설명을 입력합니다. 이름에 **aws/transfer/**이라는 접두사를 사용하는 것이 좋습니다. 예컨대, 암호 **aws/transfer/connector-1**을 지정할 수 있습니다.
10. 다음을 선택한 후 교체 구성 페이지의 기본값을 그대로 사용합니다. 그 다음 다음을 선택합니다.
11. 검토 페이지에서 저장을 선택하여 암호를 만들고 저장합니다.

암호를 만든 후 커넥터를 만들 때 암호를 선택할 수 있습니다([AS2 커넥터 구성](#) 참조). 기본 인증을 활성화하는 단계에서 사용 가능한 암호의 드롭다운 목록에서 암호를 선택합니다.

AS2 커넥터 세부 정보 보기

AWS Transfer Family 콘솔에서 AS2 AWS Transfer Family 커넥터에 대한 세부 정보 및 속성 목록을 찾을 수 있습니다. AS2 커넥터의 속성에는 URL, 역할, 프로필, MDNs 태그 및 모니터링 지표가 포함됩니다.

이것은 커넥터 세부 정보 보기 절차입니다.

커넥터 세부 정보를 보려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 커넥터를 선택합니다.
3. 커넥터 ID 옆에서 식별자를 선택하면 선택한 커넥터의 세부 정보 페이지가 표시됩니다.

AS2 커넥터의 세부 정보 페이지에서 편집을 선택하여 커넥터의 속성을 변경할 수 있습니다.

The screenshot displays the AWS Transfer Family console interface for an AS2 connector. The breadcrumb navigation at the top shows 'Transfer Family > Connectors > [connector ID]'. The connector name is partially visible as 'C-...'.

Connector configuration section includes:

- URL:** http://[redacted]
- Access role:** [redacted]
- Logging role:** [redacted]

Communication settings section includes:

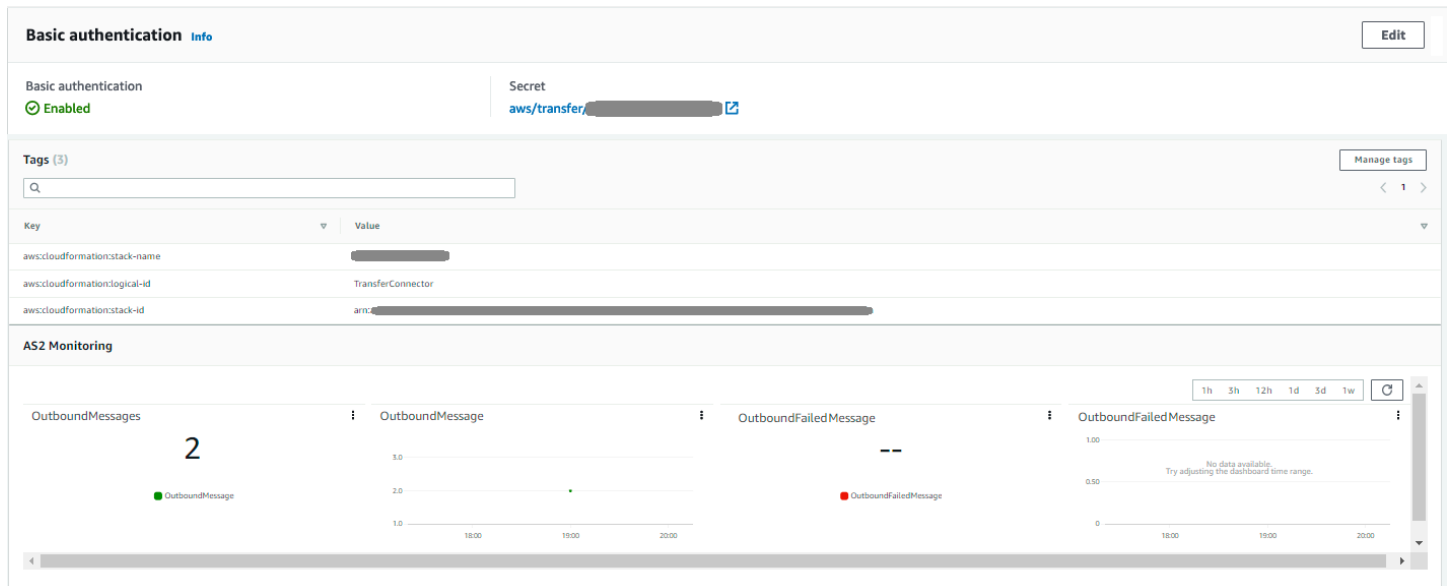
- AS2-From header:** partner-test
- AS2-To header:** local-test

AS2 configuration section includes:

- Local profile:** partner-test
- Partner profile:** local-test
- Compression:** Disabled
- Message Subject:** View
- Encryption algorithm:** AES256_CBC
- Signing algorithm:** SHA256

MDN configuration section includes:

- Request MDN:** Enabled
- Signed MDN:** Default to message signing algorithm: SHA256
- Synchronization:** Enabled



Note

형식은 다르지만 다음 AWS Command Line Interface 를 실행하여 이 정보의 대부분을 얻을 수 있습니다 (AWS CLI 명령:

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

자세한 내용은 [단원을 참조하세요.DescribeConnector](#) API 참조에 있습니다.

AS2 파트너 관리

이 주제에서는 AS2 인증서, 프로필 및 계약을 관리하는 방법을 설명합니다.

AS2 인증서 가져오기

Transfer Family AS2 프로세스는 전송된 정보의 암호화 및 서명 모두에 인증서 키를 사용합니다. 파트너는 두 가지 용도로 동일한 키를 사용하거나 각 용도에 별도의 키를 사용할 수 있습니다. 재해 또는 보안 침해 발생 시 데이터를 복호화할 수 있도록 신뢰할 수 있는 제3자가 에스스로에 공통 암호화 키를 보관해 둔 경우 별도의 서명 키를 사용하는 것이 좋습니다. 별도의 서명 키(에스스로하지 않음)를 사용하면 디지털 서명의 부인 방지 기능이 손상되지 않습니다.

Note

AS2 인증서의 키 길이는 최소 2048비트에서 최대 4096비트여야 합니다.

다음 포인트에서는 프로세스 중에 AS2 인증서가 사용되는 방법을 자세히 설명합니다.

- 인바운드 AS2
 - 거래 파트너가 서명 인증서용 퍼블릭 키를 보내면 이 키를 파트너 프로필로 가져옵니다.
 - 현지 당사자가 암호화 및 서명 인증서를 위한 퍼블릭 키를 전송합니다. 그러면 파트너가 프라이빗 키를 가져옵니다. 로컬 당사자는 서명 및 암호화를 위해 별도의 인증서 키를 보내거나 두 가지 용도로 동일한 키를 사용하도록 선택할 수 있습니다.
- 아웃바운드 AS2
 - 파트너가 암호화 인증서용 퍼블릭 키를 보내고 이 키를 파트너 프로필로 가져옵니다.
 - 로컬 당사자는 서명용 인증서의 퍼블릭 키를 보내고 서명을 위해 인증서의 프라이빗 키를 가져옵니다.

인증서 생성 방법에 대한 자세한 설명은 [the section called “1단계: 에 대한 인증서 생성 AS2”](#) 섹션을 참조하세요.

이 절차에서는 Transfer Family 콘솔을 사용하여 인증서를 가져오는 방법을 설명합니다. AWS CLI 대신 [the section called “3단계: Transfer Family 인증서 리소스로 인증서 가져오기”](#).

AS2사용 가능한 인증서를 지정하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창의 AS2 거래 파트너 에서 인증서 를 선택합니다.
3. 인증서 가져오기를 선택합니다.
4. 인증서 설명 섹션에서 쉽게 식별할 수 있는 인증서 명칭을 입력합니다. 설명으로 인증서의 용도를 식별할 수 있는지 확인하세요. 또한 인증서의 역할을 선택합니다.
5. 인증서 내용 섹션에서 거래 파트너의 공개 인증서를 제공하거나 로컬 인증서용 공개 및 프라이빗 키를 제공하세요.
6. 인증서 용도 섹션에서 이 인증서의 용도를 선택합니다. 암호화, 서명 또는 둘 다에 사용할 수 있습니다.

Note

사용량에 대해 암호화 및 서명을 선택하면 Transfer Family는 두 개의 동일한 인증서(각각 자체 ID가 있음)를 생성합니다. 하나는 사용 값이 ENCRYPTION이고 다른 하나는 사용 값이 SIGNING입니다.

7. 인증서 내용 섹션에 적절한 세부 정보를 입력합니다.

- 자체 서명 인증서를 선택하는 경우 인증서 체인을 제공하지 않습니다.
- 인증서 내용을 붙여 넣습니다.
- 인증서가 자체 서명된 인증서가 아닌 경우 인증서 체인을 제공합니다.
- 이 인증서가 로컬 인증서인 경우 프라이빗 키를 붙여 넣습니다.

8. 인증서 가져오기를 선택하여 프로세스를 완료하고 가져온 인증서의 세부 정보를 저장합니다.

AS2 인증서 교체

인증서는 6개월에서 1년 동안 유효한 경우가 많습니다. 더 오래 유지하려는 프로필을 설정했을 수 있습니다. 이를 용이하게 하기 위해 Transfer Family는 인증서 교체 서비스를 제공합니다. 프로필에 여러 인증서를 지정하여 프로필을 여러 해 동안 계속 사용할 수 있습니다. Transfer Family는 서명(옵션) 및 암호화(필수)에 인증서를 사용합니다. 원하는 경우 두 가지 용도로 사용할 단일 인증서를 지정할 수 있습니다.

인증서 교체는 만료되는 오래된 인증서를 새 인증서로 교체하는 프로세스입니다. 이 전환은 계약 파트너가 아직 아웃바운드 전송을 위한 새 인증서를 구성하지 않았거나 새 인증서를 사용할 수 있는 기간 중에 이전 인증서로 서명 또는 암호화된 페이로드를 보내는 경우 전송이 중단되지 않도록 점진적으로 진행됩니다. 기존 인증서와 새 인증서가 모두 유효한 중간 기간을 유예 기간이라고 합니다.

X.509 인증서에는 Not Before 및 Not After 날짜가 있습니다. 하지만 이러한 파라미터는 관리자에게 충분한 통제 기능을 제공하지 못할 수 있습니다. Transfer Family는 아웃바운드 페이로드에 사용되는 인증서와 인바운드 페이로드에 허용되는 인증서를 통제하는 Active Date 및 Inactive Date 설정을 제공합니다.

아웃바운드 인증서 선택은 전송 날짜 이전의 최대값을 Inactive Date로 사용합니다. 인바운드 프로세스는 범위 Not Before 및 Not After 내 및 범위 Active Date 및 Inactive Date 내에서 인증서를 수락합니다.

다음 표에서는 단일 프로필에 대해 두 개의 인증서를 구성할 수 있는 한 가지 방법을 설명합니다.

두 개의 인증서 교대

명칭	NOT BEFORE (인증 기관에서 관리)	ACTIVE DATE (Transfer Family 에서 설정)	INACTIVE DATE (Transfer Family 에서 설정)	NOT AFTER (인 증 기관에서 설 정)
Cert1(이전 인증 서)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
Cert2(최신 인증 서)	2020-11-01	2020-06-01	2021-06-01	2025-01-01

유념할 사항:

- 인증서에 Active Date 및 Inactive Date를 지정하는 경우 범위는 Not Before 및 Not After의 범위 내에 있어야 합니다.
- 각 프로필에 대해 여러 인증서를 구성하여 모든 인증서의 활성 날짜 범위가 프로필을 사용하려는 기간을 포함하도록 하는 것이 좋습니다.
- 이전 인증서가 비활성화되는 시점과 새 인증서가 활성화되는 시점 사이에 약간의 유예 시간을 지정하는 것이 좋습니다. 위 예에서 첫 번째 인증서는 2020년 12월 31일까지는 비활성화되지 않지만, 두 번째 인증서는 2020년 6월 1일에 활성화되어 6개월의 유예 기간이 제공됩니다. 2020년 6월 1부터 2020년 12월 31일까지의 기간 동안 두 인증서 모두 활성 상태입니다.

AS2 프로필 생성

이 절차를 사용하여 로컬 프로필과 파트너 프로필을 모두 생성할 수 있습니다. 이 절차에서는 Transfer Family 콘솔을 사용하여 AS2 프로필을 생성하는 방법을 설명합니다. 이 방법 대신 AWS CLI 를 사용하려면 [the section called “4단계: 사용자와 사용자의 거래 파트너를 위한 프로필 생성”](#) 섹션을 참조하세요.

AS2 프로필을 생성하려면

- 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
- 왼쪽 탐색 창의 AS2 거래 파트너 에서 프로필 을 선택한 다음 프로필 생성 을 선택합니다.
- 프로필 구성 섹션에서 프로필의 AS2 ID를 입력합니다. 이 값은 AS2 프로토콜별 HTTP 헤더 as2-from에 사용되며 사용할 인증서 등을 결정하는 거래 파트너십을 식별하는 as2-to 데 사용됩니다.

4. 프로필 타입 섹션에서 로컬 프로필 또는 파트너 프로필을 선택합니다.
5. 인증서 섹션의 드롭다운 메뉴에서 하나 이상의 인증서를 선택합니다.

Note

드롭다운 메뉴에 나열되지 않은 인증서를 가져오려면 새 인증서 가져오기를 선택합니다. 그러면 인증서 가져오기 화면에 새 브라우저 창이 열립니다. 인증서 가져오기 절차에 대한 자세한 설명은 [AS2 인증서 가져오기](#) 섹션을 참조하세요.

6. (옵션) 태그 섹션에서 이 프로필을 식별하는 데 도움이 되는 키-값 쌍을 하나 이상 지정합니다.
7. 프로필 생성을 선택하여 프로세스를 완료하고 새 프로필을 저장합니다.

AS2 계약 생성

계약은 Transfer Family 서버와 연결되어 있습니다. Transfer Family를 사용하여 메시지 또는 파일을 교환하는 AS2 프로토콜 사용 거래 파트너에 대한 세부 정보를 지정하고, 인바운드 전송을 위해 외부 파트너 소유 소스에서 Transfer Family 서버로 AS2 파일을 전송합니다.

이 절차에서는 Transfer Family 콘솔을 사용하여 AS2 계약을 생성하는 방법을 설명합니다. AWS CLI 대신 [awscli](#)를 사용하려면 섹션을 참조하세요 [the section called “5단계: 사용자와 사용자의 파트너 간의 계약서 작성”](#).

Transfer Family 서버에 대한 계약을 만들려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택한 다음 AS2 프로토콜을 사용하는 서버를 선택합니다.
3. 서버 세부 정보 페이지에서 계약 섹션으로 스크롤합니다.

Agreements (1) Info						Actions ▾	Add agreement
						< 1 >	
☐	Agreement Id ▾	Name ▲	Status ▾	Profile ▾	Partner profile ▾		
☐	a- 	test	ACTIVE	p- 	p- 		

4. 계약 추가를 선택합니다.
5. 다음과 같이 계약 파라미터를 입력합니다:

- a. 계약 구성 섹션에 설명적인 이름을 입력합니다. 이름으로 계약의 목적을 식별할 수 있는지 확인하세요. 또한 계약 상태를 활성화(기본적으로 선택됨) 또는 비활성으로 설정합니다.
- b. 통신 구성 섹션에서 로컬 프로필과 파트너 프로필을 선택합니다.
- c. 받은 편지함 폴더 구성 섹션에서 수신 파일을 저장할 Amazon S3 버킷과 버킷에 액세스할 수 있는 IAM 역할을 선택합니다. 선택적으로, 버킷에 파일을 저장하는 데 사용할 접두사(폴더)를 입력할 수 있습니다.

예컨대, 버킷에 **DOC-EXAMPLE-BUCKET**, 접두사에 **incoming**를 입력하면 수신된 파일이 / DOC-EXAMPLE-BUCKET/incoming 폴더에 저장됩니다.

- d. (옵션) 태그 섹션에서 태그를 추가합니다.
- e. 계약에 대한 모든 정보를 입력한 후 계약 생성을 선택합니다.

새 계약은 서버 세부 정보 페이지의 계약 섹션에 표시됩니다.

AS2 메시지 전송 및 수신

이 섹션에서는 AS2 메시지를 보내고 받는 프로세스를 설명합니다. 또한 AS2 메시지와 연결된 파일 이름 및 위치에 대한 세부 정보도 제공합니다.

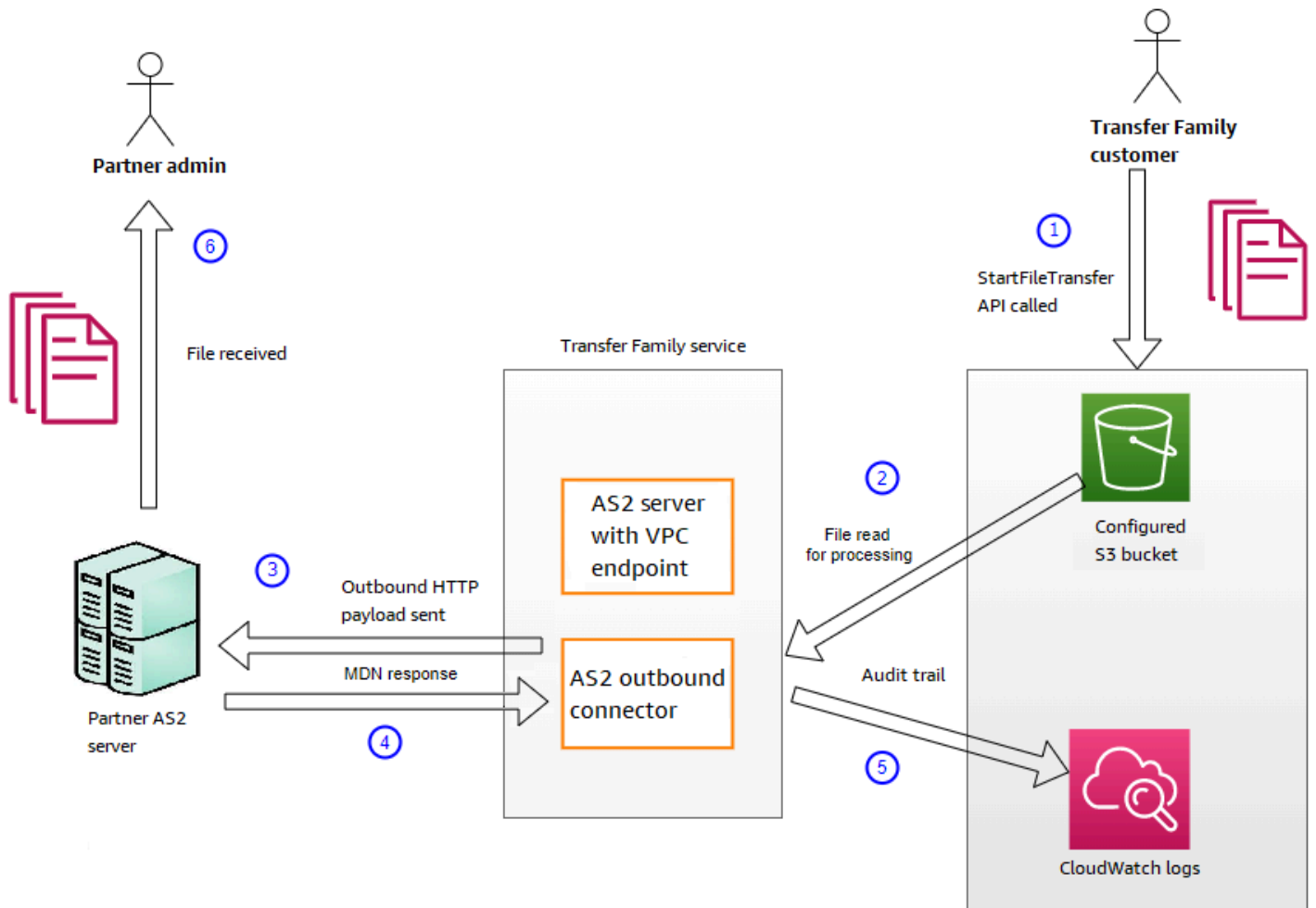
주제

- [AS2 메시지 전송 프로세스](#)
- [AS2 메시지 수신 프로세스](#)
- [를 통해 AS2 메시지 전송 및 수신 HTTPS](#)
- [AS2 커넥터를 사용하여 파일 전송](#)
- [파일 이름 및 위치](#)
- [상태 코드](#)
- [샘플 JSON 파일](#)

AS2 메시지 전송 프로세스

아웃바운드 프로세스는 에서 AWS 외부 클라이언트 또는 서비스로 전송되는 메시지 또는 파일로 정의됩니다. 아웃바운드 메시지의 순서는 다음과 같습니다.

1. 관리자가 `start-file-transfer` AWS Command Line Interface (AWS CLI) 명령 또는 `StartFileTransfer` API 작업을 호출합니다. 이 작업은 `connector` 구성을 참조합니다.
2. Transfer Family는 새 파일 요청을 감지하고 파일을 찾습니다. 파일은 압축, 서명 및 암호화됩니다.
3. 전송 HTTP 클라이언트는 페이로드를 파트너의 AS2 서버로 전송하라는 HTTP POST 요청을 수행합니다.
4. 이 프로세스는 서명된 MDN 응답을 HTTP 응답과 인라인으로 반환합니다(동기식 MDN).
5. 파일이 서로 다른 전송 단계 간에 이동하면 프로세스는 MDN 응답 수신 및 처리 세부 정보를 고객에게 전달합니다.
6. 원격 AS2 서버는 복호화되고 확인된 파일을 파트너 관리자가 사용할 수 있도록 합니다.

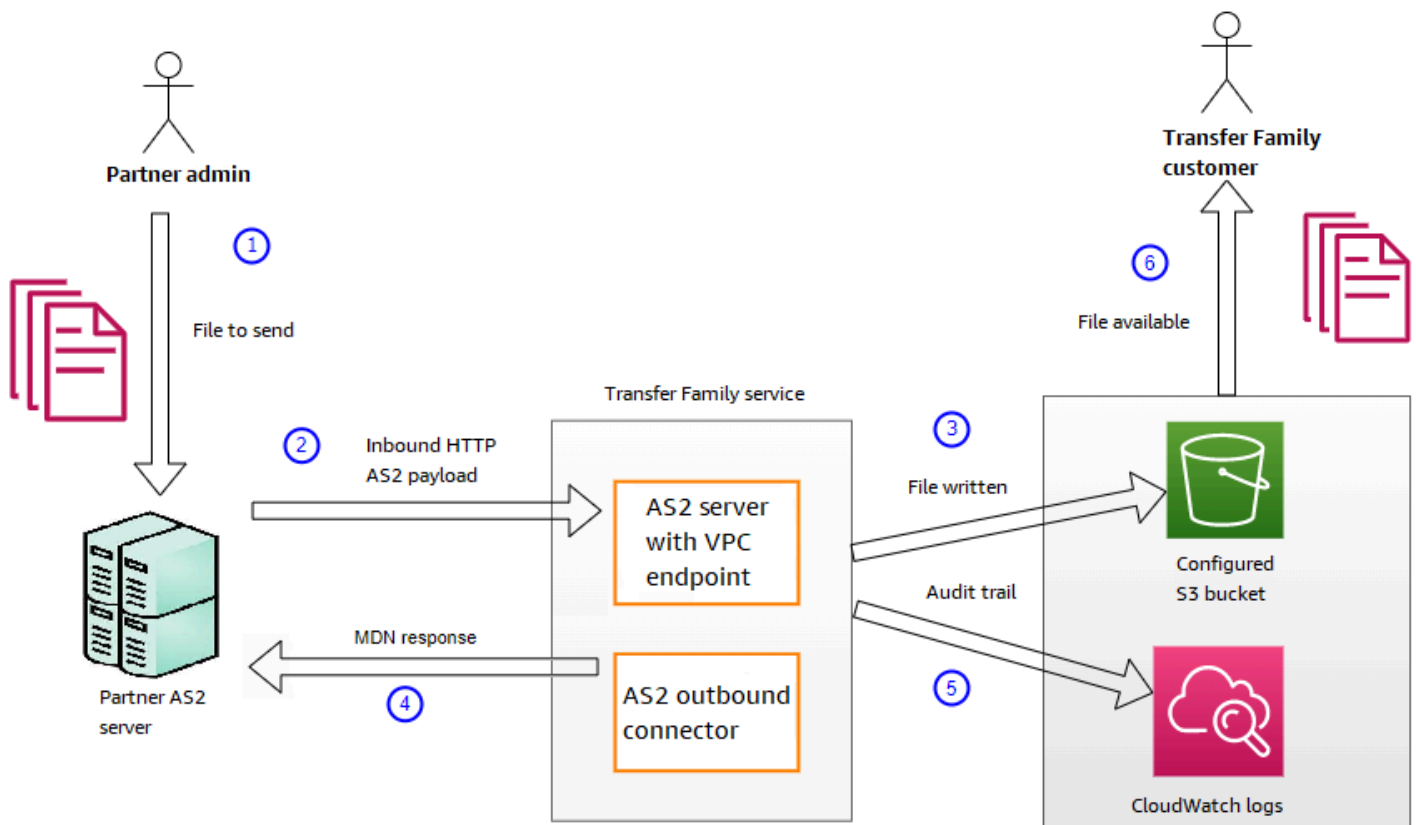


AS2 처리는 일반적인 사용 사례와 기존 AS2지원 서버 구현과의 통합에 중점을 두고 많은 RFC4130 프로토콜을 지원합니다. 지원되는 구성에 대한 자세한 설명은 [AS2 지원되는 구성](#) 섹션을 참조하세요.

AS2 메시지 수신 프로세스

인바운드 프로세스는 AWS Transfer Family 서버로 전송되는 메시지 또는 파일로 정의됩니다. 인바운드 메시지의 순서는 다음과 같습니다.

1. 관리자 또는 자동 프로세스는 파트너의 원격 AS2 서버에서 AS2 파일 전송을 시작합니다.
2. 파트너의 원격 AS2 서버가 파일 콘텐츠에 서명하고 암호화한 다음 Transfer Family에서 호스팅되는 AS2 인바운드 엔드포인트로 HTTP POST 요청을 보냅니다.
3. Transfer Family는 서버, 파트너, 인증서 및 계약에 대해 구성된 값을 사용하여 AS2페이로드를 복호화하고 확인합니다. 파일 콘텐츠는 구성된 Amazon S3 파일 스토어에 저장됩니다.
4. 서명된 MDN 응답은 HTTP 응답과 인라인으로 반환되거나 별도의 HTTP POST 요청을 통해 원래 서버로 비동기적으로 반환됩니다.
5. 감사 추적은 교환에 대한 세부 정보와 CloudWatch 함께 Amazon에 작성됩니다.
6. 암호가 복호화된 파일은 inbox/processed라는 폴더에서 사용할 수 있습니다.



를 통해 AS2 메시지 전송 및 수신 HTTPS

이 섹션에서는 AS2 프로토콜을 사용하여 를 통해 메시지를 보내고 받는 Transfer Family 서버를 구성하는 방법을 설명합니다HTTPS.

를 통해 AS2 메시지 전송 HTTPS

를 사용하여 AS2 메시지를 보내려면 다음 정보가 포함된 커넥터를 HTTPS생성합니다.

- 에 대해 를 URL지정합니다. HTTPS URL
- 암호화 알고리즘의 경우 NONE을 지정합니다.
- [AS2 커넥터 구성](#)에 설명된 대로 커넥터의 나머지 값을 입력합니다.

를 통해 AS2 메시지 수신 HTTPS

AWS Transfer Family AS2 현재 서버는 포트 5080을 통해서만 HTTP 전송을 제공합니다. 그러나 선택한 포트와 인증서를 사용하여 Transfer Family 서버 VPC 엔드포인트 앞에 있는 로드 밸런서TLS에서 를 종료할 수 있습니다. 이 접근 방식을 사용하면 수신 AS2 메시지가 를 사용하도록 할 수 있습니다HTTPS.

사전 조건

- 는 Transfer Family 서버 AWS 리전 와 동일VPC해야 합니다.
- 의 서브넷은 서버를 사용하려는 가용 영역 내에 있어야 VPC 합니다.

Note

각 Transfer Family 서버는 최대 3개의 가용 영역을 지원할 수 있습니다.

- 서버와 동일한 지역에 엘라스틱 IP 주소를 최대 3개까지 할당하세요. 또는 자체 IP 주소 범위()를 가져오도록 선택할 수 있습니다BYOIP.

Note

엘라스틱 IP 주소 수는 서버 엔드포인트에서 사용하는 가용 영역 수와 일치해야 합니다.

Network Load Balancer 구성

에서 인터넷 연결 Network Load Balancer(NLB)를 설정합니다VPC.

Network Load Balancer를 생성하고 서버의 VPC 엔드포인트를 로드 밸런서의 대상으로 정의하려면

1. 에서 Amazon Elastic Compute Cloud 콘솔을 엽니다<https://console.aws.amazon.com/ec2/>.
2. 탐색 창에서, 로드 밸런서를 선택한 다음, 로드 밸런서 만들기를 선택합니다.
3. Network Load Balancer에서 [생성(Create)]을 선택합니다.
4. 기본 구성 섹션에서 다음 정보를 입력합니다.
 - 이름에 로드 밸런서를 설명하는 이름을 입력합니다.
 - 체계에서 인터넷 연결 을 선택합니다.
 - IP address type(IP 주소 유형)에서 IPv4를 선택합니다.
5. 네트워크 매핑 섹션에서 다음 정보를 입력합니다.
 - 에서 생성한 가상 프라이빗 클라우드(VPC)를 VPC선택합니다.
 - 매핑에서 서버 엔드포인트와 함께 사용하는 VPC 것과 동일한 에서 사용할 수 있는 퍼블릭 서브넷과 연결된 가용 영역을 선택합니다.
 - 각 서브넷의 IPv4 주소에서 할당한 탄력적 IP 주소 중 하나를 선택합니다.
6. 리스너 및 라우팅 섹션에서 다음 정보를 입력합니다.
 - 프로토콜에서 TLS을 선택합니다.
 - 포트에서 **5080**를 입력합니다.
 - 기본 작업, 대상 그룹 생성을 선택합니다. 새 대상 그룹을 만드는 세부 사항에 대한 자세한 내용은 [대상 그룹 생성](#)을 참조하세요.

대상 그룹을 생성한 후 기본 작업 필드에 해당 이름을 입력합니다.

7. 보안 리스너 설정 섹션에서 기본 SSL/TLS 인증서 영역에서 인증서를 선택합니다.
8. 로드 밸런서 생성을 선택하여 를 생성합니다NLB.
9. (옵션이지만 권장됨)[Network Load Balancer의 액세스 로그](#)에 설명된 대로 Network Load Balancer의 액세스 로그를 켜서 전체 감사 추적을 유지하세요.

에서 TLS 연결이 종료되므로 이 단계를 수행하는 것이 좋습니다NLB. 따라서 Transfer Family AS2 CloudWatch 로그 그룹에 반영되는 소스 IP 주소는 거래 파트너의 외부 IP 주소 대신 의 NLB프라이빗 IP 주소입니다.

로드 밸런서를 설정하고 나면 클라이언트는 사용자 지정 포트 리스너를 통해 로드 밸런서와 통신합니다. 그러면 로드 밸런서가 포트 5080을 통해 서버와 통신합니다.

대상 그룹 생성

1. 이전 절차에서 대상 그룹 만들기를 선택하면 새 대상 그룹에 대한 그룹 세부 정보 지정 페이지로 이동합니다.
2. 기본 구성 섹션에서, 다음 정보를 입력합니다.
 - 대상 타입 선택에서 IP 주소를 선택합니다.
 - 대상 그룹 이름에 대상 그룹의 이름을 입력합니다.
 - 프로토콜에서 TCP을 선택합니다.
 - 포트에서 **5080**를 입력합니다.
 - IP address type(IP 주소 유형)에서 IPv4를 선택합니다.
 - 에서 Transfer Family AS2 서버에 대해 VPC 생성한 를 VPC선택합니다.
3. 상태 확인 섹션에서 상태 확인 프로토콜 TCP을 선택합니다.
4. Next(다음)를 선택합니다.
5. 대상 등록 페이지에서 다음 정보를 입력합니다.
 - 네트워크 의 경우 Transfer Family AS2 서버에 대해 VPC 생성한 이 지정되어 있는지 확인합니다.
 - IPv4 주소 에 Transfer Family AS2 서버 엔드포인트의 프라이빗 IPv4 주소를 입력합니다.

서버에 엔드포인트가 두 개 이상 있는 경우 IPv4 주소 추가를 선택하여 다른 IPv4 주소를 입력할 다른 행을 추가합니다. 모든 서버 엔드포인트의 사설 IP 주소를 입력할 때까지 이 프로세스를 반복합니다.

 - Ports가 **5080**로 설정되어 있는지 확인하세요.
 - 아래 보류 중인 항목으로 포함을 선택하여 항목을 대상 검토 섹션에 추가하세요.
6. 대상 검토 섹션에서 IP 대상을 검토하세요.
7. 대상 그룹 생성을 선택한 다음 이전 절차로 돌아가 를 생성하고 표시된 새 대상 그룹을 NLB 입력합니다.

탄력적 IP 주소에서 서버 액세스 테스트

탄력적 IP 주소 또는 Network Load Balancer 의 DNS 이름을 사용하여 사용자 지정 포트를 통해 서버에 연결합니다.

⚠ Important

로드 밸런서에 구성된 서브넷의 [네트워크 액세스 제어 목록\(네트워크 ACLs\)](#)을 사용하여 [클라이언트 IP 주소에서 서버에](#) 대한 액세스를 관리합니다. 네트워크 ACL 권한은 서브넷 수준에서 설정되므로 규칙은 서브넷을 사용하는 모든 리소스에 적용됩니다. 로드 밸런서의 대상 타입이 인스턴스가 아닌 IP 주소로 설정되어 있기 때문에 보안 그룹을 사용하여 클라이언트 IP 주소에서의 액세스를 제어할 수 없습니다. 따라서 로드 밸런서는 원본 IP 주소를 보존하지 않습니다. [Network Load Balancer의 상태 확인](#)이 실패하면 로드 밸런서가 서버 엔드포인트에 연결할 수 없다는 의미입니다. 이 문제를 해결하려면 다음을 확인하세요.

- 서버 [엔드포인트의 관련 보안 그룹](#)이 로드 밸런서에 구성된 서브넷으로부터의 인바운드 연결을 허용하는지 확인하세요. 로드 밸런서는 포트 5080을 통해 서버 엔드포인트에 연결할 수 있어야 합니다.
- 서버 상태가 온라인인지 확인합니다.

AS2 커넥터를 사용하여 파일 전송

AS2 커넥터는 Transfer Family 서버에서 파트너 소유 외부 대상으로 AS2 메시지를 전송하기 위해 거래 파트너 간에 관계를 설정합니다.

Transfer Family를 사용하여 다음 start-file-transfer AWS Command Line Interface (AWS CLI) 명령에 설명된 대로 커넥터 ID와 파일 경로를 참조하여 AS2 메시지를 보낼 수 있습니다.

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/myfile2.txt"
```

커넥터의 세부 정보를 가져오려면 다음 명령을 실행합니다.

```
aws transfer list-connectors
```

list-connectors 명령은 커넥터의 커넥터 ID, URLs, 및 Amazon 리소스 이름(ARNs)을 반환합니다.

특정 커넥터의 속성을 반환하려면 사용하려는 ID로 다음 명령을 실행합니다.

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

`describe-connector` 명령은 URL, 역할, 프로파일, 메시지 처리 알림(MDNs), 태그 및 모니터링 지표를 포함하여 커넥터의 모든 속성을 반환합니다.

JSON 및 파일을 확인하여 파트너가 MDN 파일을 성공적으로 수신했는지 확인할 수 있습니다. 이러한 파일 이름은 [파일 이름 및 위치](#)에 설명된 규칙에 따라 지정됩니다. 커넥터를 생성할 때 로깅 역할을 구성한 경우 CloudWatch 로그에서 AS2 메시지 상태를 확인할 수도 있습니다.

AS2 커넥터 세부 정보를 보려면 섹션을 참조하세요 [AS2 커넥터 세부 정보 보기](#). AS2 커넥터 생성에 대한 자세한 내용은 섹션을 참조하세요 [AS2 커넥터 구성](#).

파일 이름 및 위치

이 섹션에서는 AS2 전송을 위한 파일 이름 지정 규칙에 대해 설명합니다.

인바운드 파일 전송에 대해 다음 사항을 참조하세요.

- 계약서에 기본 디렉터리를 지정합니다. 기본 디렉터리는 접두사(있는 경우)와 결합된 Amazon S3 버킷 이름입니다. 예: /DOC-EXAMPLE-BUCKET/AS2-folder.
- 수신 파일이 성공적으로 처리되면 파일(및 해당 JSON 파일)이 /processed 폴더에 저장됩니다. 예: /DOC-EXAMPLE-BUCKET/AS2-folder/processed.

JSON 파일에는 다음 필드가 포함되어 있습니다.

- 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
- 수신 파일을 성공적으로 처리할 수 없는 경우 파일(및 해당 JSON 파일)이 /failed 폴더에 저장됩니다. 예: /DOC-EXAMPLE-BUCKET/AS2-folder/failed.
- 전송된 파일은 processed 폴더에 *original_filename.messageId.original_extension*로 저장됩니다. 즉, 전송 메시지 ID가 파일 이름에 원래 확장명 앞에 추가됩니다.
- JSON 파일이 생성되고 로 저장됩니다 *original_filename.messageId.original_extension.json*. 메시지 ID가 추가될 뿐 아니라 전송된 파일 이름에도 문자열 .json이 추가됩니다.
- 메시지 처리 알림(MDN) 파일이 생성되어 로 저장됩니다 *original_filename.messageId.original_extension.mdn*. 메시지 ID가 추가될 뿐 아니라 전송된 파일 이름에도 문자열 .mdn이 추가됩니다.
- ExampleFileInS3Payload.dat라는 인바운드 파일이 있는 경우 다음 파일이 생성됩니다.
 - File –
ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
 - JSON –
ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
 - MDN –
ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

아웃바운드 전송의 경우 받는 메시지 파일이 없다는 점을 제외하면 이름이 비슷하며 전송된 메시지의 전송 ID가 파일 이름에 추가된다는 차이점이 있습니다. 전송 ID는 StartFileTransfer API 작업에 의해 반환됩니다(또는 다른 프로세스 또는 스크립트가 이 작업을 호출할 때).

- transfer-id는 파일 전송과 관련된 식별자입니다. StartFileTransfer 호출에 포함된 모든 요청은 transfer-id를 공유합니다.

- 기본 디렉터리는 소스 파일에 사용하는 경로와 동일합니다. 즉, 기본 디렉터리는 StartFileTransfer API 작업 또는 start-file-transfer AWS CLI 명령에서 지정하는 경로입니다. 예:

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-BUCKET/AS2-folder/
file-to-send.txt
```

이 명령을 실행하면 JSON 파일이 /DOC-EXAMPLE-BUCKET/AS2-folder/processed (성공적인 전송의 경우) 또는 /DOC-EXAMPLE-BUCKET/AS2-folder/failed (실패한 전송의 경우)에 저장됩니다.

- JSON 파일이 생성되고 로 저장됩니다
다 `original_filename.transferId.messageId.original_extension.json`.
- MDN 파일이 생성되고 로 저장됩니다
다 `original_filename.transferId.messageId.original_extension.mdn`.
- ExampleFileOutTestOutboundSyncMdn.dat라는 아웃바운드 파일이 있는 경우 다음 파일이 생성됩니다:
 - 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

CloudWatch 로그를 확인하여 실패한 모든 를 포함하여 전송의 세부 정보를 볼 수도 있습니다.

상태 코드

다음 표에는 사용자 또는 파트너가 AS2 메시지를 보낼 때 CloudWatch 로그에 로깅할 수 있는 모든 상태 코드가 나열되어 있습니다. 다양한 메시지 처리 단계는 다양한 메시지 유형에 적용되며 모니터링 전용입니다. COMPLETED 및 FAILED 상태는 처리의 마지막 단계를 나타내며 JSON 파일에 표시됩니다.

코드	설명	처리가 완료되었습니까?
PROCESSING	메시지가 최종 형식으로 변환되는 중입니다. 예를 들어 압축 해제 및 복호화 단계 모두 이상 상태를 갖습니다.	아니요

코드	설명	처리가 완료되었습니까?
MDN_TRANSMIT	메시지 처리가 MDN 응답을 보내는 중입니다.	아니요
MDN_RECEIVE	메시지 처리가 MDN 응답을 수신하고 있습니다.	아니요
COMPLETED	메시지 처리가 성공적으로 완료되었습니다. 이 상태에는 MDN가 인바운드 메시지 또는 아웃바운드 메시지 MDN 확인을 위해 전송되는 시기가 포함됩니다.	예
FAILED	메시지 처리에 실패했습니다. 오류 코드 목록은 섹션을 참조하세요 AS2 오류 코드 .	예

샘플 JSON 파일

이 섹션에서는 실패한 성공적인 전송 및 전송을 위한 샘플 JSON 파일을 포함하여 인바운드 및 아웃바운드 전송 모두에 대한 샘플 파일을 나열합니다.

성공적으로 전송된 샘플 아웃바운드 파일:

```
{
  "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": "/DOC-EXAMPLE-BUCKET/as2testcell10000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

전송에 실패한 샘플 아웃바운드 파일:

```
{
  "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": "/testbucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}
```

성공적으로 전송된 샘플 인바운드 파일:

```
{
  "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_0ID_PartnerA_0ID.dat",
"server-id": "s-5f7422b04c2447ef9",
"timestamp": "2022-07-11T23:36:36.105030Z"
}

```

전송에 실패한 샘플 인바운드 파일:

```

{
  "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"
}

```

AS2 사용량 모니터링

Amazon CloudWatch 및 AWS CloudTrail 을 사용하여 AS2 활동을 모니터링할 수 있습니다. 다른 Transfer Family 서버 지표(metrics)를 보려면 [에 대한 Amazon CloudWatch 로깅 AWS Transfer Family](#)을 참조하십시오.

AS2 지표

지표	설명
InboundMessage	거래 파트너로부터 성공적으로 수신한 AS2 메시지의 총 개수.
	단위: 개

지표	설명
	기간: 5분
InboundFailedMessage	거래 파트너로부터 성공적으로 수신되지 못한 AS2 메시지의 총 개수. 즉, 거래 파트너가 메시지를 보냈지만 Transfer Family 서버가 메시지를 성공적으로 처리하지 못했습니다. 단위: 개 기간: 5분
OutboundMessage	Transfer Family 서버에서 거래 파트너로 성공적으로 보낸 AS2 메시지의 총 개수입니다. 단위: 개 기간 = 5분
OutboundFailedMessage	거래 파트너에게 성공적으로 전송되지 못한 AS2 메시지의 총 개수. 즉, Transfer Family 서버에서 전송되었지만 거래 파트너가 성공적으로 수신하지 못했습니다. 단위: 개 기간: 5분

AS2 상태 코드

다음 표에는 귀하 또는 파트너가 AS2 메시지를 보낼 때 CloudWatch 로그에 기록할 수 있는 모든 상태 코드가 나와 있습니다. 메시지 유형마다 다른 메시지 처리 단계가 적용되며 모니터링용으로만 사용됩니다. 완료 및 실패 상태는 처리의 마지막 단계를 나타내며 JSON 파일에서 확인할 수 있습니다.

코드	설명	처리가 완료되었나요?
가공	메시지가 최종 형식으로 변환되는 중입니다. 예를 들어, 압축	아니요

코드	설명	처리가 완료되었나요?
	해제 단계와 암호 해독 단계 모두 이 상태입니다.	
MDN_TRANSBIT	메시지 프로세싱이 MDN 응답을 보내는 중입니다.	아니요
MDN_RECEIVE	메시지 프로세싱에서 MDN 응답을 받고 있습니다.	아니요
완료됨	메시지 처리가 성공적으로 완료되었습니다. 이 상태에는 인바운드 메시지 또는 아웃바운드 메시지의 MDN 확인을 위해 MDN을 보내는 경우가 포함됩니다.	예
FAILED	메시지 처리에 실패했습니다. 오류 코드 목록은 여기 를 참조하십시오.	예

AS2 오류 코드

다음 표는 AS2 파일 전송에서 발생할 수 있는 오류 코드를 나열하고 설명합니다.

AS2 오류 코드

코드	오류	설명 및 해상도
ACCESS_DENIED	- 액세스가 거부되었습니다. 액세스 역할에 필요한 권한이 있는지 확인하세요. - 잘못된 파일 경로 <i>send-file-path</i> - ErrorCode 다음과 같은 <i>##-##</i> 자격 증명을 가져오지 못했습니다.	유효하지 않거나 형식이 StartFileTransfer 잘못된 요청을 처리할 때 발생합니다. SendFilePaths . 즉, 경로에 Amazon S3 버킷 이름이 없거나 경로에 유효하지 않은 문자가 포함되어 있습니다. Transfer Family가 액세스 역할

코드	오류	설명 및 해상도
		또는 로깅 역할을 맡지 못하는 경우에도 발생합니다. 경로에 유효한 Amazon S3 버킷과 키 이름이 포함되어 있는지 확인하십시오.
AGREEMENT_NOT_FOUND	계약을 찾을 수 없습니다.	계약을 찾을 수 없거나 계약이 비활성 프로파일과 연결되어 있습니다. Transfer Family 서버 내에서 계약을 업데이트하여 활성 프로파일을 포함하십시오.
CONNECTOR_NOT_FOUND	커넥터 또는 관련 구성을 찾을 수 없습니다.	계약을 찾을 수 없거나 계약이 비활성 프로파일과 연결되어 있습니다. 활성 프로파일을 포함하도록 커넥터를 업데이트하십시오.

코드	오류	설명 및 해상도
CREDENTIALS_RETRIEVAL_FAILED	1. Secrets Manager에서 보안 암호를 찾을 수 없습니다. 2. Secrets Manager에 액세스할 수 없습니다 3. Secrets Manager에서 보안 암호 해독 실패 4. 제한으로 인해 보안 암호 값을 가져올 수 없습니다.	AS2 Basic 인증의 경우 보안 암호를 올바르게 형식화해야 합니다. 다음 해결 방법은 이전 열에 나열된 오류에 해당합니다. 1. 보안 암호 ID가 정확한지 확인하십시오. 2. 액세스 역할에 암호를 읽을 수 있는 적절한 권한이 있는지 확인하십시오. 접근 역할은 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 그 역할이 StartFileTransfer 와 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하십시오. 3. 고객 관리 키를 보안 암호로 사용하는 경우 액세스 역할에 AWS Key Management Service (AWS KMS) 키에 대한 권한이 있는지 확인하십시오. 4. 해당 할당량은 비밀 처리를 위한 할당량을 참조하십시오.

코드	오류	설명 및 해상도
DECOMPRESSION_FAILED	메시지 압축을 풀지 못했습니다.	전송된 파일이 손상되었거나 압축 알고리즘이 유효하지 않습니다. 메시지를 다시 전송하고 ZLIB 압축이 사용되는지 확인하거나 압축을 사용하지 않고 메시지를 다시 보내십시오.
DECRYPT_FAILED	### ID 메시지를 해독하지 못했습니다. 파트너가 올바른 공개 암호화 키를 가지고 있는지 확인하십시오.	복호화에 실패했습니다. 파트너가 유효한 인증서를 사용하여 페이로드를 전송했고 암호화는 유효한 암호화 알고리즘을 사용하여 수행되었는지 확인합니다.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	엔벨로핑된 MimePart를 파싱할 수 없습니다.	MIME 페이로드가 손상되었거나 지원되지 않는 SMIME 형식입니다. 발신자는 사용 중인 형식이 지원되는지 확인한 다음 페이로드를 다시 전송해야 합니다.
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	일치하는 암호 해독 키를 찾을 수 없습니다.	파트너 프로필에 메시지와 일치하는 인증서가 할당되지 않았거나 메시지와 일치하는 인증서가 현재 만료되었거나 더 이상 유효하지 않습니다. 파트너 프로필을 업데이트하고 유효한 인증서가 포함되어 있는지 확인해야 합니다.

코드	오류	설명 및 해상도
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	지원되지 않는 알고리즘(ID: <i>encryption-ID</i>)을 사용하여 SMIME 페이로드 암호 해독을 요청했습니다.	원격 발신자가 지원되지 않는 암호화 알고리즘이 포함된 AS2 페이로드를 전송했습니다. 발신자는 AWS Transfer Family에서 지원하는 암호화 알고리즘을 선택해야 합니다.
DUPLICATE_MESSAGE	중복 또는 이중 처리된 단계.	페이로드에 중복 처리 단계가 있습니다. 예를 들어 2개의 암호화 단계가 있습니다. 서명, 압축, 암호화를 한 번에 완료하여 메시지를 재전송합니다.
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	프로필에서 유효한 공개 암호화 인증서를 찾을 수 없음: <i>local-profile-ID</i>	Transfer Family가 아웃바운드 메시지를 암호화하려고 시도하지만 로컬 프로필에 대한 암호화 인증서를 찾을 수 없습니다. 해결 옵션: - 로컬 프로필에 암호화를 위한 인증서와 개인 키가 첨부되어 있는지 확인하십시오. - 암호화 인증서가 현재 활성 상태인지 확인하십시오.

코드	오류	설명 및 해상도
ENCRYPTION_FAILED	## ## 파일을 암호화하지 못했습니다.	전송할 파일은 암호화에 사용할 수 없습니다. 파일이 예상 AS2 위치에 있고 AWS Transfer Family가 파일을 읽을 권한이 있는지 확인하십시오.
FILE_SIZE_TOO_LARGE	파일 크기가 너무 큼니다.	이는 파일 크기 제한을 초과하는 파일을 보내거나 받을 때 발생합니다.
HTTP_ERROR_RESPONSE_FROM_PARTNER	### URL ID= <i>message-ID</i> 인 메시지에 대해 상태 400을 반환했습니다.	파트너의 AS2 서버와 통신할 때 예상치 못한 HTTP 응답 코드가 반환되었습니다. 파트너는 AS2 서버 로그에서 추가 진단을 제공할 수 있습니다.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	암호화가 필요합니다.	파트너가 Transfer Family에 암호화되지 않은 메시지를 보냈지만 이 메시지는 지원되지 않습니다. 발신자는 암호화된 페이로드를 사용해야 합니다.
INVALID_ENDPOINT_PROTOCOL	HTTP와 HTTPS만 지원됩니다.	AS2 커넥터 구성에서 HTTP 또는 HTTPS를 프로토콜로 지정해야 합니다.

코드	오류	설명 및 해상도
INVALID_REQUEST	1. 메시지 헤더에 문제가 있습니다. 2. 보안 JSON을 구문 분석할 수 없습니다. 시크릿 JSON이 예상 형식과 일치하지 않았습니다. 3. 보안 암호는 JSON 문자열이어야 합니다. 4. 사용자 이름은 콜론을 포함할 수 없습니다. 사용자 이름은 제어 문자를 포함할 수 없습니다. 사용자 이름은 ASCII 문자만 포함해야 합니다. 비밀번호는 제어 문자를 포함할 수 없습니다. 비밀번호는 ASCII 문자만 포함해야 합니다.	이 오류에는 여러 가지 원인이 있습니다. 다음 해결 방법은 이전 열에 나열된 오류에 해당합니다. 1. as2-from 및 as2-to 필드를 확인합니다. 원본 메시지 ID가 MDN 형식에 맞는지 확인하십시오. 또한 메시지 ID 형식에 AS2 헤더가 누락되지 않았는지 확인하십시오. 2. AS2 커넥터에 대한 기본 인증 활성화에 설명된 대로 암호 값이 문서화된 형식과 일치하는지 확인하십시오. 3. 암호는 바이너리가 아닌 문자열로 제공되어야 합니다. 4. 사용자 이름 또는 비밀번호를 필요에 따라 수정하십시오.
INVALID_URL_FORMAT	잘못된 URL 형식: <i>URL</i>	잘못된 URL로 구성된 커넥터를 사용하여 아웃바운드 메시지를 보낼 때 이 문제가 발생합니다. 커넥터가 유효한 HTTP 또는 HTTPS URL로 구성되어 있는지 확인하십시오.

코드	오류	설명 및 해상도
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	해당 사항 없음	수신자는 발신자를 인증할 수 없습니다. 거래 파트너가 처리 수정자 오류: authentication-failed와 함께 Transfer Family에 MDN을 반환합니다.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	해당 사항 없음	이는 수신자가 메시지 내용을 압축 해제할 수 없을 때 발생합니다. 거래 파트너가 처리 수정자 오류: decompression-failed와 함께 Transfer Family에 MDN을 반환합니다.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	해당 사항 없음	수신자는 메시지 내용을 해독할 수 없습니다. 거래 파트너가 처리 수정자 오류: authentication-failed와 함께 Transfer Family에 MDN을 반환합니다.
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	해당 사항 없음	수신자는 메시지가 서명되거나 암호화되기를 기대하지만, 그렇지 않습니다. 거래 파트너가 처분 수정자 Error: 와 함께 Transfer Family에 MDN을 반환합니다. insufficient-message-security 커넥터에서 서명 및/또는 암호화를 활성화하여 거래 파트너의 기대에 부합하도록 하십시오.

코드	오류	설명 및 해상도
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	해당 사항 없음	수신자는 콘텐츠 무결성을 확인할 수 없습니다. 거래 파트너가 처분 수정자 Error: 와 함께 Transfer Family에 MDN을 반환합니다. integrity-check-failed
PATH_NOT_FOUND	디렉터리 <i>file-path</i> 를 생성할 수 없습니다. 상위 경로를 찾을 수 없습니다.	Transfer Family가 고객의 Amazon S3 버킷에 디렉터를 생성하려고 시도했지만 버킷을 찾을 수 없습니다. StartFileTransfer 명령에 언급된 각 경로에 기존 버킷의 이름이 포함되어 있는지 확인하십시오.
SEND_FILE_NOT_FOUND	파일 경로 <i>## ##</i> 를 찾을 수 없습니다.	Transfer Family는 파일 보내기 작업에서 파일을 찾을 수 없습니다. 구성된 홈 디렉토리 및 경로가 유효하고 Transfer Family에 파일에 대한 읽기 권한이 있는지 확인합니다.
SERVER_NOT_FOUND	이벤트와 연결된 서버를 찾을 수 없습니다.	Transfer Family가 메시지를 받았을 때 서버를 찾지 못했습니다. 수신 메시지를 처리하는 중에 서버가 삭제되면 이런 일이 발생할 수 있습니다.

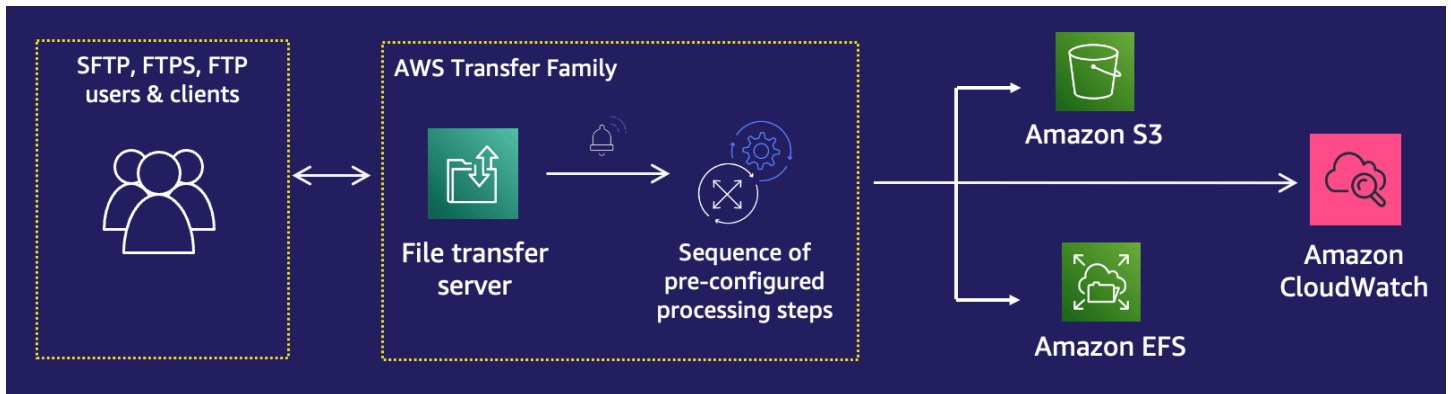
코드	오류	설명 및 해상도
SERVER_NOT_ONLINE	서버 <i>server-ID</i> 가 온라인 상태가 아닙니다.	Transfer Family 서버가 오프라인 상태입니다. 메시지를 수신하고 처리할 수 있도록 서버를 시작합니다.
SIGNING_FAILED	파일에 서명하지 못했습니다.	전송할 파일을 서명할 수 없거나 서명을 수행할 수 없습니다. 파일이 예상 AS2 위치에 있고 AWS Transfer Family가 파일을 읽을 권한이 있는지 확인하십시오.
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	프로필: ## 프로필 ID에 대한 인증서를 찾을 수 없습니다.	아웃바운드 메시지에 서명하려고 시도했지만 로컬 프로필에 대한 서명 인증서를 찾을 수 없습니다. 해결 옵션: • 로컬 프로필에 서명을 위한 인증서와 개인 키가 첨부되어 있는지 확인하십시오. • 서명 인증서가 현재 활성 상태인지 확인하십시오.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	호스트 이름을 IP 주소로 확인할 수 없습니다.	Transfer Family는 AS2 커넥터에 구성된 공용 DNS 서버에서 DNS 대 IP 주소 확인을 수행할 수 없습니다. 커넥터가 유효한 파트너 URL을 가리키도록 업데이트하십시오.

코드	오류	설명 및 해상도
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	엔드포인트에 대한 연결이 시간 초과되었습니다.	Transfer Family는 구성된 파트너의 AS2 서버에 소켓 연결을 설정할 수 없습니다. 구성된 IP 주소에서 파트너의 AS2 서버를 사용할 수 있는지 확인하십시오.
UNABLE_TO_RESOLVE_HOSTNAME	### ##의 호스트 이름을 확인할 수 없습니다.	Transfer Family 서버가 공용 DNS 서버를 사용하여 파트너의 호스트 이름을 확인할 수 없습니다. 구성된 호스트가 등록되어 있고 DNS 레코드를 게시할 시간이 있었는지 확인하십시오.
VERIFICATION_FAILED	### ID AS2 메시지에 대한 서명 확인에 실패했거나 MIC 코드가 일치하지 않았습니다.	발신자의 서명 인증서가 원격 프로파일의 서명 인증서와 일치하는지 확인하십시오. 또한 MIC 알고리즘이 AWS Transfer Family과 호환되는지도 확인하십시오.

코드	오류	설명 및 해상도
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- 프로필: ### ### ID 메시지 서명과 일치하는 공개 인증서를 찾을 수 없습니다. - 존재하지 않는 프로필 (partner-profile-ID)에 대한 인증서를 얻을 수 없습니다. - 프로필(partner-profile-ID)에서 유효한 인증서를 찾을 수 없습니다.	AWS Transfer Family이 받은 메시지의 서명을 확인하려고 하는데 파트너 프로필과 일치하는 서명 인증서를 찾을 수 없습니다. 해결 옵션: - 파트너 프로필에 서명을 위한 인증서가 첨부되어 있는지 확인하십시오. - 인증서가 현재 활성 상태인지 확인하십시오. - 인증서가 파트너를 위한 정확한 서명 인증서인지 확인하십시오.

AWS Transfer Family 관리형 워크플로

AWS Transfer Family 는 파일 처리를 위한 관리형 워크플로를 지원합니다. 관리형 워크플로를 사용하면, SFTP, FTPS 또는 를 통해 파일을 전송한 후 워크플로를 시작할 수 있습니다FTP. 이 기능을 사용하면 파일 처리에 필요한 모든 단계를 조정하여 business-to-business (B2B) 파일 교환에 대한 규정 준수 요구 사항을 안전하고 비용 효율적으로 충족할 수 있습니다. 또한 감사 및 가시성의 end-to-end 이점을 누릴 수 있습니다.



관리형 워크플로는 파일 처리 작업을 오케스트레이션하여 다운스트림 애플리케이션에서 데이터를 사용하기 전에 데이터를 사전 처리하는 데 도움이 됩니다. 이러한 파일 처리 작업에는 다음이 포함될 수 있습니다.

- 파일을 사용자별 폴더로 이동.
- 워크플로의 일부로 파일 복호화.
- 파일 태그 지정.
- AWS Lambda 함수를 생성하고 워크플로에 연결하여 사용자 지정 처리 수행.
- 파일이 성공적으로 전송되면 알림을 보냅니다. (이 사용 사례를 자세히 설명하는 블로그 게시물은 [AWS Transfer Family 관리형 워크플로를 사용하여 파일 전송 알림 사용자 지정](#)을 참조하세요.)

조직 내 여러 사업부에 걸쳐 있는 일반적인 업로드 후 파일 처리 작업을 빠르게 복제하고 표준화하려면 코드형 인프라(IaC)를 사용하여 워크플로를 배포할 수 있습니다. 전체 업로드된 파일에 대해 관리형 워크플로를 시작하도록 지정할 수 있습니다. 또한 세션이 조기에 끊어져 일부만 업로드된 파일에 대해 다른 관리형 워크플로를 시작하도록 지정할 수 있습니다. 기본 제공되는 예외 처리 기능을 통해 파일 처리 결과에 신속하게 대응하는 동시에 오류 처리 방법을 제어할 수 있습니다. 또한 각 워크플로 단계는 세부 로그를 생성하며, 이를 감사하여 데이터 계보를 추적할 수 있습니다.

시작하려면 다음 단계를 수행합니다.

1. 요구 사항에 따라 복사, 태그 지정 및 기타 단계와 같은 사전 처리 작업을 포함하도록 워크플로를 설정합니다. 세부 정보는 [워크플로 만들기](#)를 참조하세요.
2. Transfer Family가 워크플로를 실행하는 데 사용하는 실행 역할을 구성합니다. 세부 정보는 [IAM 워크플로 정책](#)를 참조하세요.
3. 워크플로를 서버에 매핑하여 파일 도착 시 이 워크플로에 지정된 작업이 실시간으로 평가 및 시작 되도록 합니다. 세부 정보는 [워크플로 구성 및 실행](#)를 참조하세요.

관련 정보

- 워크플로 실행을 모니터링하려면 [Transfer Family에 대한 CloudWatch 지표 사용](#)을 참조하세요.
- 자세한 실행 로그 및 문제 해결 정보는 [Amazon을 사용하여 워크플로 관련 오류 해결 CloudWatch](#)를 참조하세요.
- 참석할 수 있는 워크숍이 있어 File Transfer 솔루션을 구축할 수 있습니다. 이 솔루션은 관리형 SFTP/FTPS 엔드포인트 AWS Transfer Family 에 를 활용하고 사용자 관리를 위해 Amazon Cognito 및 DynamoDB를 활용합니다. 이 워크숍의 세부 정보는 [여기](#)에서 확인할 수 있습니다.
- Transfer Family 워크플로에 대한 간략한 소개는 [AWS Transfer Family 관리형 워크플로](#)를 보세요.

주제

- [워크플로 만들기](#)
- [사전 정의된 단계 사용](#)
- [사용자 지정 파일 처리 단계 사용](#)
- [IAM 워크플로 정책](#)
- [워크플로의 예외 처리](#)
- [워크플로 실행 모니터링](#)
- [템플릿에서 워크플로 생성](#)
- [Transfer Family 서버에서 워크플로 제거](#)
- [관리형 워크플로 제한 및 제약 조건](#)

관리형 워크플로를 시작하는 데 도움이 더 필요하다면 다음 리소스를 참조하세요.

- [AWS Transfer Family 관리형 워크플로 데모 비디오](#)
- [AWS Transfer Family 워크플로 블로그 게시물을 사용하여 클라우드 네이티브 파일 전송 플랫폼 구축](#)

워크플로 만들기

이 주제에 설명된 AWS Management Console대로 를 사용하여 관리형 워크플로를 생성할 수 있습니다. 워크플로를 가능한 한 쉽게 만들기 위해 콘솔의 대부분의 섹션에서 상황별 도움말 패널을 사용할 수 있습니다.

워크플로에는 다음과 같은 두 가지 단계가 있습니다.

- 공칭 단계 - 공칭 단계는 들어오는 파일에 적용할 파일 처리 단계입니다. 공칭 단계를 두 개 이상 선택한 경우 각 단계는 선형 시퀀스로 처리됩니다.
- 예외 처리 단계 - 예외 처리자는 명목 단계가 실패하거나 검증 오류가 발생할 경우 AWS Transfer Family 실행되는 파일 처리 단계입니다.

워크플로 만들기

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 워크플로를 선택합니다.
3. 워크플로 페이지에서 워크플로 생성을 선택합니다.
4. 워크플로 생성 페이지에서 설명을 입력합니다. 이 설명은 워크플로 페이지에 표시됩니다.
5. 공칭 단계 섹션에서 단계 추가를 선택합니다. 단계를 하나 이상 추가합니다.
 - a. 사용 가능한 옵션에서 단계 타입을 선택합니다. 다양한 단계 타입에 대한 자세한 내용은 [the section called “사전 정의된 단계 사용”](#)을 참조하세요.
 - b. 다음을 선택한 다음 해당 단계에 대한 파라미터를 구성합니다.
 - c. 다음을 선택한 다음 해당 단계에 대한 세부 정보를 검토합니다.
 - d. 단계 생성을 선택하여 단계를 추가하고 계속합니다.
 - e. 필요에 따라 단계를 계속 추가합니다. 워크플로의 최대 단계 수는 8개입니다.
 - f. 필요한 공칭 단계를 모두 추가한 후 예외 처리기 — 옵션 섹션으로 아래로 스크롤하여 단계 추가를 선택합니다.

Note

실패 알림을 실시간으로 받을 수 있도록 워크플로가 실패할 때 실행할 예외 처리기와 단계를 설정하는 것이 좋습니다.

6. 예외 처리기를 구성하려면 앞에서 설명한 것과 같은 방식으로 단계를 추가하세요. 파일로 인해 특정 단계에서 예외가 발생하는 경우 예외 처리기가 하나씩 간접적으로 호출됩니다.
7. (옵션) 태그 섹션으로 스크롤하여 워크플로에 사용할 태그를 추가합니다.
8. 플릿 구성을 살펴본 후 워크플로 생성을 선택합니다.

Important

워크플로를 만든 후에는 편집할 수 없으므로 구성을 주의 깊게 검토해야 합니다.

워크플로 구성 및 실행

워크플로를 실행하려면 먼저 Transfer Family 서버에 연결해야 합니다.

업로드된 파일에서 워크플로를 실행하도록 Transfer Family를 구성하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택합니다.
 - 기존 서버에 워크플로를 추가하려면 워크플로에 사용할 서버를 선택합니다.
 - 또는 새 서버를 만들고 이 서버에 워크플로를 추가할 수도 있습니다. 자세한 내용은 [SFTP, FTPS 또는 FTP 서버 엔드포인트 구성](#) 단원을 참조하십시오.
3. 서버의 세부 정보 페이지에서 추가 세부 정보 섹션까지 아래로 스크롤한 다음 편집을 선택합니다.

Note

기본적으로 서버에는 연결된 워크플로가 없습니다. 추가 세부 정보 섹션을 사용하여 워크플로를 선택한 서버에 연결할 수 있습니다.

4. 추가 세부 정보 편집 페이지의 관리형 워크플로 섹션에서 모든 업로드에서 실행할 워크플로를 선택합니다.

Note

워크플로가 아직 없는 경우 새 워크플로 생성을 선택하여 워크플로를 생성합니다.

- a. 사용할 워크플로 ID를 선택합니다.

- b. 실행 역할을 선택합니다. 이 역할은 워크플로의 단계를 실행할 때 Transfer Family가 맡는 역할입니다. 자세한 내용은 [IAM 워크플로 정책](#)를 참조하세요. 저장(Save)을 선택합니다.

Note

워크플로를 더 이상 서버와 연결하지 않으려면 연결을 제거하면 됩니다. 자세한 내용은 [Transfer Family 서버에서 워크플로 제거](#)를 참조하세요.

워크플로를 실행하려면

워크플로를 실행하려면 관련 워크플로로 구성된 Transfer Family 서버에 파일을 업로드합니다.

Note

서버에서 워크플로를 제거하고 새 워크플로로 바꾸거나 워크플로의 실행 역할에 영향을 미치는 서버 구성을 업데이트할 때마다 새 워크플로를 실행하기 전에 약 10분을 기다려야 합니다. Transfer Family 서버는 워크플로 세부 정보를 캐시하며 서버가 캐시를 새로 고치는 데 10분이 걸립니다.

또한 활성 SFTP 세션에서 로그아웃한 다음 10분 대기 기간 후에 다시 로그인하여 변경 사항을 확인해야 합니다.

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 /DOC-EXAMPLE-BUCKET/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

파일이 업로드되고 나면 파일에 정의된 작업이 수행됩니다. 예를 들어 워크플로에 복사 단계가 포함된 경우 해당 단계에서 정의한 위치에 파일이 복사됩니다. Amazon CloudWatch Logs를 사용하여 실행한 단계와 실행 상태를 추적할 수 있습니다.

워크플로 세부 정보 보기

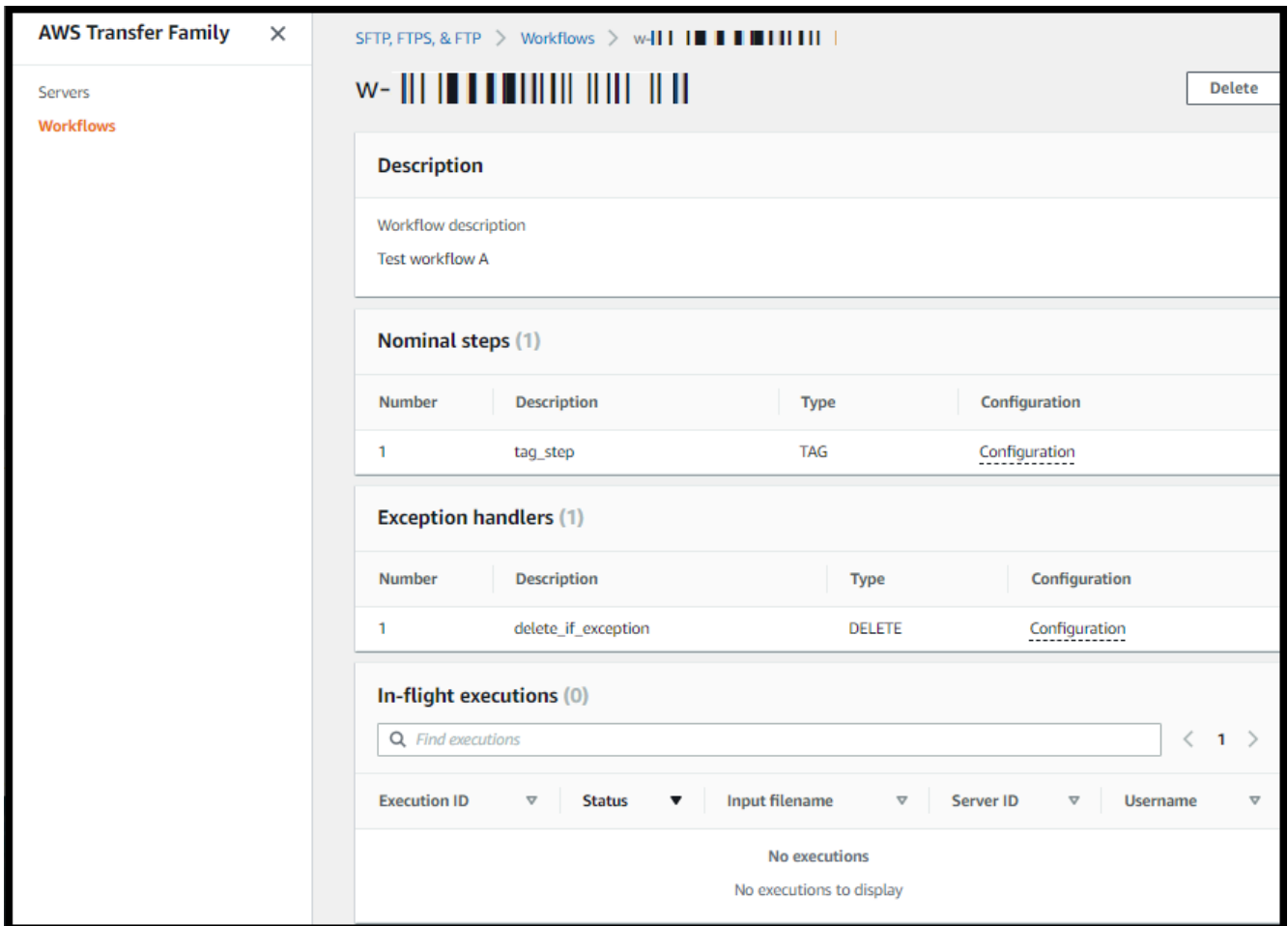
이전에 만든 워크플로 또는 워크플로 실행에 대한 세부 정보를 볼 수 있습니다. 이러한 세부 정보를 보려면 콘솔 또는 AWS Command Line Interface ()를 사용할 수 있습니다AWS CLI.

Console

워크플로 세부 정보 보기

1. 에서 AWS Transfer Family 콘솔을 엽니다<https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 워크플로를 선택합니다.
3. 워크플로 페이지에서 워크플로를 선택합니다.

워크플로 세부 정보 페이지가 열립니다.



CLI

워크플로 세부 정보를 보려면 다음 예제와 같이 `describe-workflow` CLI 명령을 사용합니다. 워크플로 ID `w-1234567890abcdef0`를 사용자의 고유한 값으로 바꿉니다. 자세한 내용은 AWS CLI 명령 참조에서 [describe-workflow](#)를 참조하세요.

```
# 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": "DOC-EXAMPLE-BUCKET",
          "Key": "home/shared_files/"
        }
      }
    },
    "OnException": {}
  }
}

```

워크플로가 AWS CloudFormation 스택의 일부로 생성된 경우 AWS CloudFormation 콘솔(<https://console.aws.amazon.com/cloudformation>)을 사용하여 워크플로를 관리할 수 있습니다.

Transfer Family > Workflows > workflow-32096-20743

Workflow Details Delete

Info This workflow belongs to the AWS CloudFormation stack **WorkflowStack**. [Manage this stack](#) on the CloudFormation console.

Description

Workflow description

-

Nominal steps (1) [Info](#)

Number	Description	Type	Configuration
1	tagFileForArchive	TAG	Details

Exception handlers (0) [Info](#)

Number	Description	Type	Configuration

사전 정의된 단계 사용

워크플로를 만들 때 이 항목에 설명된 다음과 같은 사전 정의된 단계 중 하나를 추가하도록 선택할 수 있습니다. 또한 사용자 지정 파일 처리 단계 추가를 선택할 수도 있습니다. 자세한 내용은 [the section called “사용자 지정 파일 처리 단계 사용”](#)를 참조하세요.

주제

- [파일 복사](#)
- [파일 복호화](#)
- [파일 태그 지정](#)
- [파일 삭제](#)
- [워크플로에 명명된 변수](#)
- [태그 및 삭제 워크플로 예시](#)

파일 복사

파일 복사 단계는 업로드된 파일의 사본을 새 Amazon S3 위치에 생성합니다. 현재는 Amazon S3에서만 파일 복사 단계를 사용할 수 있습니다.

다음 파일 복사 단계는 file-test 대상 버킷의 test 폴더에 파일을 복사합니다.

파일 복사 단계가 워크플로의 첫 단계가 아닌 경우 파일 위치를 지정할 수 있습니다. 파일 위치를 지정하면 이전 단계에서 사용한 파일 또는 업로드된 원본 파일을 복사할 수 있습니다. 이 기능을 사용하면 파일 보관 및 기록 보존을 위해 원본 파일을 그대로 유지하면서 원본 파일의 사본을 여러 개 만들 수 있습니다. 예는 [태그 및 삭제 워크플로 예시](#)를 참조하세요.

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

버킷 및 키 세부 정보 제공

파일 복사 단계의 대상 버킷 이름과 키를 제공해야 합니다. 키는 경로 이름 또는 파일 이름일 수 있습니다. 키를 경로 이름으로 취급할지 파일 이름으로 처리할지는 키 끝에 슬래시(/) 문자를 사용하는지 여부에 따라 결정됩니다.

마지막 문자가 /인 경우 파일은 폴더에 복사되며 이름은 변경되지 않습니다. 최종 문자가 영숫자인 경우 업로드한 파일의 이름이 키 값으로 바뀝니다. 이 경우 해당 이름의 파일이 이미 있는 경우 기존 항목 덮어쓰기 필드의 설정에 따라 동작이 달라집니다.

- 기존 파일 덮어쓰기를 선택하면 기존 파일이 처리 중인 파일로 대체됩니다.
- 기존 항목 덮어쓰기를 선택하지 않은 경우 아무 일도 일어나지 않고 워크플로 처리가 중지됩니다.

i Tip

동일한 파일 경로에서 동시 쓰기를 실행하면 파일을 덮어쓸 때 예상치 못한 동작이 발생할 수 있습니다.

예를 들어 키 값이 test/인 경우 업로드한 파일이 test 폴더에 복사됩니다. 키 값이 test/today인 경우(및 기존 파일 덮어쓰기가 선택된 경우) 업로드하는 모든 파일이 test 폴더에 today(으)로 이름이 지정된 파일에 복사되고 이후의 각 파일은 이전 파일을 덮어씁니다.

i Note

Amazon S3는 버킷과 객체를 지원하며 계층 구조가 없습니다. 하지만 객체 키 이름에 접두사와 구분 기호를 사용하여 계층 구조를 나타내고 폴더와 비슷한 방식으로 데이터를 구성할 수 있습니다.

파일 복사 단계에서 이름이 지정된 변수를 사용하세요.

파일 복사 단계에서 변수를 사용하여 파일을 사용자별 폴더에 동적으로 복사할 수 있습니다. 현재는 `${transfer:UserName}` 또는 `${transfer:UploadDate}`를 변수로 사용하여 파일을 업로드하는 특정 사용자의 대상 위치 또는 현재 날짜를 기준으로 파일을 복사할 수 있습니다.

다음 예에서는 사용자가 파일을 richard-roe 업로드하면 파일이 file-test2/richard-roe/processed/ 폴더에 복사됩니다. 사용자가 mary-major 파일을 업로드하면 파일이 file-test2/mary-major/processed/ 폴더에 복사됩니다.

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

file-test2 ▼

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

마찬가지로 `${transfer:UploadDate}`를 변수로 사용하여 현재 날짜의 이름이 지정된 대상 위치에 파일을 복사할 수 있습니다. 다음 예에서 2022년 2월 1일에 대상을 `${transfer:UploadDate}/processed`로 설정하면 업로드된 파일이 `file-test2/2022-02-01/processed/` 폴더에 복사됩니다.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

file-test2

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

이 두 변수를 함께 사용하여 기능을 조합하여 사용할 수도 있습니다. 예:

- 대상 키 접두사를 **folder/\${transfer:UserName}/\${transfer:UploadDate}/(으)**로 설정하면 중첩된 폴더가 생성됩니다. 예: folder/marymajor/2023-01-05/.
- 대상 키 접두사를 **folder/\${transfer:UserName}-\${transfer:UploadDate}/(으)**로 설정하여 두 변수를 연결할 수 있습니다. 예: folder/marymajor-2023-01-05/.

IAM 복사 단계에 대한 권한

복사 단계를 성공적으로 수행하려면 워크플로의 실행 역할에 다음 권한이 포함되어 있어야 합니다.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::destination-bucket-name"
  ]
}
```

```

    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::destination-bucket-name/*"
    }
  ]
}

```

Note

이 `s3:ListBucket` 권한은 기존 항목 덮어쓰기를 선택하지 않은 경우에만 필요합니다. 이 권한은 버킷을 검사하여 같은 이름의 파일이 이미 존재하는지 확인합니다. 기존 파일 덮어쓰기를 선택한 경우 워크플로에서 파일을 확인할 필요 없이 그냥 쓰기만 하면 됩니다.

Amazon S3 파일에 태그가 있는 경우 IAM 정책에 하나 또는 두 개의 권한을 추가해야 합니다.

- 버전이 지정되지 않은 Amazon S3 파일에 `s3:GetObjectTagging`을 추가합니다.
- 버전이 지정된 Amazon S3 파일에 `s3:GetObjectVersionTagging`을 추가합니다.

파일 복호화

AWS 스토리지 블로그에는 [PGP 및 를 사용하여 파일을 암호화 및 복호화하고 파일을 암호화 및 복호화 AWS Transfer Family](#)하는 방법을 설명하는 게시물이 있습니다.

워크플로에서 PGP복호화 사용

Transfer Family에는 Pretty Good Privacy(PGP) 복호화에 대한 지원이 내장되어 있습니다. SFTP, FTPS또는 를 통해 Amazon Simple Storage Service(Amazon S3) 또는 Amazon Elastic File System(Amazon)FTP에 업로드된 파일에 PGP복호화를 사용할 수 있습니다EFS.

PGP 복호화를 사용하려면 파일 복호화에 사용할 PGP 프라이빗 키를 생성하고 저장해야 합니다. 그런 다음 사용자는 Transfer Family 서버에 파일을 업로드하기 전에 해당 PGP 암호화 키를 사용하여 파일을 암호화할 수 있습니다. 암호화된 파일을 받은 후 워크플로에서 해당 파일을 복호화할 수 있습니다. 자세한 자습서는 [파일 복호화를 위한 관리형 워크플로 설정](#)를 참조하세요.

워크플로에서 PGP복호화를 사용하려면

1. 워크플로를 호스팅할 Transfer Family 서버를 식별하거나 새 서버를 생성합니다. PGP 키를 올바른 보안 암호 이름으로 에 저장하려면 먼저 서버 ID AWS Secrets Manager 가 있어야 합니다.
2. PGP 키를 필요한 보안 암호 이름으로 AWS Secrets Manager 에 저장합니다. 세부 정보는 [PGP 키 관리](#)를 참조하세요. 워크플로는 Secrets Manager의 보안 암호 이름을 기반으로 복호화에 사용할 올바른 PGP 키를 자동으로 찾을 수 있습니다.

Note

Secrets Manager에 암호를 저장하면 AWS 계정 에 요금이 발생합니다. 요금에 대한 자세한 내용은 [AWS Secrets Manager 요금](#)을 참조하세요.

3. PGP 키 페어를 사용하여 파일을 암호화합니다. (지원되는 클라이언트 목록은 [지원되는 PGP 클라이언트](#)를 참조하세요.) 명령줄을 사용하는 경우 다음 명령을 실행하세요. 이 명령을 사용하려면 PGP 키 페어 `username@example.com`를 생성하는 데 사용한 이메일 주소로 를 바꿉니다. `testfile.txt`를 암호화할 파일의 이름으로 바꿉니다.

```
gpg -e -r username@example.com testfile.txt
```

4. 암호화된 파일을 Transfer Family 서버에 업로드합니다.
5. 워크플로에서 복호화 단계를 구성합니다. 자세한 내용은 [복호화 단계 추가](#)를 참조하세요.

복호화 단계 추가

복호화 단계는 워크플로의 EFS 일부로 Amazon S3 또는 Amazon에 업로드된 암호화된 파일을 복호화합니다. 복호화 구성에 대한 자세한 내용은 [워크플로에서 PGP복호화 사용](#)을 참조하세요.

워크플로의 복호화 단계를 생성할 때는 복호화한 파일의 대상을 지정해야 합니다. 대상 위치에 파일이 이미 있는 경우 기존 파일을 덮어쓸지 여부도 선택해야 합니다. Amazon Logs를 사용하여 복호화 워크플로 결과를 모니터링하고 각 파일에 대한 감사 CloudWatch 로그를 실시간으로 가져올 수 있습니다.

해당 단계에서 파일 복호화 타입을 선택하면 파라미터 구성 페이지가 나타납니다. PGP 복호화 파라미터 구성 섹션의 값을 입력합니다.

사용 가능한 옵션은 다음과 같습니다.

- 단계 이름 - 단계를 설명하는 이름을 입력합니다.

- 파일 위치 - 파일 위치를 지정하여 이전 단계에서 사용한 파일 또는 업로드된 원본 파일을 복호화할 수 있습니다.

 Note

이 단계가 워크플로의 첫 번째 단계인 경우에는 이 파라미터를 사용할 수 없습니다.

- 복호화된 파일의 대상 - 복호화된 EFS 파일의 대상으로 Amazon S3 버킷 또는 Amazon 파일 시스템을 선택합니다.
- Amazon S3를 선택하는 경우 대상 버킷 이름과 대상 키 접두사를 제공해야 합니다. 사용자 이름을 기준으로 대상 키 접두사를 파라미터화하려면 대상 키 접두사에 **`${transfer:UserName}`**를 입력합니다. 마찬가지로 업로드 날짜별로 대상 키 접두사를 파라미터화하려면 대상 키 접두사에 **`${Transfer:UploadDate}`**를 입력합니다.
- Amazon 을 선택한 경우 대상 파일 시스템과 경로를 제공해야 EFS합니다.

 Note

여기서 선택하는 스토리지 옵션은 이 워크플로가 연결된 Transfer Family 서버에서 사용하는 스토리지 시스템과 일치해야 합니다. 그렇지 않으면 이 워크플로를 실행하려고 시도하는 동안 오류가 발생합니다.

- 기존 파일 덮어쓰기 - 파일을 업로드했는데 같은 파일 이름을 가진 파일이 대상에 이미 있는 경우 동작은 이 파라미터의 설정에 따라 달라집니다.
- 기존 파일 덮어쓰기를 선택하면 기존 파일이 처리 중인 파일로 대체됩니다.
- 기존 항목 덮어쓰기를 선택하지 않은 경우 아무 일도 일어나지 않고 워크플로 처리가 중지됩니다.

 Tip

동일한 파일 경로에서 동시 쓰기를 실행하면 파일을 덮어쓸 때 예상치 못한 동작이 발생할 수 있습니다.

다음 스크린샷은 파일 복호화 단계에서 선택할 수 있는 옵션의 예를 보여줍니다.

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

decrypt step example

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

example-bucket

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.

`${transfer:UserName}`

☐ Overwrite existing
Overwrite if a file with the same file name already exists at the destination.

IAM 복호화 단계에 대한 권한

복호화 단계를 성공적으로 수행하려면 워크플로의 실행 역할에 다음 권한이 포함되어 있어야 합니다.

```
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::destination-bucket-name"
    ],
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
},
{
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue",
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
* "
}
```

Note

이 s3:ListBucket 권한은 기존 항목 덮어쓰기를 선택하지 않은 경우에만 필요합니다. 이 권한은 버킷을 검사하여 같은 이름의 파일이 이미 존재하는지 확인합니다. 기존 파일 덮어쓰기를 선택한 경우 워크플로에서 파일을 확인할 필요 없이 그냥 쓰기만 하면 됩니다.

Amazon S3 파일에 태그가 있는 경우 IAM 정책에 하나 또는 두 개의 권한을 추가해야 합니다.

- 버전이 지정되지 않은 Amazon S3 파일에 s3:GetObjectTagging을 추가합니다.
- 버전이 지정된 Amazon S3 파일에 s3:GetObjectVersionTagging을 추가합니다.

파일 태그 지정

추가 다운스트림 처리를 위해 인입 파일에 태그를 지정하려면 태그 단계를 사용하세요. 인입 파일에 할당하려는 태그의 값을 입력합니다. 현재 태그 작업은 Transfer Family 서버 스토리지로 Amazon S3를 사용하는 경우에만 지원됩니다.

다음 태그 단계 예에서는 각각 `scan_outcome` 및 `clean`를 태그 키와 값으로 할당합니다.

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

태그 단계를 성공적으로 수행하려면 워크플로의 실행 역할에 다음 권한이 포함되어 있어야 합니다.

```
{
  "Sid": "Tag",
  "Effect": "Allow",
  "Action": [
    "s3:PutObjectTagging",
    "s3:PutObjectVersionTagging"
  ],
  "Resource": [
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
  ]
}
```

Note

워크플로에 복사 또는 복호화 단계 전에 실행되는 태그 단계가 포함된 경우 IAM 정책에 하나 또는 두 개의 권한을 추가해야 합니다.

- 버전이 지정되지 않은 Amazon S3 파일에 `s3:GetObjectTagging`을 추가합니다.
- 버전이 지정된 Amazon S3 파일에 `s3:GetObjectVersionTagging`을 추가합니다.

파일 삭제

이전 워크플로 단계에서 처리된 파일을 삭제하거나 원래 업로드된 파일을 삭제하려면 파일 삭제 단계를 사용하세요.

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

삭제 단계를 성공적으로 수행하려면 워크플로의 실행 역할에 다음 권한이 포함되어 있어야 합니다.

```
{
    "Sid": "Delete",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
* "
}
```

워크플로에 명명된 변수

복사 및 복호화 단계의 경우 변수를 사용하여 작업을 동적으로 수행할 수 있습니다. 현재는 다음과 같은 명명된 변수를 AWS Transfer Family 지원합니다.

- 업로드하는 사용자를 기준으로 `${transfer:UserName}`을 사용하여 대상으로 파일을 복사하거나 암호를 해독합니다.
- 현재 날짜를 기준으로 `${transfer:UploadDate}`를 사용하여 대상으로 파일을 복사하거나 암호를 해독합니다.

태그 및 삭제 워크플로 예시

다음 예는 데이터 분석 플랫폼과 같은 다운스트림 애플리케이션에서 처리해야 하는 수신 파일에 태그를 지정하는 워크플로를 보여줍니다. 인입 파일에 태그를 지정 후 워크플로는 원래 업로드된 파일을 삭제하여 스토리지 비용을 절약합니다.

Console

태그 및 이동 워크플로 예

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 워크플로를 선택합니다.
3. 워크플로 페이지에서 워크플로 생성을 선택합니다.
4. 워크플로 생성 페이지에서 설명을 입력합니다. 이 설명은 워크플로 페이지에 표시됩니다.
5. 첫 번째 단계(복사)를 추가합니다.
 - a. 공칭 단계 섹션에서 단계 추가를 선택합니다.
 - b. 파일 복사를 선택한 후 다음을 선택합니다.
 - c. 단계 이름을 입력한 다음 대상 버킷과 키 접두사를 선택합니다.

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. 다음을 선택한 다음 해당 단계에 대한 세부 정보를 검토합니다.
 - e. 단계 생성을 선택하여 단계를 추가하고 계속합니다.
6. 두 번째 단계(태그)를 추가합니다.
- a. 공칭 단계 섹션에서 단계 추가를 선택합니다.
 - b. 파일 태그 지정을 선택한 후 다음을 선택합니다.
 - c. 단계 이름을 입력합니다.
 - d. 파일 위치의 경우 이전 단계에서 만든 파일에 태그 지정을 선택합니다.
 - e. 키와 값을 입력합니다.

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. 다음을 선택한 다음 해당 단계에 대한 세부 정보를 검토합니다.
 - g. 단계 생성을 선택하여 단계를 추가하고 계속합니다.
7. 세 번째 단계 추가(삭제).
- a. 공칭 단계 섹션에서 단계 추가를 선택합니다.
 - b. 파일 삭제를 선택하고 다음을 선택합니다.

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. 단계 이름을 입력합니다.

- d. 파일 위치에서 원본 소스 파일 삭제를 선택합니다.
 - e. 다음을 선택한 다음 해당 단계에 대한 세부 정보를 검토합니다.
 - f. 단계 생성을 선택하여 단계를 추가하고 계속합니다.
8. 워크플로 구성을 검토한 다음 워크플로 생성을 선택합니다.

CLI

태그 및 이동 워크플로 예

1. 다음 코드를 파일에 저장합니다. 예: tagAndMoveWorkflow.json. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "DOC-EXAMPLE-BUCKET",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```

```

        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
]

```

첫 번째 단계에서는 업로드된 파일을 새 Amazon S3 위치에 복사합니다. 두 번째 단계에서는 새 위치에 복사된 파일(previous.file)에 태그(카-값 쌍)를 추가합니다. 마지막으로 세 번째 단계에서는 원본 파일(original.file)을 삭제합니다.

2. 저장된 파일에서 워크플로를 생성합니다. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```

aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID

```

예:

```

aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1

```

Note

파일을 사용하여 파라미터를 로드하는 방법에 대한 자세한 내용은 [파일에서 파라미터를 로드하는 방법](#)을 참조하세요.

3. 기존 서버를 업데이트합니다.

Note

이 단계에서는 이미 Transfer Family 서버가 있고 이 서버에 워크플로를 연결하려는 것으로 가정합니다. 그렇지 않은 경우 [SFTP, FTPS 또는 FTP 서버 엔드포인트 구성](#)을 참조하세요. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```

aws transfer update-server --server-id server-ID --region region-ID
--workflow-details '{"OnUpload": [{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'

```

예:

```
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"}]}'
```

사용자 지정 파일 처리 단계 사용

사용자 지정 파일 처리 단계를 사용하면 AWS Lambda를 사용하여 Bring Your Own 파일 처리 로직을 사용할 수 있습니다. 파일이 도착하면 Transfer Family 서버는 파일 암호화, 멀웨어 검사 또는 잘못된 파일 타입 검사와 같은 사용자 지정 파일 처리 로직이 포함된 Lambda 함수를 간접적으로 호출합니다. 다음 예시에서는 대상 AWS Lambda 함수를 사용하여 이전 단계의 출력 파일을 처리합니다.

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

Lambda 함수의 예는 [사용자 지정 워크플로 단계를 위한 Lambda 함수 예](#)를 참조하세요. 예를 들어 이벤트(Lambda로 전달된 파일의 위치 포함)는 [파일 업로드 AWS Lambda 시로 전송된 이벤트 예](#)를 참조하세요.

사용자 지정 워크플로 단계를 사용하면 [SendWorkflowStepState](#) API 작업을 호출하도록 Lambda 함수를 구성해야 합니다. 는 단계가 성공 또는 실패 상태로 완료되었음을 워크플로 실행에 [SendWorkflowStepState](#) 알립니다. [SendWorkflowStepState](#) API 작업 상태는 Lambda 함수의 결과를 기반으로 예외 핸들러 단계 또는 선형 시퀀스의 명목 단계를 호출합니다.

Lambda 함수가 실패하거나 시간이 초과되면 단계가 실패하고 CloudWatch 로그StepErrored에 이 표시됩니다. Lambda 함수가 공칭 단계의 일부이고 함수가 Status="FAILURE"로 [SendWorkflowStepState](#)에 응답하거나 제한 시간이 초과되면 흐름은 예외 처리 단계로 계속됩니다. 이 경우 워크플로는 나머지(있는 경우) 공칭 단계를 계속 실행하지 않습니다. 자세한 내용은 [워크플로의 예외 처리](#)를 참조하세요.

[SendWorkflowStepState](#) API 작업을 호출할 때 다음 파라미터를 전송해야 합니다.

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Lambda 함수가 실행될 때 전달되는 입력 이벤트에서 ExecutionId, Token, 및 WorkflowId를 추출할 수 있습니다(예는 다음 섹션에 표시됨). 이때 Status 값은 SUCCESS 또는 FAILURE가 될 수 있습니다.

Lambda 함수에서 [SendWorkflowStepState](#) API 작업을 호출하려면 관리형 워크플로가 AWS SDK 도입된 후 게시된 버전의 를 사용해야 합니다. [???](#)

여러 Lambda 함수를 연속적으로 사용

여러 사용자 지정 단계를 차례로 사용하는 경우 파일 위치 옵션은 단일 사용자 지정 단계만 사용하는 경우와 다르게 작동합니다. Transfer Family는 Lambda 처리 파일을 다음 단계의 입력으로 사용하기 위해 다시 전달하는 것을 지원하지 않습니다. 따라서 `previous.file` 옵션을 사용하도록 구성된 사용자 지정 단계가 여러 개 있는 경우 모두 동일한 파일 위치(첫 번째 사용자 지정 단계의 입력 파일 위치)를 사용합니다.

Note

사용자 지정 단계 이후에 사전 정의된 단계(태그 지정, 복사, 복호화 또는 삭제)가 있는 경우에도 `previous.file` 설정이 다르게 작동합니다. 사전 정의된 단계가 `previous.file` 설정을

사용하도록 구성된 경우 사전 정의된 단계는 사용자 정의 단계에서 사용한 것과 동일한 입력 파일을 사용합니다. 사용자 정의 단계에서 처리된 파일은 사전 정의된 단계로 전달되지 않습니다.

사용자 정의 처리 후 파일에 액세스

Amazon S3를 스토리지로 사용하고 있고 워크플로에 원래 업로드된 파일에서 작업을 수행하는 사용자 지정 단계가 포함되어 있는 경우, 후속 단계에서 처리된 파일에 액세스할 수 없습니다. 즉, 사용자 지정 단계 이후의 모든 단계는 사용자 지정 단계 출력의 업데이트된 파일을 참조할 수 없습니다.

예를 들어 워크플로에 다음과 같은 세 단계가 있다고 가정하겠습니다.

- 1단계 — example-file.txt라는 이름의 파일을 업로드합니다.
- 2단계 — 어떤 식으로든 example-file.txt를 변경하는 Lambda 함수를 간접적으로 호출합니다.
- 3단계 — example-file.txt의 업데이트된 버전에서 추가 처리를 시도합니다.

3단계에 대한 sourceFileLocation을 `${original.file}`로 구성한 경우 3단계에서는 1단계에서 서버가 스토리지에 파일을 업로드한 시점의 원래 파일 위치를 사용합니다. 3단계에서 `${previous.file}`을 사용하는 경우 3단계에서는 2단계에서 입력으로 사용한 파일 위치를 다시 사용합니다.

따라서 3단계에서 오류가 발생합니다. 예를 들어 3단계에서 업데이트된 example-file.txt를 복사하려고 하면 다음과 같은 오류 메시지가 나타납니다.

```
{
  "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"
  },
}
```

이 오류는 사용자 지정 단계가 의 엔터티 태그(ETag)를 수정example-file.txt하여 원본 파일과 일치하지 않도록 하기 때문에 발생합니다.

Note

Amazon은 엔터티 태그를 사용하여 파일을 식별하지 않기 EFS 때문에 Amazon을 사용하는 경우에는 이 동작이 발생하지 EFS 않습니다.

파일 업로드 AWS Lambda 시 로 전송된 이벤트 예

다음 예제에서는 파일 업로드가 완료될 AWS Lambda 때 로 전송되는 이벤트를 보여줍니다. 한 예로, 도메인이 Amazon S3으로 구성된 Transfer Family 서버를 사용합니다. 다른 예제에서는 도메인이 Amazon 를 사용하는 Transfer Family 서버를 사용합니다EFS.

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": "DOC-EXAMPLE-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"
}
}

```

사용자 지정 워크플로 단계를 위한 Lambda 함수 예

다음 Lambda 함수는 실행 상태에 대한 정보를 추출한 다음 [SendWorkflowStepState](#) API 작업을 호출하여 또는 단계의 워크플로로 상태를 반환합니다. SUCCESS/FAILURE. 함수가 SendWorkflowStepState API 작업을 호출하기 전에 워크플로 로직을 기반으로 작업을 수행하도록 Lambda를 구성할 수 있습니다.

```

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 사용자 지정 단계에 대한 권한

Lambda를 직접적으로 호출하는 단계가 성공하도록 허용하려면 워크플로의 실행 역할에 다음 권한이 포함되어 있어야 합니다.

```
{
  "Sid": "Custom",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:region:account-id:function:function-name"
  ]
}
```

IAM 워크플로 정책

서버에 워크플로를 추가할 때는 실행 역할을 선택해야 합니다. 서버는 워크플로를 실행할 때 이 역할을 사용합니다. 역할에 적절한 권한이 없는 경우 워크플로를 실행할 AWS Transfer Family 수 없습니다.

이 섹션에서는 워크플로를 실행하는 데 사용할 수 있는 AWS Identity and Access Management (IAM) 권한 집합에 대해 설명합니다. 다른 예는 이 주제 후반부에서 설명합니다.

Note

Amazon S3 파일에 태그가 있는 경우 IAM 정책에 하나 또는 두 개의 권한을 추가해야 합니다.

- 버전이 지정되지 않은 Amazon S3 파일에 `s3:GetObjectTagging`을 추가합니다.
- 버전이 지정된 Amazon S3 파일에 `s3:GetObjectVersionTagging`을 추가합니다.

워크플로에 대한 실행 역할을 만들려면

1. 새 IAM 역할을 생성하고 AWS 관리형 정책을 AWSTransferFullAccess 역할에 추가합니다. 새 IAM 역할 생성에 대한 자세한 내용은 섹션을 참조하세요 [the section called “IAM 역할 및 정책 생성”](#).
2. 다음 권한이 있는 다른 정책을 생성하여 이를 역할에 연결합니다. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConsoleAccess",
      "Effect": "Allow",
      "Action": "s3:GetBucketLocation",
      "Resource": "*"
    },
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    },
    {
      "Sid": "AllObjectActions",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ]
    },
    {
      "Sid": "GetObjectVersion",
      "Effect": "Allow",
      "Action": "s3:GetObjectVersion",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ]
    }
  ]
}
```

```

        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:region:account-id:function:function-name"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ]
    }
]
}

```

3. 이 역할을 저장하고 서버에 워크플로를 추가할 때 실행 역할로 지정하세요.

Note

IAM 역할을 구성할 때 워크플로에 대해 가능한 한 리소스에 대한 액세스를 제한하도록 AWS 권장합니다.

워크플로 신뢰 관계

워크플로 실행 역할에는 `transfer.amazonaws.com`과의 신뢰 관계도 필요합니다. AWS Transfer Family에 대한 신뢰 관계를 설정하려면 [신뢰 관계를 구축하기 위해](#)를 참조하세요.

신뢰 관계를 구축하는 동시에 혼란스러운 대리인 문제를 피하도록 조치를 취할 수도 있습니다. 이 문제에 대한 설명과 이를 방지하는 방법의 예는 [the section called “교차 서비스 혼동된 대리인 방지”](#)을 참조하세요.

실행 역할 예시: 복호화, 복사, 태그 지정

태그 지정, 복사 및 복호화 단계를 포함하는 워크플로가 있는 경우 다음 IAM 정책을 사용할 수 있습니다. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyRead",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Sid": "CopyWrite",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:::destination-bucket-name/*"
    },
    {
      "Sid": "CopyList",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": [
        "arn:aws:s3:::source-bucket-name",
        "arn:aws:s3:::destination-bucket-name"
      ]
    },
    {
      "Sid": "Tag",
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
    }
  ]
}
```



```

        "Resource": "arn:aws:s3:::destination-bucket-name/*",
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Archive": "yes"
            }
        }
    },
    {
        "Sid": "ListBucket",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::destination-bucket-name"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObjectVersion",
            "s3:DeleteObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::destination-bucket-name/*"
    },
    {
        "Sid": "Decrypt",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
*"
    }
]
}

```

실행 역할 예시: 함수 실행 및 삭제

이 예제에서는 AWS Lambda 함수를 호출하는 워크플로가 있습니다. 워크플로가 업로드된 파일을 삭제하고 이전 단계에서 실패한 워크플로 실행에 대해 조치를 취할 예외 핸들러 단계가 있는 경우 다음 IAM 정책을 사용합니다. 각 *user input placeholder*를 사용자의 정보로 바꿉니다.

```
{
  "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:region:account-id:function:function-name"
      ]
    }
  ]
}
```

워크플로의 예외 처리

워크플로 실행 중에 오류가 발생하는 경우 지정한 예외 처리 단계가 실행됩니다. 워크플로의 공칭 단계를 지정하는 것과 같은 방식으로 워크플로의 오류 처리 단계를 지정합니다. 예를 들어 들어오는 파일의 유효성을 검사하기 위해 공칭의 단계로 사용자 지정 처리를 구성했다고 가정해 보겠습니다. 파일 검증이 실패하는 경우 예외 처리 단계를 통해 관리자에게 이메일을 보낼 수 있습니다.

다음 예 워크플로에는 두 단계가 포함되어 있습니다.

- 업로드된 파일의 CSV 형식이 맞는지 확인하는 하나의 명목 단계

- 업로드된 파일의 CSV 형식이 아니고 명목 단계가 실패할 경우 이메일을 보내는 예외 처리 단계

예외 처리 단계를 시작하려면 명목 단계의 AWS Lambda 함수가 `로 응답해야 합니다` `Status="FAILURE"`. 워크플로에서 오류를 처리하는 방법에 대한 자세한 내용은 [the section called “사용자 지정 파일 처리 단계 사용”](#)를 참조하세요.

w-1234567890abcdef0

Delete

Description

Workflow description

Check for CSV files

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

워크플로 실행 모니터링

Amazon은 에서 실행하는 AWS 리소스와 애플리케이션을 AWS 클라우드 실시간으로 CloudWatch 모니터링합니다. Amazon CloudWatch 을 사용하여 워크플로에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다. Amazon 를 사용하여 워크플로 지표와 통합 로그를 볼 수 있습니다 CloudWatch.

CloudWatch 워크플로에 대한 로깅

CloudWatch 는 워크플로 진행 상황 및 결과에 대한 통합 감사 및 로깅을 제공합니다.

워크플로에 대한 Amazon CloudWatch 로그 보기

- 에서 Amazon CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
- 왼쪽 탐색 창에서 로그를 선택한 다음, 로그 그룹을 선택합니다.
- 로그 그룹 페이지의 탐색 모음에서 AWS Transfer Family 서버에 적합한 리전을 선택합니다.
- 서버에 해당하는 로그 그룹을 선택합니다.

예를 들어 서버 ID가 s-1234567890abcdef0인 경우 로그 그룹은 /aws/transfer/s-1234567890abcdef0입니다.

5. 서버의 로그 그룹 세부 정보 페이지에는 가장 최근의 로그 스트림이 표시됩니다. 탐색 중인 사용자에게 대한 로그 스트림은 두 가지입니다.

- 각 Secure Shell(SSH) 파일 전송 프로토콜(SFTP) 세션당 1개.
- 서버에서 실행 중인 워크플로의 로그 스트림 워크플로의 로그 스트림 형식은 *username.workflowID.uniqueStreamSuffix*입니다.

예를 들어 사용자가 mary-major이면 다음과 같은 로그 스트림이 있습니다.

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

이 예에 나열된 16자리 영숫자 식별자는 가상의 식별자입니다. Amazon에 표시되는 값은 CloudWatch 다릅니다.

mary-major-usa-east.1234567890abcdef0의 로그 이벤트 페이지에는 각 사용자 세션의 세부 정보가 표시되고 mary.w-abcdef01234567890.021345abcdef6789 로그 스트림에는 워크플로에 대한 세부 정보가 포함됩니다.

다음은 복사 단계가 포함된 워크플로(w-abcdef01234567890)를 기반으로 하는 mary.w-abcdef01234567890.021345abcdef6789의 샘플 로그 스트림입니다.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "DOC-EXAMPLE-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": "DOC-EXAMPLE-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 워크플로 지표

AWS Transfer Family 는 워크플로에 대한 여러 지표를 제공합니다. 이전 1분 간 시작, 성공적으로 완료, 및 실패한 워크플로 실행 수에 대한 지표를 볼 수 있습니다. Transfer Family에 대한 모든 CloudWatch 지표는 에 설명되어 있습니다 [Transfer Family에 대한 CloudWatch 지표 사용](#).

템플릿에서 워크플로 생성

템플릿에서 워크플로와 서버를 생성하는 AWS CloudFormation 스택을 배포할 수 있습니다. 이 절차에는 워크플로를 빠르게 배포하는 데 사용할 수 있는 예가 포함되어 있습니다.

AWS Transfer Family 워크플로 및 서버를 생성하는 AWS CloudFormation 스택을 생성하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 다음 코드를 파일에 저장합니다.

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. 다음 항목을 실제 값으로 대체합니다.

- Replace *workflow-execution-role-arn* 실제 워크플로 실행 역할ARN의 경우를 사용합니다. 예제: `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
- Lambda 함수의 ARN을 `arn:aws:lambda:region:account-id:function:function-name`로 바꿉니다. 예: `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.

4. AWS CloudFormation 사용 설명서의 AWS CloudFormation 스택 템플릿 [선택의 기존 템플릿에서 스택을 배포하기](#) 위한 지침을 따릅니다.

스택이 배포된 후 CloudFormation 콘솔의 출력 탭에서 스택에 대한 세부 정보를 볼 수 있습니다. 템플릿은 서비스 관리 사용자를 사용하는 새 AWS Transfer Family SFTP 서버와 새 워크플로를 생성하고 워크플로를 새 서버와 연결합니다.

Transfer Family 서버에서 워크플로 제거

워크플로를 Transfer Family 서버와 연결했는데 이제 해당 연결을 제거하려는 경우 콘솔을 사용하거나 프로그래밍 방식으로 제거할 수 있습니다.

Console

Transfer Family 서버에서 워크플로 제거

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택합니다.
3. 서버 ID 옆에서 서버 식별자를 선택합니다.
4. 서버의 세부 정보 페이지에서 추가 세부 정보 섹션까지 아래로 스크롤한 다음 편집을 선택합니다.
5. 추가 세부 정보 편집 페이지의 관리형 워크플로 섹션에서 모든 설정에 대한 정보를 지웁니다.
 - 전체 파일 업로드를 위한 워크플로의 워크플로 목록에서 대시(-)를 선택합니다.
 - 아직 지우지 않은 경우 부분 파일 업로드 워크플로의 워크플로 목록에서 대시(-)를 선택합니다.
 - 관리형 워크플로 실행 역할의 역할 목록에서 대시(-)를 선택합니다.

대시가 보이지 않는 경우 각 메뉴의 첫 번째 값이므로 대시가 보일 때까지 위로 스크롤하세요.

결과는 다음과 같아야 합니다.

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

Select a workflow ▼ [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that AWS Transfer Family should run on all files that are only partially uploaded via this server

Select a workflow ▼ [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

- ▼

6. 변경 내용을 저장하려면 아래로 스크롤하여 저장을 선택합니다.

CLI

update-server (또는 의 UpdateServer 경우API) 호출을 사용하고 OnUpload 및 OnPartialUpload 파라미터에 대한 빈 인수를 제공합니다.

에서 다음 명령을 AWS CLI 실행합니다.

```
aws transfer update-server --server-id your-server-id --workflow-details
'{"OnPartialUpload":[],"OnUpload":[]}'
```

*your-server-id*를 서버의 ID로 바꿉니다. 예를 들어, 서버 ID가 s-01234567890abcdef인 경우 명령은 다음과 같습니다.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
'{"OnPartialUpload":[],"OnUpload":[]}'
```

관리형 워크플로 제한 및 제약 조건

제한 사항

현재 다음과 같은 제한 사항이 AWS Transfer Family의 업로드 후 처리 워크플로에 적용됩니다.

- 교차 계정 및 교차 리전 AWS Lambda 함수는 지원되지 않습니다. 그러나 AWS Identity and Access Management (IAM) 정책이 올바르게 구성된 경우 계정 간에 복사할 수 있습니다.

- 모든 워크플로 단계에서 워크플로로 액세스하는 모든 Amazon S3 버킷은 워크플로와 동일한 리전에 있어야 합니다.
- 복호화 단계의 경우 복호화 대상이 리전 및 지원 스토어의 원본과 일치해야 합니다(예를 들어, 해독할 파일이 Amazon S3에 저장되어 있는 경우 지정된 대상도 Amazon S3에 있어야 함).
- 비동기 사용자 지정 단계만 지원됩니다.
- 사용자 지정 단계 제한 시간은 근사값입니다. 즉, 지정된 제한 시간보다 약간 더 오래 걸릴 수 있습니다. 또한 워크플로는 Lambda 함수에 따라 달라집니다. 따라서 실행 중에 함수가 지연되는 경우 워크플로는 지연을 인식하지 못합니다.
- 제한 한도를 초과하는 경우 Transfer Family는 대기열에 워크플로 작업을 추가하지 않습니다.
- 크기가 0인 파일에 대해서는 워크플로가 시작되지 않습니다. 크기가 0보다 큰 파일은 관련 워크플로를 시작합니다.

제한 사항

또한 Transfer Family의 워크플로에는 다음과 같은 기능 제한이 적용됩니다.

- 리전별, 계정별 워크플로 수는 10개로 제한됩니다.
- 사용자 지정 단계의 최대 제한 시간은 30분입니다.
- 워크플로의 최대 단계 수는 8개입니다.
- 워크플로당 최대 태그 수는 50개입니다.
- 복호화 단계가 포함된 최대 동시 실행 수는 워크플로당 250개입니다.
- Transfer Family 서버당 사용자당 최대 3개의 PGP 프라이빗 키를 저장할 수 있습니다.
- 복호화된 파일의 최대 크기는 10GB입니다.
- 버스트 용량이 100이고 리필 비율이 1인 [토큰 버킷](#) 시스템을 사용하여 새 실행률을 제한합니다.
- 서버에서 워크플로를 제거하고 새 워크플로로 바꾸거나 워크플로의 실행 역할에 영향을 미치는 서버 구성을 업데이트할 때마다 새 워크플로를 실행하기 전에 약 10분을 기다려야 합니다. Transfer Family 서버는 워크플로 세부 정보를 캐시하며 서버가 캐시를 새로 고치는 데 10분이 걸립니다.

또한 활성 SFTP 세션에서 로그아웃한 다음 10분 대기 기간 후에 다시 로그인하여 변경 사항을 확인해야 합니다.

서버 관리

이 섹션에서는 서버 목록을 보는 방법, 서버 세부 정보를 보는 방법, 서버 세부 정보를 편집하는 방법, SFTP활성화된 서버의 호스트 키를 변경하는 방법에 대한 정보를 찾을 수 있습니다.

주제

- [서버 목록 보기](#)
- [서버 삭제](#)
- [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#)
- [AS2 서버 세부 정보 보기](#)
- [서버 세부 정보 편집](#)
- [SFTP지원 서버의 호스트 키 관리](#)
- [콘솔 내 사용량 모니터링](#)

서버 목록 보기

AWS Transfer Family 콘솔에서 선택한 AWS 리전에 있는 모든 서버의 목록을 찾을 수 있습니다.

AWS 리전에 있는 서버 목록을 찾으려면

- 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.

현재 AWS 리전에 서버가 하나 이상 있는 경우 콘솔이 열리고 서버 목록이 표시됩니다. 서버 목록이 보이지 않으면, 올바른 AWS 리전에 있는지 확인하세요. 탐색 창에서 서버를 선택할 수도 있습니다.

로그의 세부 정보 보기에 대한 자세한 내용은 [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#)를 참조하세요.

서버 삭제

이 절차에서는 AWS Transfer Family 콘솔 또는 를 사용하여 Transfer Family 서버를 삭제하는 방법을 설명합니다 AWS CLI.

⚠ Important

엔드포인트에 액세스할 수 있도록 설정된 각 프로토콜에 대해 서버를 삭제할 때까지 요금이 청구됩니다.

⚠ Warning

서버를 삭제하면 해당 사용자가 모두 삭제됩니다. 서버를 사용하여 액세스한 버킷의 데이터는 삭제되지 않으며 해당 Amazon S3 버킷에 대한 권한을 가진 AWS 사용자가 계속 액세스할 수 있습니다.

Console

콘솔을 사용하여 서버를 삭제하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택합니다.
3. 삭제할 서버의 확인란을 선택합니다.
4. 작업에 대해 삭제를 선택합니다.
5. 표시되는 확인 대화 상자에서 단어 **delete**를 입력한 다음 삭제를 선택하여 서버 삭제를 확인합니다.

서버 페이지에서 서버가 삭제되며 더 이상 요금이 청구되지 않습니다.

AWS CLI

를 사용하여 서버를 삭제하려면 CLI

1. (선택 사항) 다음 명령을 실행하여 영구적으로 삭제하려는 서버의 세부 정보를 확인합니다.

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

이 `describe-server` 명령은 서버의 모든 세부 정보를 반환합니다.

2. 다음 명령을 실행하여 서버를 삭제합니다.

```
aws transfer delete-server --server-id your-server-id
```

성공하면 명령이 서버를 삭제하고 정보를 반환하지 않습니다.

SFTP, FTPS 및 FTP 서버 세부 정보 보기

개별 AWS Transfer Family 서버의 세부 정보 및 속성 목록을 찾을 수 있습니다. 서버 속성에는 프로토콜, 자격 증명 제공자, 상태, 엔드포인트 타입, 사용자 지정 호스트 이름, 엔드포인트, 사용자, 로깅 역할, 서버 호스트 키 및 태그가 포함됩니다.

서버 세부 정보를 보려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.
3. 서버 ID 옆에서 식별자를 선택하여 다음과 같은 서버 세부 정보 페이지를 표시합니다.

편집을 선택하여 이 페이지에서 서버의 속성을 변경할 수 있습니다. 서버 편집에 대한 자세한 내용은 [서버 세부 정보 편집](#)을 참조하세요. AS2 서버의 세부 정보 페이지는 약간 다릅니다. AS2 서버의 경우 섹션을 참조하세요 [AS2 서버 세부 정보 보기](#).

Protocols Edit Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider Edit Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda

Note

서버 호스트 키 설명 및 가져온 날짜 값은 2022년 9월 기준으로 새로 추가되었습니다. 이러한 값은 다중 호스트 키 기능을 지원하기 위해 도입되었습니다. 이 기능을 사용하려면 여러 호스트 키가 도입되기 전에 사용 중이던 단일 호스트 키를 모두 마이그레이션해야 합니다.

마이그레이션된 서버 호스트 키의 가져온 날짜 값은 서버의 마지막 수정 날짜로 설정됩니다. 즉, 마이그레이션된 호스트 키로 표시되는 날짜는 어떤 식으로든 서버 호스트 키 마이그레이션 전에 서버를 마지막으로 수정한 날짜와 일치합니다.

마이그레이션된 유일한 키는 가장 오래된 또는 유일한 서버 호스트 키입니다. 모든 추가 키에는 가져온 시점의 실제 날짜가 표시됩니다. 또한 마이그레이션된 키에는 마이그레이션된 키임을 쉽게 식별할 수 있는 설명이 있습니다.

마이그레이션은 9월 2일에서 9월 13일 사이에 이루어졌습니다. 이 범위 내의 실제 마이그레이션 날짜는 서버 리전에 따라 다릅니다.

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 -

AS2 서버 세부 정보 보기

개별 AWS Transfer Family 서버의 세부 정보 및 속성 목록을 찾을 수 있습니다. 서버 속성에는 프로토콜, 상태 등이 포함됩니다. AS2 서버의 경우 AS2 비동기 MDN 발신 IP 주소를 볼 수도 있습니다.

Protocols

Edit

Identity provider

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

AS2 Auth

Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

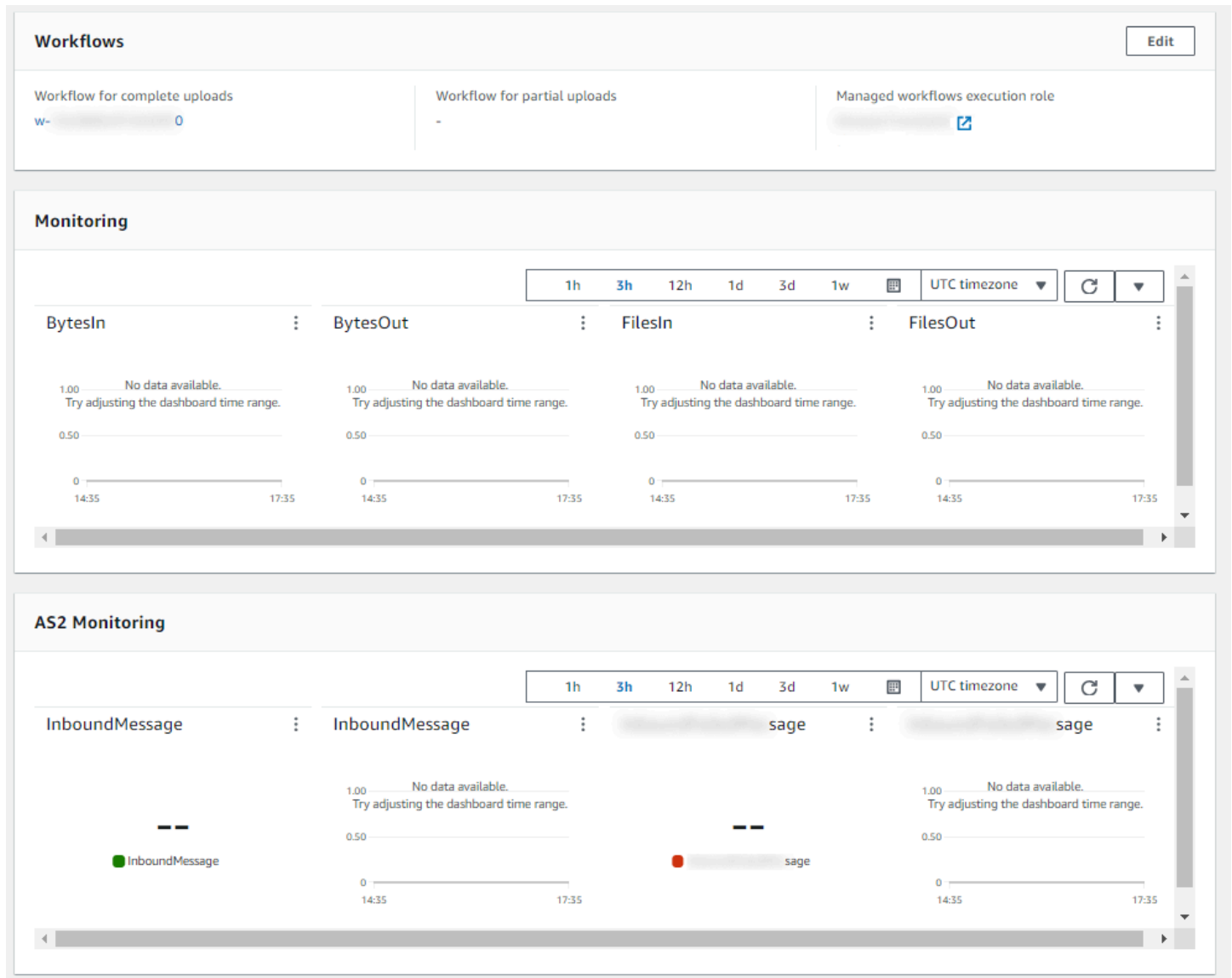
각 AS2 서버에는 세 개의 정적 IP 주소가 할당됩니다. 를 통해 거래 파트너에게 비동기식으로 전송할 MDNs 때 이러한 IP 주소를 사용합니다.

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



AS2 서버 세부 정보 페이지의 하단에는 연결된 워크플로와 모니터링 및 태그 지정 정보에 대한 세부 정보가 포함되어 있습니다.



서버 세부 정보 편집

AWS Transfer Family 서버를 생성한 후 서버 구성을 편집할 수 있습니다.

주제

- [File Transfer 프로토콜 편집](#)
- [사용자 지정 자격 증명 제공자 파라미터 편집](#)
- [서버 엔드포인트 편집](#)
- [로깅 구성 편집](#)
- [보안 정책 편집](#)
- [서버의 관리형 워크플로 변경](#)
- [서버의 디스플레이 배너 변경](#)
- [서버를 온라인이나 오프라인으로 전환](#)

서버의 구성을 편집하는 방법

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버를 선택합니다.
3. 서버 ID 옆에서 식별자를 선택하여 다음과 같은 서버 세부 정보 페이지를 표시합니다.

이 페이지에서 편집을 선택하여 서버의 속성을 변경할 수 있습니다.

- 프로토콜을 변경하려면 [File Transfer 프로토콜 편집](#)을 참조하세요.
- 자격 증명 공급자의 경우 서버 생성 후에는 서버의 자격 증명 공급자 타입을 변경할 수 없습니다. 자격 증명 공급자를 변경하려면, 서버를 삭제하고 원하는 자격 증명 공급자를 이용해 새 서버를 만들어야 합니다.

Note

서버에서 사용자 지정 ID 공급자를 사용하는 경우 일부 속성을 편집할 수 있습니다. 자세한 내용은 [사용자 지정 자격 증명 제공자 파라미터 편집](#)을 참조하세요.

- 엔드포인트 타입 또는 사용자 지정 호스트 이름을 변경하려면 [서버 엔드포인트 편집](#)을 참조하세요.

- 계약을 추가하려면 먼저 서버에 프로토콜AS2로 를 추가해야 합니다. 세부 정보는 [File Transfer 프로토콜 편집](#)을 참조하세요.
- 서버의 호스트 키를 관리하려면 [SFTP지원 서버의 호스트 키 관리](#)를 참조하세요.
- 추가 세부 정보에서 다음 정보를 편집할 수 있습니다.
 - 로깅 역할을 변경하려면 [로깅 구성 편집](#)를 참조하세요.
 - 보안 정책을 변경하려면 [보안 정책 편집](#)를 참조하세요.
 - 서버 호스트 키를 변경하려면 [SFTP지원 서버의 호스트 키 관리](#)를 참조하세요.
 - 서버의 관리 워크플로를 변경하려면 [서버의 관리형 워크플로 변경](#)를 참조하세요.
 - 서버의 디스플레이 배너를 편집하려면 [서버의 디스플레이 배너 변경](#)를 참조하세요.
- 추가 구성 에서 다음 정보를 편집할 수 있습니다.
 - SetStat 옵션 : 클라이언트가 Amazon S3 버킷SETSTAT에 업로드하는 파일에 를 사용하려고 할 때 생성되는 오류를 무시하려면 이 옵션을 활성화합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 SetStatOption 설명서를 참조하세요.
 - TLS 세션 재개 : 는 FTPS 세션의 제어 및 데이터 연결 간에 협상된 보안 암호를 재개하거나 공유하는 메커니즘을 제공합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 TlsSessionResumptionMode 설명서를 참조하세요.
 - 패시브 IP : FTP 및 FTPS 프로토콜에 대한 패시브 모드를 나타냅니다. 방화벽, 라우터 또는 로드 밸런서의 퍼블릭 IP IPv4 주소와 같은 단일 주소를 입력합니다. 자세한 내용은 [ProtocolDetails](#) 주제의 PassiveIp 설명서를 참조하세요.
- 서버를 시작 또는 중지하려면 [서버를 온라인이나 오프라인으로 전환](#)를 참조하세요.
- 서버를 삭제하려면 [서버 삭제](#)를 참조하세요.
- 사용자 속성을 편집하려면 [액세스 통제 관리](#)를 참조하세요.

Protocols Edit	Identity provider Edit
Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda ↗

Note

서버 호스트 키 설명 및 가져온 날짜 값은 2022년 9월 기준으로 새로 추가되었습니다. 이러한 값은 다중 호스트 키 기능을 지원하기 위해 도입되었습니다. 이 기능을 사용하려면 여러 호스트 키가 도입되기 전에 사용 중이던 단일 호스트 키를 모두 마이그레이션해야 했습니다.

마이그레이션된 서버 호스트 키의 가져온 날짜 값은 서버의 마지막 수정 날짜로 설정됩니다. 즉, 마이그레이션된 호스트 키로 표시되는 날짜는 어떤 식으로든 서버 호스트 키 마이그레이션 전에 서버를 마지막으로 수정한 날짜와 일치합니다.

마이그레이션된 유일한 키는 가장 오래된 또는 유일한 서버 호스트 키입니다. 모든 추가 키에는 가져온 시점의 실제 날짜가 표시됩니다. 또한 마이그레이션된 키에는 마이그레이션된 키임을 쉽게 식별할 수 있는 설명이 있습니다.

마이그레이션은 9월 2일에서 9월 13일 사이에 이루어졌습니다. 이 범위 내의 실제 마이그레이션 날짜는 서버 리전에 따라 다릅니다.

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 -

File Transfer 프로토콜 편집

AWS Transfer Family 콘솔에서 파일 전송 프로토콜을 편집할 수 있습니다. File Transfer 프로토콜은 클라이언트를 서버의 엔드포인트에 연결합니다.

프로토콜을 편집하려면

1. 서버 세부 정보 페이지에서 프로토콜 옆의 편집을 선택합니다.

2. 프로토콜 편집 페이지에서 프로토콜 확인란 또는 확인란을 선택하거나 선택 취소하여 다음 파일 전송 프로토콜을 추가하거나 제거합니다.

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP) - 파일 전송 SSH

에 대한 자세한 내용은 섹션을 SFTP참조하세요 [SFTP활성화 서버 생성](#).

- 파일 전송 프로토콜 보안(FTPS) - TLS 암호화를 사용한 파일 전송

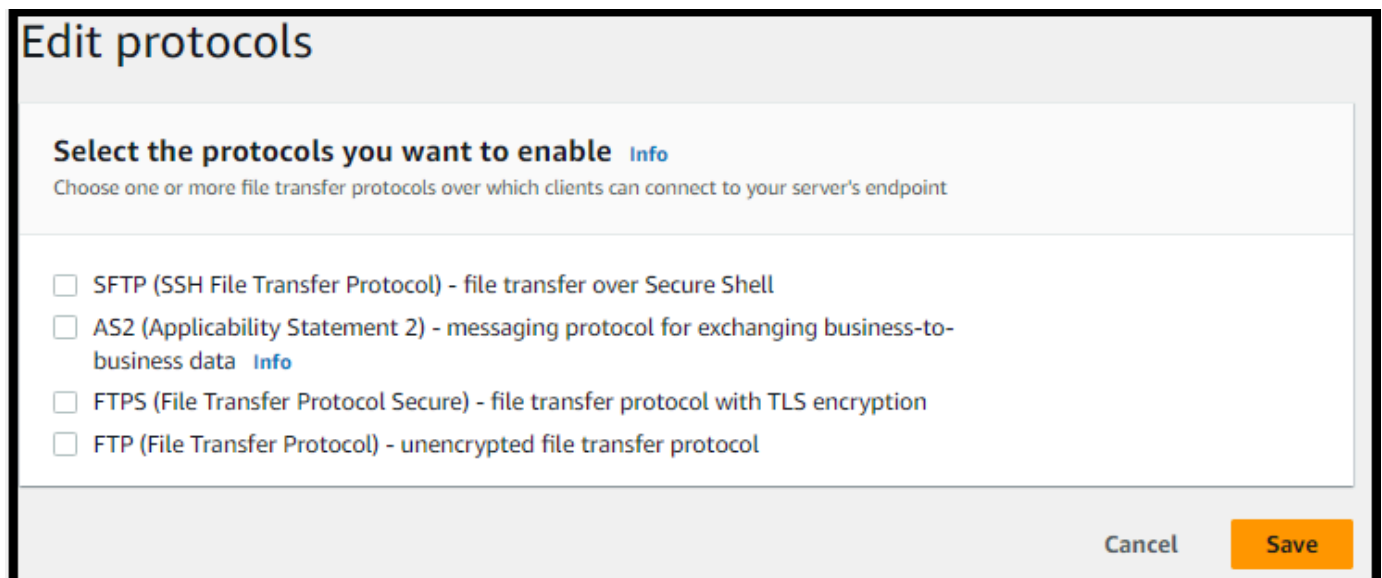
에 대한 자세한 내용은 섹션을 FTP참조하세요 [FTPS활성화 서버 생성](#).

- 파일 전송 프로토콜(FTP) - 암호화되지 않은 파일 전송

에 대한 자세한 내용은 섹션을 FTPS참조하세요 [FTP활성화 서버 생성](#).

Note

에 대해서만 활성화된 기존 서버가 SFTP있고 FTPS 및 를 추가하려는 경우 FTPS 및 와 호환되는 적절한 자격 증명 공급자 및 엔드포인트 유형 설정이 있는지 확인해야 FTP합니다FTP.



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](#)

를 선택하는 경우 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용할 AWS Certificate Manager (ACM)에 저장된 인증서를 선택해야 FTPS합니다FTPS.

새 퍼블릭 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [퍼블릭 인증서 요청](#)을 참조하세요.

기존 인증서를 로 가져오려면 AWS Certificate Manager 사용 설명서의 [로 인증서 가져오기](#)ACM를 참조하세요.

프라이빗 IP 주소를 FTPS 통해 프라이빗 인증서를 사용하도록 요청하려면 AWS Certificate Manager 사용 설명서의 [프라이빗 인증서 요청을 참조하세요](#).

다음 암호화 알고리즘 및 키 크기를 사용하는 인증서가 지원됩니다:

- 2048비트RSA(RSA_2048)
- 4096비트RSA(RSA_4096)
- 타원 프라임 곡선 256비트(EC_prime256v1)
- 타원 프라임 곡선 384 비트(EC_secp384r1)
- 타원 프라임 곡선 521비트(EC_secp521r1)

 Note

인증서는 지정된 FQDN 또는 IP 주소와 발급자에 대한 정보가 있는 유효한 SSL/TLS X.509 버전 3 인증서여야 합니다.

Choose 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

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate

Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS

3. 저장(Save)을 선택합니다. 서버 세부 정보 페이지로 돌아갑니다.

사용자 지정 자격 증명 제공자 파라미터 편집

AWS Transfer Family 콘솔에서 사용자 지정 자격 증명 공급자의 경우 Lambda 함수를 사용하는지 API 게이트웨이를 사용하는지에 따라 일부 설정을 변경할 수 있습니다. 어느 경우든 서버에서 SFTP 프로토콜을 사용하는 경우 인증 방법을 편집할 수 있습니다.

- Lambda를 자격 증명 제공자로 사용하는 경우 기본 Lambda 함수를 변경할 수 있습니다.

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](#)

- API Gateway를 자격 증명 공급자로 사용하는 경우 Gateway URL 또는 호출 역할 또는 둘 다를 업데이트할 수 있습니다.

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

서버 엔드포인트 편집

AWS Transfer Family 콘솔에서 서버 엔드포인트 유형과 사용자 지정 호스트 이름을 수정할 수 있습니다.

서버 엔드포인트 세부 정보를 편집하려면

1. 서버 세부 정보 페이지에서 엔드포인트 세부 정보 옆의 편집을 선택합니다.
2. 엔드포인트 구성 편집 페이지에서 엔드포인트 타입으로 다음 중 하나를 선택합니다.
 - 퍼블릭 - 이 옵션을 사용하면 인터넷을 통해 서버에 액세스할 수 있습니다.
 - VPC - 이 옵션을 사용하면 가상 프라이빗 클라우드()에서 서버에 액세스할 수 있습니다VPC.에 대한 자세한 내용은 섹션을 VPC참조하세요[Virtual Private Cloud\(VPC\)에 서버 생성](#).
3. 사용자 지정 호스트 이름의 경우 다음 중 하나를 선택합니다.
 - 없음 - 사용자 지정 도메인을 사용하지 않으려면 없음을 선택합니다.

에서 제공하는 서버 호스트 이름을 가져옵니다 AWS Transfer Family. 서버 호스트 이름은 `serverId.server.transfer.regionId.amazonaws.com` 형식을 취합니다.

- Amazon Route 53 DNS별칭 - Route 53에서 자동으로 생성된 별DNS칭을 사용하려면 이 옵션을 선택합니다.
- 기타 DNS - 외부 DNS 서비스에 이미 소유하고 있는 호스트 이름을 사용하려면 기타를 DNS선택합니다.

Amazon Route 53 DNS별칭 또는 기타DNS를 선택하면 서버의 엔드포인트와 연결할 이름 확인 방법이 지정됩니다.

예를 들어 사용자 지정 도메인이 `sftp.inbox.example.com`일 수 있습니다. 사용자 지정 호스트 이름은 사용자가 제공하고 DNS 서비스가 확인할 수 있는 DNS 이름을 사용합니다. Route 53을 DNS 해석기로 사용하거나 자체 DNS 서비스 공급자를 사용할 수 있습니다. AWS Transfer Family가 Route 53을 이용해 트래픽을 사용자 지정 도메인에서 SFTP 엔드포인트로 라우팅하는 방법은 [사용자 지정 호스트 이름으로 작업](#)를 참조하세요.

4. 저장(Save)을 선택합니다. 서버 세부 정보 페이지로 돌아갑니다.

로깅 구성 편집

AWS Transfer Family 콘솔에서 로깅 구성을 변경할 수 있습니다.

Note

서버를 생성할 때 Transfer Family가 CloudWatch 로깅 IAM 역할을 생성한 경우 IAM 해당 역할을 라고 합니다 `AWSTransferLoggingAccess`. 모든 Transfer Family 서버에 사용할 수 있습니다.

로깅 구성 편집

1. 서버 세부 정보 페이지에서 추가 세부 정보 옆의 편집을 선택합니다.
2. 구성에 따라 로깅 역할, 구조화된 JSON 로깅 또는 둘 다 중에서 선택합니다. 자세한 내용은 [서버의 로깅 업데이트](#) 단원을 참조하십시오.

보안 정책 편집

이 절차에서는 AWS Transfer Family 콘솔 또는 를 사용하여 Transfer Family 서버의 보안 정책을 변경하는 방법을 설명합니다 AWS CLI.

Note

엔드포인트가 FIPS활성화된 경우 FIPS 보안 정책을 비FIPS보안 정책으로 변경할 수 없습니다.

Console

콘솔을 사용하여 보안 정책을 편집하려면

1. 서버 세부 정보 페이지에서 추가 세부 정보 옆의 편집을 선택합니다.
2. 암호화 알고리즘 옵션의 경우 서버에서 사용하도록 설정된 암호화 알고리즘이 포함된 보안 정책을 선택합니다.

보안 정책에 대한 자세한 설명은 섹션을 참조하세요 [에 대한 보안 정책 AWS Transfer Family](#).

3. 저장(Save)을 선택합니다.

업데이트된 보안 정책을 볼 수 있는 서버 세부 정보 페이지로 돌아갑니다.

AWS CLI

를 사용하여 보안 정책을 편집하려면 CLI

1. 다음 명령을 실행하여 서버에 연결된 현재 보안 정책을 확인합니다.

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

이 describe-server 명령은 다음 줄을 포함하여 서버의 모든 세부 정보를 반환합니다.

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

이 경우 서버의 보안 정책은 입니다 TransferSecurityPolicy-2018-11.

- 명령에 보안 정책의 정확한 이름을 제공해야 합니다. 예를 들어 다음 명령을 실행하여 서버를 업데이트합니다TransferSecurityPolicy-2023-05.

```
aws transfer update-server --server-id your-server-id --security-policy-name
"TransferSecurityPolicy-2023-05"
```

Note

사용 가능한 보안 정책의 이름은 [에 대한 보안 정책 AWS Transfer Family](#)에 나열되어 있습니다.

성공하면 명령은 다음 코드를 반환하고 서버의 보안 정책을 업데이트합니다.

```
{
  "ServerId": "your-server-id"
}
```

서버의 관리형 워크플로 변경

AWS Transfer Family 콘솔에서 서버와 연결된 관리형 워크플로를 변경할 수 있습니다.

관리형 워크플로 변경

- 서버 세부 정보 페이지에서 추가 세부 정보 옆의 편집을 선택합니다.
- 추가 세부 정보 편집 페이지의 관리형 워크플로 섹션에서 모든 업로드에서 실행할 워크플로를 선택합니다.

Note

워크플로가 아직 없는 경우 새 워크플로 생성을 선택하여 워크플로를 생성합니다.

- 사용할 워크플로 ID를 선택합니다.
- 실행 역할을 선택합니다. 이 역할은 워크플로의 단계를 실행할 때 Transfer Family가 맡는 역할입니다. 자세한 내용은 [IAM 워크플로 정책](#)를 참조하세요. 저장(Save)을 선택합니다.

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

[role dropdown] [refresh]

3. 저장(Save)을 선택합니다. 서버 세부 정보 페이지로 돌아갑니다.

서버의 디스플레이 배너 변경

AWS Transfer Family 콘솔에서 서버와 연결된 디스플레이 배너를 변경할 수 있습니다.

디스플레이 배너를 변경하려면

1. 서버 세부 정보 페이지에서 추가 세부 정보 옆의 편집을 선택합니다.
2. 추가 세부정보 편집 페이지의 디스플레이 배너 섹션에서 사용 가능한 디스플레이 배너의 텍스트를 입력합니다.
3. 저장(Save)을 선택합니다. 서버 세부 정보 페이지로 돌아갑니다.

서버를 온라인이나 오프라인으로 전환

AWS Transfer Family 콘솔에서 서버를 온라인으로 가져오거나 오프라인으로 전환할 수 있습니다.

서버를 온라인 상태로 전환하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.
3. 오프라인 상태인 서버의 확인란을 선택합니다.
4. 작업에서 시작을 선택합니다.

서버가 오프라인에서 온라인으로 전환되는 데는 몇 분 정도 걸릴 수 있습니다.

Note

오프라인으로 전환하기 위해 서버를 중단해도, 해당 서버에 대한 서비스 요금은 계속 발생합니다. 추가 서버 관련 요금을 방지하려면, 해당 서버를 삭제해야 합니다.

서버를 오프라인 상태로 전환하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 탐색 창에서 서버를 선택합니다.
3. 온라인 상태인 서버의 확인란을 선택합니다.
4. 작업에서 중지를 선택합니다.

서버가 시작 또는 종료 중일 때는 서버가 파일 작업을 수행할 수 없습니다. 콘솔은 시작 및 중단 상태를 표시하지 않습니다.

오류 조건 START_FAILED 또는 를 발견한 경우 AWS Support 에 STOP_FAILED 문의하여 문제를 해결하세요.

SFTP지원 서버의 호스트 키 관리

Important

기존 사용자를 기존 SFTP지원 서버에서 새 SFTP지원 서버로 마이그레이션할 계획이 없는 경우 이 섹션을 무시하세요.

실수로 서버의 호스트 키를 변경하면 작업에 영향을 줄 수 있습니다. SFTP 클라이언트 구성 방식에 따라 신뢰할 수 있는 호스트 키가 없다는 메시지와 함께 즉시 실패하거나 위협적인 프롬프트가 표시될 수 있습니다. 연결을 자동화하는 스크립트가 있는 경우 이 스크립트도 실패할 가능성이 높습니다.

기본적으로 는 SFTP사용 가능한 서버의 호스트 키를 AWS Transfer Family 제공합니다. 기본 호스트 키를 다른 서버의 호스트 키로 바꿀 수 있습니다. 기존 사용자를 기존 SFTP지원 서버에서 새 SFTP지원 서버로 이동하려는 경우에만 이 작업을 수행합니다.

사용자가 SFTP지원 서버의 신뢰성을 다시 확인하라는 메시지가 표시되지 않도록 하려면 온프레미스 서버의 호스트 키를 SFTP지원 서버로 가져옵니다. 이렇게 하면 사용자가 잠재적 man-in-the-middle 공격에 대한 경고를 받지 못할 수도 있습니다.

추가 보안 조치로 호스트 키를 주기적으로 교체할 수도 있습니다.

Note

Transfer Family 콘솔을 사용하면 모든 서버에 대해 서버 호스트 키를 지정하고 추가할 수 있지만 이러한 키는 SFTP 프로토콜을 사용하는 서버에만 유용합니다.

주제

- [추가 서버 호스트 키 추가](#)
- [서버 호스트 키 삭제](#)
- [서버 호스트 키 교체](#)
- [추가 서버 호스트 키 정보](#)

추가 서버 호스트 키 추가

AWS Transfer Family 콘솔에서 서버 호스트 키를 추가할 수 있습니다. 형식이 다른 호스트 키를 추가하면 클라이언트가 서버에 연결할 때 서버를 식별하고 보안 프로필을 개선하는 데 유용할 수 있습니다. 예를 들어 원본 키가 RSA 키인 경우 키를 추가할 수 있습니다ECDSA.

Note

SFTP 클라이언트는 활성 서버 키 중 하나와 일치할 수 있는 첫 번째 퍼블릭 키를 사용하여 연결합니다.

추가 서버 호스트 키 추가

1. 에서 AWS Transfer Family 콘솔을 엽니다<https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버 를 선택한 다음 SFTP 프로토콜을 사용하는 서버를 선택합니다.
3. 서버 세부 정보 페이지에서 서버 호스트 키 섹션까지 아래로 스크롤합니다.

Server host keys (1)						Actions	Add host key
						< 1 >	
☐	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	hostkey-	SHA256: [fingerprint]	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26		

4. 호스트 키 추가를 선택합니다.

서버 호스트 키 추가 페이지가 표시됩니다.

5. 서버 호스트 키 섹션에서 클라이언트가 SFTP 활성화된 서버를 통해 서버를 연결할 때 서버를 식별하는 데 사용되는 RSAECDSA, 또는 ED25519 프라이빗 키를 입력합니다.

Note

서버 호스트 키를 생성할 때는 반드시 -N ""를 지정해야 합니다(암호 없음). 키 쌍을 생성하는 방법에 대한 자세한 내용은 [macOS, Linux 또는 Unix에서 SSH 키 생성](#)을 참조하세요.

Server Host Key [Info](#)

Private key - optional

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

 You can ignore this section unless you are migrating users from an existing SFTP server.

6. (옵션) 설명을 추가하여 여러 서버 호스트 키를 구분합니다. 키에 태그를 추가할 수도 있습니다.

7. 키 추가를 선택합니다. 서버 세부 정보 페이지로 돌아갑니다.

AWS Command Line Interface (AWS CLI)를 사용하여 호스트 키를 추가하려면 [the section called “ImportHostKey”](#) API 작업을 사용하고 새 호스트 키를 제공합니다. 새 SFTP지원 서버를 생성하는 경우 [the section called “CreateServer”](#) API 작업에서 호스트 키를 파라미터로 제공합니다. AWS CLI 를 사용하여 기존 호스트 키의 설명을 업데이트할 수도 있습니다.

다음 예제 import-host-key AWS CLI 명령은 지정된 SFTP활성화 서버의 호스트 키를 가져옵니다.

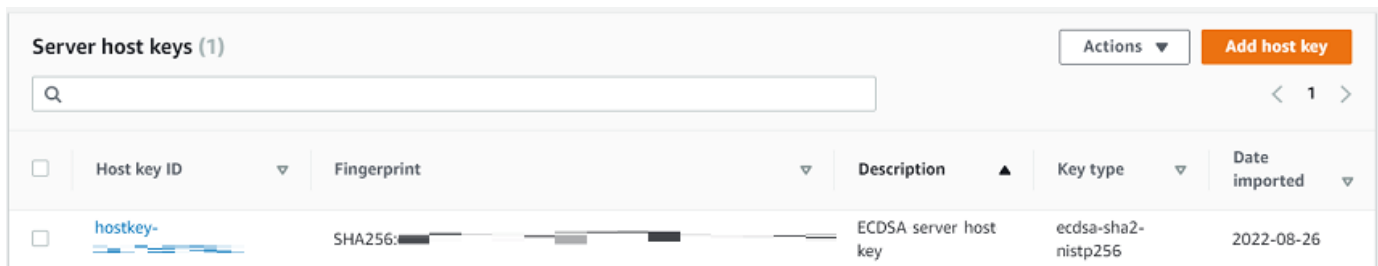
```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

서버 호스트 키 삭제

AWS Transfer Family 콘솔에서 서버 호스트 키를 삭제할 수 있습니다.

서버 호스트 키를 삭제하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 왼쪽 탐색 창에서 서버 를 선택한 다음 SFTP 프로토콜을 사용하는 서버를 선택합니다.
3. 서버 세부 정보 페이지에서 서버 호스트 키 섹션까지 아래로 스크롤합니다.



Server host keys (1)					Actions	Add host key
	Host key ID	Fingerprint	Description	Key type	Date imported	
☐	hostkey-	SHA256: [fingerprint]	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26	

4. 서버 호스트 키 섹션에서 키를 선택한 다음 작업에서 삭제를 선택합니다.
5. 표시되는 확인 대화 상자에 단어 **delete**을 입력한 다음 삭제를 선택한 다음 삭제를 선택합니다.

서버 페이지에서 호스트 키가 삭제됩니다.

를 사용하여 호스트 키를 삭제하려면 [the section called “DeleteHostKey”](#) API 작업을 AWS CLI사용하고 서버 ID와 호스트 키 ID를 제공합니다.

다음 예제 delete-host-key AWS CLI 명령은 지정된 SFTP활성화 서버의 호스트 키를 삭제합니다.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

서버 호스트 키 교체

서버 호스트 키를 주기적으로 교체할 수 있습니다.

Note

Transfer Family는 각 알고리즘에 처음 추가된 키를 활성 호스트 키로 사용합니다. SFTP 서버 당 최대 10개의 호스트 키를 연결할 수 있지만 알고리즘당 하나의 키만 특정 시간에 활성화됩니다.

예를 들어 다음 서버 호스트 키 세트를 추가했다고 가정합니다.

서버 호스트 키

호스트 키 타입	서버에 추가된 날짜	활성 상태입니까?
RSA	2020년 4월 1일	아니요
ECDSA	2020년 2월 1일	아니요
ED25519	2019년 12월 1일	아니요
RSA	2019년 10월 1일	예
ECDSA	2019년 6월 1일	예
ED25519	2019년 3월 1일	예

각 알고리즘에서 가장 오래된 키가 활성 상태입니다. 2019년 10월 1일에 추가한 RSA 키를 제거하면 2020년 4월 1일에 추가한 RSA 키가 활성화됩니다.

서버 호스트 키를 교체하려면

1. 새 서버 호스트 키를 추가합니다. 이 절차는 [추가 서버 호스트 키 추가](#)에 설명되어 있습니다.
2. 이전에 추가한 것과 같은 타입의 호스트 키를 하나 이상 삭제합니다. 이 절차는 [서버 호스트 키 삭제](#)에 설명되어 있습니다.

3. 동일한 타입 중 가장 먼저 남아 있는 키가 활성화하려는 키인지 확인합니다.

추가 서버 호스트 키 정보

호스트 키를 선택하여 해당 키에 대한 세부 정보를 표시할 수 있습니다.

The screenshot shows the 'Host key configuration' page for a specific host key. The breadcrumb navigation is 'Transfer Family > Servers > s-... > Hostkey: hostkey-...'. The host key name 'hostkey-...' is displayed at the top with a 'Delete' button. Below, the 'Host key configuration' section contains the following details:

- Fingerprint:** SHA256: [fingerprint]
- Description:** Imported host key
- Key type:** ssh-rsa
- Date imported:** Fri, 09 Jul 2021 16:51:20 GMT
- Amazon Resource Name (ARN):** arn:aws:transfer:us-east-2:[:host-key/s-.../hostkey-...]

Buttons for 'Delete' and 'Edit' are visible in the top right corner of the configuration section.

서버 세부 정보 화면의 작업 메뉴에서 호스트 키를 삭제하거나 설명을 편집할 수 있습니다. 호스트 키를 선택한 다음 메뉴에서 적절한 작업을 선택합니다.

The screenshot shows the 'Server host keys (2)' list. A search bar is at the top. An 'Add host key' button is in the top right. An 'Actions' menu is highlighted with a red box, showing options: 'Edit' and 'Delete'. The table below lists the host keys:

	Host key ID	Fingerprint	Description	Key type	Date imported
☐	hostkey-...	SHA256: [fingerprint]	ECDSA private key to use with new Transfer server.	ecdsa-sha2-nistp521	2022-09-27
☒	hostkey-...	SHA256: [fingerprint]	Imported host key	ssh-rsa	2021-06-17

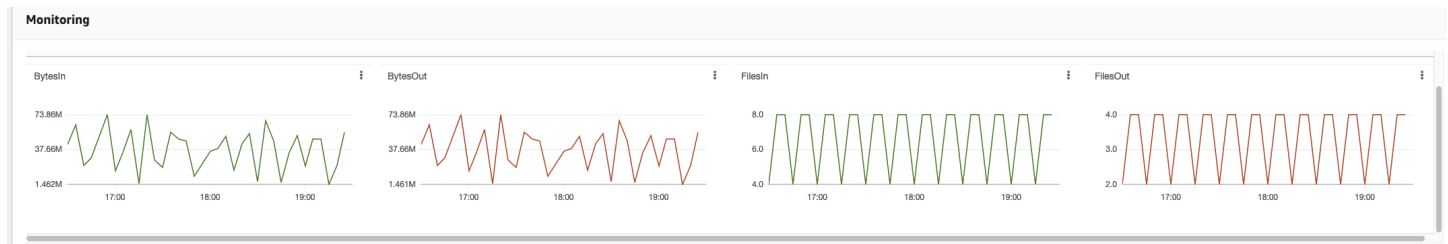
콘솔 내 사용량 모니터링

서버 세부 정보 페이지에서 서버 메트릭에 대한 정보를 얻을 수 있습니다. 이를 통해 파일 전송 워크로드를 한 곳에서 모니터링할 수 있습니다. 중앙 집중식 대시보드를 사용하여 파트너와 교환한 파일 수를 추적하고 파트너의 사용량을 면밀히 추적할 수 있습니다. 자세한 내용은 [SFTP, FTPS 및 FTP 서버 세부 정보 보기](#)를 참조하세요. 다음 표에서는 Transfer Family에 사용할 수 있는 측정치를 설명합니다.

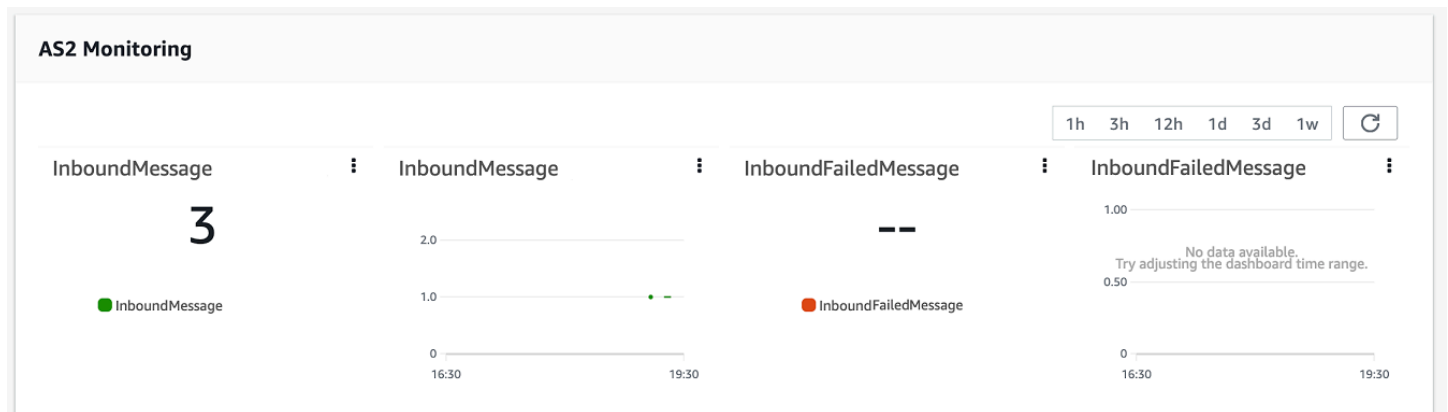
네임스페이스	지표	설명
AWS/Transfer	BytesIn	서버로 전송된 총 바이트 수. 단위: 개 기간: 5분
	BytesOut	서버에서 전송된 총 바이트 수입니다. 단위: 개 기간: 5분
	FilesIn	서버로 전송된 총 파일 수. AS2 프로토콜을 사용하는 서버의 경우 이 지표는 수신된 메시지 수를 나타냅니다. 단위: 개 기간: 5분
	FilesOut	서버에서 전송된 총 파일 수. 단위: 개 기간: 5분
	InboundMessage	거래 파트너로부터 성공적으로 수신된 총 AS2 메시지 수입니다. 단위: 개 기간: 5분
	InboundFailedMessage	거래 파트너로부터 수신하지 못한 총 AS2 메시지 수입니다. 즉, 거래 파트너가 메시지를 보냈지만 Transfer Family 서버가 메시지를 성공적으로 처리하지 못했습니다. 단위: 개

네임스페이스	지표	설명
		기간: 5분
	OnPartialUploadExecutionsStarted	서버에서 시작된 총 워크플로 실행 수 on-partial-upload입니다. 단위: 개 기간: 1분
	OnPartialUploadExecutionsSuccess	서버에서 성공 on-partial-upload한 총 워크플로 실행 수입니다. 단위: 개 기간: 1분
	OnPartialUploadExecutionsFailed	서버에서 실패한 on-partial-upload 워크플로 실행의 총 수입니다. 단위: 개 기간: 1분
	OnUploadExecutionsStarted	서버에서 시작된 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분
	OnUploadExecutionsSuccess	서버에서 성공적인 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분
	OnUploadExecutionsFailed	서버에서 실패한 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분

모니터링 섹션에는 4개의 개별 그래프가 있습니다. 이 그래프는 입력 바이트, 출력 바이트, 파일 입력 및 출력 파일을 보여 줍니다.



AS2 프로토콜이 활성화된 서버의 경우 AS2 모니터링 정보 아래에 모니터링 섹션이 있습니다. 이 섹션에는 성공 및 실패 인바운드 메시지 수에 대한 세부 정보가 포함되어 있습니다.



선택한 그래프를 자체 창에서 열려면 확장 아이콘



을 선택합니다. 그래프의 세로 줄임표 아이콘



을 클릭하여 다음 항목이 포함된 드롭다운 메뉴를 열 수도 있습니다.

- 확대 - 선택한 그래프를 자체 창에서 엽니다.
- 새로 고침 - 그래프를 최신 데이터로 다시 로드합니다.
- 지표에서 보기 - Amazon 에서 해당 지표 세부 정보를 엽니다 CloudWatch.
- 로그 보기 - 에서 해당 로그 그룹을 엽니다 CloudWatch.

액세스 통제 관리

(IAM) 정책을 사용하여 AWS Transfer Family 리소스에 대한 사용자의 액세스를 제어할 수 있습니다. AWS Identity and Access Management . IAM 정책은 리소스에 대한 특정 수준의 액세스를 허용하는 일반적으로 JSON 형식의 문입니다. IAM 정책을 사용하여 사용자가 수행하고 수행하지 않도록 허용할 파일 작업을 정의합니다. IAM 정책을 사용하여 사용자에게 액세스 권한을 부여하려는 Amazon S3 버킷 또는 버킷을 정의할 수도 있습니다. 사용자에게 이러한 정책을 지정하려면 IAM 정책과 신뢰 관계가 연결된 AWS Transfer Family 에 대한 IAM 역할을 생성합니다.

각 사용자에게는 IAM 역할이 할당됩니다. AWS Transfer Family 에서 사용하는 IAM 역할 유형을 서비스 역할이라고 합니다. 사용자가 서버에 로그인하면 는 사용자에게 매핑된 IAM 역할을 AWS Transfer Family 가 가정합니다. Amazon S3 버킷에 대한 사용자 액세스 권한을 제공하는 IAM 역할을 생성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 서비스에 권한을 위임하는 역할 생성을 참조하세요](#).

IAM 정책 내에서 특정 권한을 사용하여 Amazon S3 객체에 대한 쓰기 전용 액세스 권한을 부여할 수 있습니다. 세부 정보는 [파일을 쓰고 나열할 수 있는 권한만 부여](#)를 참조하세요.

AWS 스토리지 블로그에는 최소 권한 액세스를 설정하는 방법을 자세히 설명하는 게시물이 포함되어 있습니다. 자세한 내용은 [AWS Transfer Family 워크플로에서 최소 권한 액세스 구현을 참조하세요](#).

Note

Amazon S3 버킷이 AWS Key Management Service (AWS KMS)를 사용하여 암호화된 경우 정책에 추가 권한을 지정해야 합니다. 세부 정보는 [Amazon S3의 데이터 암호화](#)를 참조하세요. 또한 IAM 사용 설명서에서 [세션 정책에](#) 대한 자세한 내용을 확인할 수 있습니다.

주제

- [Amazon S3 버킷에 대한 읽기 및 쓰기 액세스 허용](#)
- [Amazon S3 버킷을 위한 세션 정책 생성](#)
- [사용자가 S3 버킷에서 mkdir를 실행하지 못하도록 방지](#)

Amazon S3 버킷에 대한 읽기 및 쓰기 액세스 허용

이 섹션에서는 특정 Amazon S3 버킷에 대한 읽기 및 쓰기 액세스를 허용하는 IAM 정책을 생성하는 방법을 설명합니다. 사용자에게 이 IAM 정책이 있는 IAM 역할을 할당하면 해당 사용자에게 지정된 Amazon S3 버킷에 대한 읽기/쓰기 액세스 권한이 부여됩니다.

다음 정책은 Amazon S3 버킷에 대한 프로그래밍 방식의 읽기 및 쓰기 액세스 권한을 제공합니다. GetObjectACL 및 PutObjectACL 명령문은 크로스 계정 액세스를 활성화할 필요가 있는 경우에만 요구됩니다. 예컨대, Transfer Family 서버가 다른 계정의 버킷에 액세스할 필요가 있는 경우입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-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:::DOC-EXAMPLE-BUCKET/*"]
    }
  ]
}
```

ListBucket 작업은 버킷 자체에 대한 권한을 요구합니다. PUT, GET, DELETE 작업은 객체 권한을 요구합니다. 리소스는 서로 다르기 때문에 서로 다른 Amazon 리소스 이름()을 사용하여 지정됩니다 ARNs.

사용자의 액세스를 지정된 Amazon S3 버킷의 home 접두사로만 제약하는 방법은 [Amazon S3 버킷을 위한 세션 정책 생성](#) 섹션을 참조하세요.

Amazon S3 버킷을 위한 세션 정책 생성

세션 정책은 사용자를 Amazon S3 버킷의 특정 부분으로 제한하는 AWS Identity and Access Management (IAM) 정책입니다. 이 정책은 액세스를 실시간으로 평가해 이를 수행합니다.

Note

세션 정책은 Amazon S3에서만 사용됩니다. Amazon 의 경우 POSIX 파일 권한을 EFS사용하여 액세스를 제한합니다.

세션 정책은 사용자 그룹 전원이 Amazon S3 버킷의 특정 부분에만 액세스하도록 제한해야 할 때 사용됩니다. 예를 들어 사용자 그룹이 home 디렉터리에만 액세스해야 할 수도 있습니다. 해당 사용자 그룹은 동일한 IAM 역할을 공유합니다.

Note

세션 정책의 최대 길이는 2,048자입니다. 자세한 내용은 API 참조의 CreateUser 작업에 대한 [정책 요청 파라미터](#)를 참조하세요.

세션 정책을 생성하려면 정책에서 다음 IAM 정책 변수를 사용합니다.

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

관리형 정책에서는 위의 변수를 사용할 수 없습니다. IAM 역할 정의에서 정책 변수로 사용할 수도 없습니다. IAM 정책에서 이러한 변수를 생성하고 사용자를 설정할 때 직접 제공합니다. 그리고 이 세션 정책에서는 `${aws:Username}` 변수는 사용할 수 없습니다. 이 변수는 필요한 IAM 사용자 이름이 아닌 사용자 이름을 나타냅니다 AWS Transfer Family.

다음 코드는 예 세션 정책을 보여줍니다.

```

{
  "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

위의 정책 예에서는 사용자의 홈 디렉터리가 디렉터리임을 나타내기 위해 후행 슬래시를 포함하도록 설정된 것으로 가정합니다. 그 반면에 후행 슬래시가 없이 사용자의 HomeDirectory를 설정하는 경우에는 이를 정책의 일부로 포함해야 합니다.

이전 예 정책에서, `transfer:HomeFolder`, `transfer:HomeBucket`, `transfer:HomeDirectory` 정책 파라미터의 사용을 기억해 두세요. 이러한 파라미터 HomeDirectory는 [HomeDirectory](#) 및 에 설명된 대로 사용자용으로 구성된 에 대해 설정됩니다 [API Gateway 메서드 구현](#). 이러한 파라미터의 정의는 다음과 같습니다.

- `transfer:HomeBucket` 파라미터는 HomeDirectory의 첫 번째 구성 요소로 대체됩니다.
- `transfer:HomeFolder` 파라미터가 HomeDirectory 파라미터의 나머지 부분으로 대체됩니다.
- `transfer:HomeDirectory` 파라미터에는 선행 슬래시(/)가 제거되어 Resource 문에서 S3 Amazon 리소스 이름(ARN)의 일부로 사용할 수 있습니다.

Note

귀하가 논리적 디렉터를 사용하는 경우—즉 사용자의 `homeDirectoryType`가 LOGICAL인 경우—이러한 정책 파라미터(`HomeBucket`, `HomeDirectory`, 및 `HomeFolder`)는 지원되지 않습니다.

예를 들어, Transfer Family 사용자에 대해 구성된 HomeDirectory 파라미터가 `/home/bob/amazon/stuff/(이)`라고 가정해 보겠습니다.

- `transfer:HomeBucket`를 `/home(으)`로 설정합니다.
- `transfer:HomeFolder`를 `/bob/amazon/stuff/(으)`로 설정합니다.
- `transfer:HomeDirectory`는 `home/bob/amazon/stuff/`가 됩니다.

첫 번째 "Sid"은(는) 사용자가 `/home/bob/amazon/stuff/`부터 시작하여 모든 디렉터를 나열할 수 있게 해 줍니다.

두 번째 "Sid"은(는) 동일한 경로인 `/home/bob/amazon/stuff/`에 대한 사용자 put 및 get 액세스를 제한합니다.

앞의 정책을 활성화하면, 로그인 시 사용자는 자신의 홈 디렉터리에 있는 객체만 액세스할 수 있습니다. 연결 시는 이러한 변수를 사용자에게 적합한 값으로 바 AWS Transfer Family 끕니다. 이렇게 하면 같은 정책 설명서를 다수의 사용자에게 쉽게 적용할 수 있습니다. 이 접근 방식은 Amazon S3 버킷에 대한 사용자의 액세스를 관리하기 위한 IAM 역할 및 정책 관리의 오버헤드를 줄입니다.

세션 정책을 사용하면 업무 요건에 따라 각 사용자의 액세스를 조절할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 [AssumeRole AssumeRoleWithSAML, 및 에 대한 권한을 AssumeRoleWithWebIdentity](#) 참조하세요.

Note

AWS Transfer Family 는 정책의 Amazon 리소스 이름(ARN) JSON대신 정책 를 저장합니다. 따라서 IAM 콘솔에서 정책을 변경할 때는 AWS Transfer Family 콘솔로 돌아가서 최신 정책 콘텐츠로 사용자를 업데이트해야 합니다. 사용자 구성 섹션의 정책 정보 탭에서 사용자를 업데이트할 수 있습니다.

를 사용하는 경우 다음 명령을 사용하여 정책을 업데이트할 AWS CLI수 있습니다.

```
aws transfer update-user --server-id server --user-name user --policy \
    "$(aws iam get-policy-version --policy-arn policy --version-id version --
    output json)"
```

사용자가 S3 버킷에서 **mkdir**를 실행하지 못하도록 방지

Amazon S3 버킷에 디렉터리를 생성할 수 있는 모든 기능을 제한할 수 있습니다. 이렇게 하려면 s3:PutObject 작업을 허용하지만 키가 "/"(전진 슬래시)로 종료될 때도 거부하는 IAM 정책을 생성합니다. 다음 예 정책은 사용자가 Amazon S3 버킷에 파일을 업로드하도록 허용하지만 Amazon S3 버킷에서는 mkdir 명령을 거부합니다.

```
{
  "Sid": "DenyMkdir",
  "Action": [
    "s3:PutObject"
  ],
  "Effect": "Deny",
  "Resource": [
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/",
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/*"
  ]
}
```

```
}
```

Note

두 번째 리소스 라인을 사용하면 사용자가 `put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file`와(과) 같은 명령을 실행하여 하위 폴더를 생성할 수 없습니다.

에 대한 로깅 AWS Transfer Family

AWS Transfer Family 는 AWS CloudTrail 및 Amazon 와 통합 CloudTrail 되며 서로 다르지만 보완적인 목적을 CloudWatch 제공합니다 CloudWatch.

- CloudTrail 는 내에서 수행된 작업의 레코드를 생성하는 AWS 서비스입니다 AWS 계정. 콘솔 로그인, AWS Command Line Interface 명령 및 SDK/API 또는 API 호출과 같은 활동에 대한 호출을 지속적으로 모니터링하고 기록합니다. 이를 통해 환경의 모든 활동 기록을 제공하여 감사, 액세스 관리 및 규정 준수를 CloudTrail 지원하는 누가 어떤 조치를 언제, 어디서 취했는지에 대한 로그를 유지할 수 있습니다 AWS . 자세한 내용은 [AWS CloudTrail 사용 설명서 섹션](#)을 참조하세요.
- CloudWatch 는 AWS 리소스 및 애플리케이션에 대한 모니터링 서비스입니다. 지표와 로그를 수집하여 리소스 사용률, 애플리케이션 성능 및 전체 시스템 상태에 대한 가시성을 제공합니다. 문제 해결, 경보 설정 및 오토스케일링과 같은 운영 작업을 CloudWatch 지원합니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서 섹션](#)을 참조하세요.

주제

- [AWS CloudTrail로깅 대상 AWS Transfer Family](#)
- [에 대한 Amazon CloudWatch 로깅 AWS Transfer Family](#)

AWS CloudTrail로깅 대상 AWS Transfer Family

AWS Transfer Family에서 AWS Transfer Family 사용자AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다. CloudTrail 모든 API 호출을 AWS Transfer Family 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Transfer Family 콘솔로부터의 호출과 AWS Transfer Family API 작업에 대한 코드 호출이 포함됩니다.

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트race가 아니므로 특정 순서로 표시되지 않습니다.

AWS Transfer Family에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 지역에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 지역의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한

CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- [추적 생성 개요](#)
- [CloudTrail 지원되는 서비스 및 통합](#)
- [에 대한 Amazon SNS 알림 구성 CloudTrail](#)
- [여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신](#)

모든 AWS Transfer Family 작업은 에 의해 CloudTrail 기록되고 문서화됩니다. [ActionsAPI reference](#) 예를 들어 CreateServer, 에 대한 호출 ListUsers 및 StopServer 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management 사용자 보안 인증으로 했는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지.

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하십시오.

트레일을 생성하면 에 대한 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 AWS Transfer Family 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Transfer Family, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 [AWS CloudTrail사용 설명서를](#) 참조하십시오.

주제

- [AWS CloudTrail 로깅 활성화](#)
- [서버 생성을 위한 로그 항목 예제](#)

AWS CloudTrail 로깅 활성화

AWS CloudTrail을(를) 사용하여 AWS Transfer Family API 호출을 모니터링할 수 있습니다. API 호출을 모니터링하면, 유용한 보안 및 운영 정보를 얻을 수 있습니다. [Amazon S3 객체 수준 로깅을 활성화한](#) 경우, 요청자 필드에 RoleSessionName이(가) [AWS:Role Unique Identifier]/username.sessionid@server-id(으)로 포함됩니다. AWS Identity and Access Management (IAM) 역할에 대한 자세한 설명은 AWS Identity and Access Management 사용자 가이드의 [고유 식별자](#)를 참조하세요.

Important

RoleSessionName의 최대 길이는 64자입니다. RoleSessionName 길이가 더 길면 server-id이(가) 잘립니다.

서버 생성을 위한 로그 항목 예제

다음 예제는 작업을 보여주는 CloudTrail 로그 항목 (JSON 형식) 을 보여줍니다. CreateServer

```
{
  "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"
  }
}

```

에 대한 Amazon CloudWatch 로깅 AWS Transfer Family

Amazon은 AWS Transfer Family 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. CloudWatch 를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.

CloudWatch 홈 페이지에는 Transfer Family 및 사용하는 다른 모든 AWS 서비스에 대한 지표가 자동으로 표시됩니다. 사용자 지정 대시보드를 추가로 생성해 사용자 지정 애플리케이션에 대한 지표를 표시하고, 선택한 지표의 사용자 지정 집합을 표시할 수 있습니다.

지표를 감시해 알림을 보내거나 임계값을 위반한 경우 모니터링 중인 리소스를 자동으로 변경하는 경보를 생성할 수 있습니다. 예를 들어 Transfer Family 서버로 전송되는 파일을 모니터링하고 해당 데이터를 사용하여 증가된 부하를 처리하기 위해 추가 서버를 배포해야 하는지 여부를 결정할 수 있습니다. 이 데이터를 사용하여 과소 사용된 인스턴스를 중지하거나 삭제하여 비용을 절감할 수도 있습니다.

주제

- [서버에 대한 로깅 생성, 업데이트 및 보기](#)
- [워크플로에 대한 로깅 관리](#)
- [CloudWatch 로깅 역할 구성](#)
- [Transfer Family 로그 스트림 보기](#)
- [Amazon CloudWatch 경보 생성](#)
- [S3 액세스 로그에 Amazon S3 API 호출 로깅](#)
- [혼동된 대리자 문제를 제한하는 예](#)
- [CloudWatch Transfer Family의 로그 구조](#)
- [CloudWatch 로그 항목 예](#)
- [Transfer Family에 대한 CloudWatch 지표 사용](#)
- [AWS 사용자 알림 와 함께 사용 AWS Transfer Family](#)

서버에 대한 로깅 생성, 업데이트 및 보기

모든 AWS Transfer Family 서버의 경우 로깅을 위한 두 가지 옵션, 즉 LoggingRole (서버에 연결된 워크플로 로깅에 사용됨) 또는 중에서 선택할 수 있습니다 StructuredLogDestinations. StructuredLogDestinations 사용의 이점은 다음과 같습니다.

- 구조화된 JSON 형식으로 로그를 수신합니다.

- JSON 형식이 지정된 필드를 자동으로 검색하는 Amazon CloudWatch Logs Insights를 사용하여 로그를 쿼리합니다.
- AWS Transfer Family 리소스 간에 로그 그룹을 공유하면 여러 서버의 로그 스트림을 단일 로그 그룹으로 결합하여 모니터링 구성 및 로그 보존 설정을 더 쉽게 관리할 수 있습니다.
- 대시보드에 추가할 수 있는 집계된 지표 및 시각화를 CloudWatch 생성합니다.
- 로그 그룹을 사용하여 통합된 로그 지표, 시각화 및 대시보드를 생성하여 사용량 및 성능 데이터를 추적할 수 있습니다.

LoggingRole 또는 StructuredLogDestinations에 대한 옵션은 개별적으로 구성 및 제어됩니다. 각 서버에 대해 하나 또는 두 가지 로깅 방법을 모두 설정하거나, 로깅이 전혀 없도록 서버를 구성할 수 있습니다(권장되지는 않음).

Transfer Family 콘솔을 사용하여 새 서버를 생성할 경우 기본값으로 로깅이 활성화됩니다. 서버를 생성한 후 UpdateServer API 호출을 사용하여 로깅 구성을 변경할 수 있습니다. 자세한 내용은 섹션을 참조하세요 [StructuredLogDestinations](#).

현재 워크플로의 경우 로깅을 활성화하려면 로깅 역할을 지정해야 합니다.

- CreateServer 또는 UpdateServer API 호출을 사용하여 워크플로를 서버에 연결하면 시스템에서 로깅 역할을 자동으로 생성하지 않습니다. 워크플로 이벤트를 기록하려면 서버에 로깅 역할을 명시적으로 연결해야 합니다.
- Transfer Family 콘솔을 사용하여 서버를 생성하고 워크플로를 연결하는 경우 이름에 서버 ID가 포함된 로그 그룹에 로그가 전송됩니다. 형식은 /aws/transfer/*server-id*이며, 예를 들면 /aws/transfer/s-1111aaaa2222bbbb3와 같습니다. 서버 로그는 동일한 로그 그룹이나 다른 로그 그룹으로 전송될 수 있습니다.

콘솔에서 서버를 만들고 편집할 때 고려할 로깅 고려 사항

- 콘솔을 통해 생성된 새 서버는 워크플로가 서버에 연결되어 있지 않은 한 구조화된 JSON 로깅만 지원됩니다.
- 콘솔에서 새로 만든 서버의 경우 로깅 없음을 선택할 수 없습니다.
- 기존 서버는 콘솔을 통해 언제든지 구조화된 JSON 로깅을 활성화할 수 있습니다.
- 콘솔을 통해 구조화된 JSON 로깅을 활성화하면 기존 로깅 메서드가 비활성화되어 고객에게 요금이 두 배로 청구되지 않습니다. 단, 워크플로가 서버에 연결된 경우는 예외입니다.
- 구조화된 JSON 로깅을 활성화한 경우 나중에 콘솔을 통해 비활성화할 수 없습니다.
- 구조화된 JSON 로깅을 활성화하면 콘솔을 통해 언제든지 로그 그룹 대상을 변경할 수 있습니다.

- 구조화된 JSON 로깅을 활성화한 경우 를 통해 두 로깅 유형을 모두 활성화한 경우 콘솔을 통해 로깅 역할을 편집할 수 없습니다API. 단, 워크플로가 서버에 연결된 경우는 예외입니다. 하지만 로깅 역할은 추가 세부 정보에 계속 표시됩니다.

API 또는 를 사용하여 서버를 생성하고 편집하기 위한 로깅 고려 사항 SDK

- 를 통해 새 서버를 생성하는 경우 로깅 유형 중 하나 또는 둘 다를 구성하거나 로깅 없음을 선택할 API수 있습니다.
- 기존 서버의 경우 언제든지 구조화된 JSON 로깅을 활성화 및 비활성화합니다.
- API 언제든지 를 통해 로그 그룹을 변경할 수 있습니다.
- API 언제든지 를 통해 로깅 역할을 변경할 수 있습니다.

구조적 로깅을 활성화하려면 다음 권한이 있는 계정에 로그인해야 합니다

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs>ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

정책 예제는 단원에서 확인할 수 있습니다 [CloudWatch 로깅 역할 구성](#).

주제

- [서버에 대한 로깅 생성](#)
- [서버의 로깅 업데이트](#)
- [서버 구성 보기](#)

서버에 대한 로깅 생성

새 서버를 만들 때 추가 세부 정보 구성 페이지에서 기존 로그 그룹을 지정하거나 새 로그 그룹을 만들 수 있습니다.

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Info Logging role is only required when selecting a workflow in the Managed workflows section below.

기존 로그 그룹을 선택하는 경우와 연결된 로그 그룹을 선택해야 합니다 AWS 계정.

Transfer Family > Servers > Create server

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

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Info Logging role is only required when selecting a workflow in the Managed workflows section below.

로그 그룹 생성을 선택하면 CloudWatch 콘솔(<https://console.aws.amazon.com/cloudwatch/>)이 로그 그룹 생성 페이지로 열립니다. 자세한 내용은 [로그에서 CloudWatch 로그 그룹 생성을 참조하세요](#).

서버의 로깅 업데이트

로깅 세부 정보는 업데이트 시나리오에 따라 다릅니다.

Note

구조화된 JSON 로깅을 선택하면 Transfer Family가 이전 형식으로 로깅을 중지하지만 새 JSON 형식으로 로깅을 시작하는 데 약간의 시간이 걸리는 지연이 발생할 수 있습니다. 이로 인해 이벤트가 로그되지 않을 수 있습니다. 서비스 중단은 없겠지만 로깅 방법을 변경한 후 처음 1시간 동안은 로그가 삭제될 수 있으므로 파일 전송에 주의해야 합니다.

기존 서버를 편집하는 경우 옵션은 서버 상태에 따라 달라집니다.

- 서버에는 이미 로깅 역할이 활성화되어 있지만 구조화된 JSON 로깅이 활성화되어 있지 않습니다.

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

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

i Workflows events will be delivered to a log group labelled with the server ID.

- 서버에 로깅이 활성화되지 않았습니다.

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 ▼



i Logging role is only required when selecting a workflow in the Managed workflows section below.

- 서버에 이미 구조화된 JSON 로깅이 활성화되어 있지만 로깅 역할이 지정되지 않았습니다.

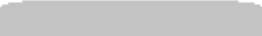
Edit additional details

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 ▼



i Logging role is only required when selecting a workflow in the Managed workflows section below.

- 서버에 이미 구조화된 JSON 로깅이 활성화되어 있고 로깅 역할도 지정되어 있습니다.

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/s- [redacted] ▼



Create 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.

서버 구성 보기

서버 구성 페이지의 세부 정보는 시나리오에 따라 다릅니다.

시나리오에 따라 서버 구성 페이지는 다음 예 중 하나와 비슷할 수 있습니다.

- 로깅이 활성화되지 않았습니다.

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] [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- 구조화된 JSON 로깅이 활성화되었습니다.

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] [REDACTED]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- 로깅 역할이 활성화되었지만 구조화된 JSON 로깅은 활성화되지 않았습니다.

Additional details

Edit

Log group
-

Logging role [Info](#)
AWSTransferLoggingAccess [🔗](#)

Server host key [Info](#)
SHA256:lx39/[REDACTED]
[REDACTED]

Security Policy [Info](#)
TransferSecurityPolicy-2018-11

Domain
Amazon S3

Workflow for complete uploads
w-[REDACTED]

Workflow for partial uploads
-

Managed workflows execution role
[REDACTED]execution-role[REDACTED] [🔗](#)

Login display banner
[View the display message](#)

SetStat option
Ignore

TLS session resumption
-

Passive IP
-

- 두 가지 유형의 로깅(로깅 역할 및 구조화된 JSON 로깅)이 모두 활성화됩니다.

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 -

워크플로에 대한 로깅 관리

CloudWatch 는 워크플로 진행 상황 및 결과에 대한 통합 감사 및 로깅을 제공합니다. 또한 워크플로에 대한 여러 지표를 AWS Transfer Family 제공합니다. 이전 1분 간 시작, 성공적으로 완료, 및 실패한 워크플로 실행 수에 대한 지표를 볼 수 있습니다. Transfer Family에 대한 모든 CloudWatch 지표는 에 설명되어 있습니다 [Transfer Family에 대한 CloudWatch 지표 사용](#).

워크플로에 대한 Amazon CloudWatch 로그 보기

- 에서 Amazon CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
- 왼쪽 탐색 창에서 로그를 선택한 다음, 로그 그룹을 선택합니다.
- 로그 그룹 페이지의 탐색 모음에서 AWS Transfer Family 서버에 적합한 리전을 선택합니다.
- 서버에 해당하는 로그 그룹을 선택합니다.

예를 들어 서버 ID가 s-1234567890abcdef0인 경우 로그 그룹은 /aws/transfer/s-1234567890abcdef0입니다.

- 서버의 로그 그룹 세부 정보 페이지에는 가장 최근의 로그 스트림이 표시됩니다. 탐색 중인 사용자에 대한 로그 스트림은 두 가지입니다.
 - 각 Secure Shell(SSH) 파일 전송 프로토콜(SFTP) 세션당 1개.
 - 서버에서 실행 중인 워크플로의 로그 스트림 워크플로의 로그 스트림 형식은 `username.workflowID.uniqueStreamSuffix`입니다.

예를 들어 사용자가 mary-major이면 다음과 같은 로그 스트림이 있습니다.

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

이 예에 나열된 16자리 영숫자 식별자는 가상의 식별자입니다. Amazon에 표시되는 값은 CloudWatch 다릅니다.

mary-major-usa-east.1234567890abcdef0의 로그 이벤트 페이지에는 각 사용자 세션의 세부 정보가 표시되고 mary.w-abcdef01234567890.021345abcdef6789 로그 스트림에는 워크플로에 대한 세부 정보가 포함됩니다.

다음은 복사 단계가 포함된 워크플로(w-abcdef01234567890)를 기반으로 하는 mary.w-abcdef01234567890.021345abcdef6789의 샘플 로그 스트림입니다.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "DOC-EXAMPLE-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": "DOC-EXAMPLE-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 로깅 역할 구성

액세스를 설정하려면 리소스 기반 IAM 정책과 해당 액세스 정보를 제공하는 IAM 역할을 생성합니다.

Amazon CloudWatch 로깅을 활성화하려면 로깅을 활성화 CloudWatch하는 IAM 정책을 생성하는 것으로 시작합니다. 그런 다음 IAM 역할을 생성하고 정책을 연결합니다. 이렇게 하려면 [서버를 생성](#)하거나 [기존 서버를 편집](#)해야 합니다. 에 대한 자세한 내용은 [Amazon 사용 설명서의 Amazon 이란 무엇입니까 CloudWatch?](#) 및 [Amazon CloudWatch 로그란 무엇입니까?](#)를 CloudWatch참조하세요.

CloudWatch

다음 예제 IAM 정책을 사용하여 CloudWatch 로깅을 허용합니다.

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": "arn:aws:logs:region-id:AWS ##:log-group:/aws/transfer/*"
  }
]
}

```

앞의 예제 정책에서 `에` 대해 `Resource`바꿉니다.*region-id* 그리고 *AWS ##* 값을 사용합니다. 예제: **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

그런 다음 역할을 생성하고 생성한 CloudWatch 로그 정책을 연결합니다.

IAM 역할을 생성하고 정책을 연결하려면

1. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.

역할 생성 페이지에서 AWS 서비스가 선택되어 있는지 확인합니다.

2. 서비스 목록에서 전송을 선택하고, 다음: 권한을 선택합니다. 이렇게 하면 AWS Transfer Family 및 IAM 역할 간에 신뢰 관계가 설정됩니다. 또한 `aws:SourceAccount` 및 `aws:SourceArn` 조건 키를 추가하여 혼동되는 부정 문제로부터 자신을 보호하세요. 자세한 설명은 다음 설명서를 참조하세요:

- 와 신뢰 관계를 설정하는 절차 AWS Transfer Family: [신뢰 관계를 구축하기 위해](#)
- 혼동된 대리인 문제에 대한 설명: [혼동된 대리인 문제](#)

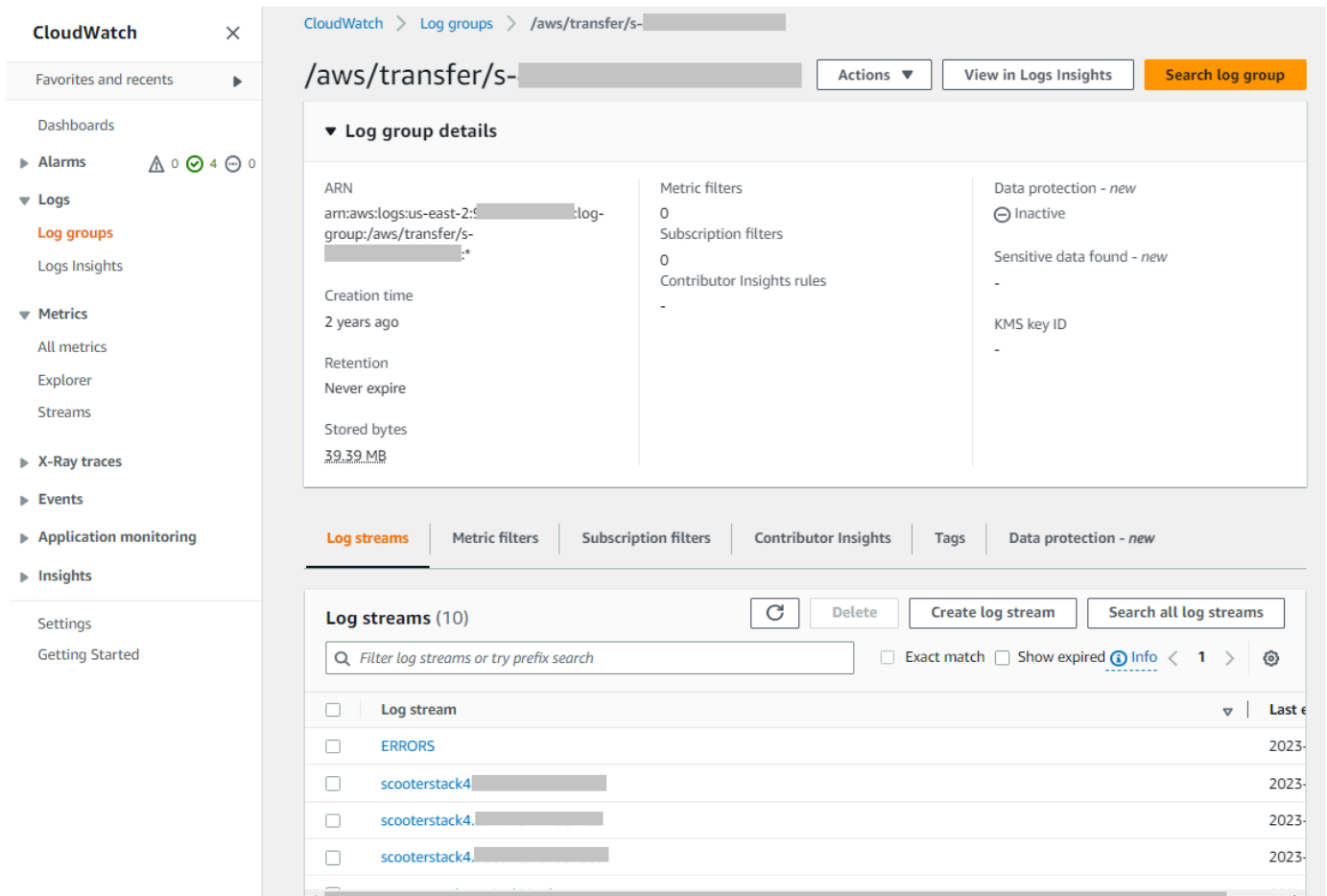
3. 권한 정책 연결 섹션에서 방금 생성한 CloudWatch 로그 정책을 찾아 선택하고 다음: 태그 를 선택합니다.
4. (옵션) 태그의 키와 값을 입력하고 다음: 검토를 선택합니다.
5. 검토 페이지에 새 역할의 명칭과 설명을 입력한 다음 역할 생성을 선택합니다.
6. 로그를 보려면 Server ID(서버 ID)를 선택하여 서버 구성 페이지를 열고 로그 보기를 선택합니다. 로그 스트림을 볼 수 있는 CloudWatch 콘솔로 리디렉션됩니다.

서버의 CloudWatch 페이지에서 사용자 인증(성공 및 실패), 데이터 업로드(PUT 작업) 및 데이터 다운로드(GET 작업)에 대한 레코드를 볼 수 있습니다.

Transfer Family 로그 스트림 보기

Transfer Family 서버 로그를 보려면

1. 서버의 세부 정보 페이지로 이동합니다.
2. 로그 보기를 선택합니다. 그러면 Amazon 가 열립니다 CloudWatch.
3. 선택한 서버의 로그 그룹이 표시됩니다.



4. 로그 스트림을 선택하여 스트림의 세부 정보 및 개별 항목을 표시할 수 있습니다.
 - 에 대한 목록이 있는 경우 ERRORS를 선택하여 서버의 최신 오류에 대한 세부 정보를 볼 수 있습니다.

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](#)

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=

- 예 로그 스트림을 보려면 다른 항목을 선택하세요.

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](#)

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	

- 서버에 연결된 관리형 워크플로가 있는 경우 워크플로 실행에 대한 로그를 볼 수 있습니다.

Note

워크플로의 로그 스트림 형식은 `username.workflowId.uniqueStreamSuffix`입니다. 예를 들어 `decrypt-user.w-a1111222233334444.aa1111bb2222`는 사용자 **decrypt-user** 및 워크플로 **w-a1111222233334444**의 로그 스트림 명칭일 수 있습니다.

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](#)

Filter events: Clear 1m 30m 1h 12h Custom

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-user/test.json.gpg", "versionId": "...", "etag": "..."
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": {}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-..."

Note

확장된 로그 항목의 경우 복사를 선택하여 항목을 클립보드에 복사할 수 있습니다. CloudWatch 로그에 대한 자세한 내용은 [로그 데이터 보기를 참조하세요](#).

Amazon CloudWatch 경보 생성

다음 예제에서는 AWS Transfer Family 지표 를 사용하여 Amazon CloudWatch 경보를 생성하는 방법을 보여줍니다FilesIn.

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,
});
```

AWS 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
```

S3 액세스 로그에 Amazon S3 API 호출 로깅

[Amazon S3 액세스 로그를 사용하여 파일 전송 사용자를 대신하여 수행된 S3 요청을 식별하는](#) 경우 RoleSessionName는 파일 전송을 서비스하는 IAM 역할을 표시하는 데 사용됩니다. 또한 전송에

사용된 사용자 이름, 세션 ID, 서버 ID와 같은 추가 정보도 표시됩니다. 형식은 [AWS:Role Unique Identifier]/username.sessionid@server-id(이)며, 요청자 필드에 포함되어 있습니다. 예를 들어, 다음은 S3 버킷으로 복사된 파일에 대한 S3 액세스 로그의 샘플 요청자 필드 콘텐츠입니다.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

위의 요청자 필드에는 라는 IAM 역할이 표시됩니다IamRoleName. IAM 역할 고유 식별자에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [고유 식별자](#)를 참조하세요.

혼동된 대리자 문제를 제한하는 예

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 서비스 AWS간 사칭은 혼동된 대리자 문제를 초래할 수 있습니다. 자세한 내용은 [교차 서비스 혼동된 대리인 방지](#)를 참조하세요.

Note

다음 예에서는 각각을 바꿉니다.*user input placeholder* 자신의 정보를 사용합니다. 이 예제에서는 서버에 연결된 워크플로가 없는 경우 워크플로의 ARN 세부 정보를 제거할 수 있습니다.

다음 로깅/인보이스 정책 예제에서는 계정의 모든 서버(및 워크플로)가 역할을 수임하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": [
```

```

        "arn:aws:transfer:region:account-id:server/*",
        "arn:aws:transfer:region:account-id:workflow/*"
    ]
}
}
}
]
}

```

다음 예제 로깅/인보이스 정책을 통해 특정 서버(및 워크플로)가 역할을 수입할 수 있습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:region:account-id:server/server-id",
            "arn:aws:transfer:region:account-id:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}

```

CloudWatch Transfer Family의 로그 구조

이 항목에서는 Transfer Family 로그에 입력되는 필드 (JSON 구조화된 로그 항목과 기존 로그 항목 모두에 대해)에 대해 설명합니다.

주제

- [Transfer Family를 위한 JSON 구조화된 로그](#)
- [Transfer Family의 레거시 로그](#)

Transfer Family를 위한 JSON 구조화된 로그

다음 표에는 새로운 JSON 구조 로그 형식의 Transfer Family SFTP/FTP/FTPS 작업에 대한 로그 입력 필드에 대한 세부 정보가 포함되어 있습니다.

필드	설명	입력 예
activity-type	The action by the user	열기 닫기 부분_닫기 연결 끊김 연결됨
bytes-in	Number of bytes uploaded by the user	29238420042
bytes-out	Number of bytes downloaded by the user	23094032490328
ciphers	Specifies the SSH cipher negotiated for the connection (available ciphers are listed in 암호화 알고리즘)	aes256-gcm@openssh.com
client	The user's client software	SSH-2.0-OpenSSH_7.4
home-dir	The directory that the end user lands on when they connect to the endpoint if their home directory type is PATH: if they have a logical home directory, this value is always /	/user-home-bucket/test
kex	Specifies the negotiated SSH key exchange (KEX) for the connection (available KEX are listed in 암호화 알고리즘)	diffie-hellman-group14-sha256

필드	설명	입력 예
message	Provides more information related to the error	<i><string></i>
method	The authentication method	publickey
mode	Specifies how a client opens a file	CREATE TRUNCATE WRITE
operation	The client operation on a file	OPEN CLOSE
path	Actual file path affected	/user-test-bucket/test-file-1.pdf
resource-arn	A system-assigned, unique identifier for a specific resource (for example, a server)	arn:aws:transfer:ap-northeast-1:12346789012:서버/s-1234567890 akeu2js2
role	The IAM role of the user	arn:aws:iam: :0293883675: 역할/테스트 사용자 역할
session-id	A system-assigned, unique identifier for a single session	9ca9a0e1cec6ad9d
source-ip	Client IP address	18.323.0.129
user	The end user's username	myname192
user-policy	The permissions specified for the end user: this field is populated if the user's policy is a session policy.	The JSON code for the session policy that is being used

Transfer Family의 레거시 로그

다음 표에는 다양한 Transfer Family 작업에 대한 로그 항목의 세부 정보가 나와 있습니다.

Note

이러한 항목은 새로운 JSON 구조화된 로그 형식이 아닙니다.

다음 표에는 다양한 Transfer Family 작업에 대한 로그 항목의 세부 정보가 새로운 JSON 구조 로그 형식으로 포함되어 있습니다.

작업	Amazon 로그 내의 해당 CloudWatch 로그
인증 실패 횟수	ERRORS AUTH_FAILURE Method=publickey User=lhr Message="RSA SHA256:Lfz3R2nmLY4raK+b7Rb1rSvUIbAE+a+Hxg0c7l1JIZ0" SourceIP=3.8.172.211
복사/태그 지정/삭제/복호화 워크플로우	{"유형": "StepStarted", "세부 정보": {"입력": {"파일 위치": {"백업 저장소": "EFS", "파일 시스템 ID": "fs-12345678", "경로": "/lhr/regex.py"}}, "단계 유형": "태그", "단계 이름": "성공_태그_단계"}, "워크플로 ID": "w-1111aaaa22bbbb3", "실행 ID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "전송 세부 정보": {"서버 ID": "s-1234abcd5678efghi", "사용자 이름": "lhr", "세션 ID": "1234567890 abcdef0"}}
맞춤 단계 워크플로우	{"유형": "CustomStepInvoked", "세부 정보": {"출력": {"토큰": "MZM4MJG5YWUTYT EzMy 00 Yjlz LWI3OG MtYz U4OGI2 ZjQyMz E5"}, "단계 유형": "사용자 정의", "단계 이름": "efs-s3_copy_2"}, "워크플로우 ID": "w-9283e49d33297c3f7", "실행 ID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "전송 세부 정보": {"서버 ID": "s-zzzz11aaaa22223", "사용자 이름": "lhr", "세션 ID": "1234567890abcdef0"}}
삭제	lhr.33a8fb495ffb383b DELETE Path=/bucket/user/123.jpg

작업	Amazon 로그 내의 해당 CloudWatch 로그
다운로드	lhr.33a8fb495ffb383b OPEN Path=/bucket/user/123.jpg Mode=READ llhr.33a8fb495ffb383b 닫기 경로=/버킷/사용자/123.jpg BytesOut =3618546
로그인/로그아웃	사용자.914984e553bcddb6 커넥티드 소스 IP=1.22.111.222 사용자=LHR =논리적 클라이언트=SSH-2.0-openssh_7.4 역할=arn:AWS:iam: :123456789012:role/sftp-s3-access HomeDir user.914984e553bcddb6 DISCONNECTED
명칭 바꾸기	lhr.33a8fb495ffb383b 이름 바꾸기 경로=/버킷/사용자/Lambo.png =/버킷/사용자/페라리.png NewPath
샘플 워크플로우 오류 로그	<pre>{ "type": " ", "details": { "오류 유형": "StepErrored", "BAD_REQUEST", "오류 메시지": "Ef 파일에 태그를 지정할 수 없음", "단계 유형": "TAG", "단계 이름": "성공_tag_step", "워크플로 ID": "w-1234abcd5678efghi", "실행 ID": "실행 ID: 81234abcd-1234-efgh-5678-ijklmnopqr90", "전송 세부 정보": { "서버 ID": "s-1234abcd5678efghi", "사용자 이름": "lhr", "세션 ID": "1234567890abcdef0" } } }</pre>
Symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK LinkPath =/fs-12345678/lhr/pqr.jpg TargetPath =abc.jpg
업로드	lhr.33a8fb495ffb383b OPEN Path=/bucket/user/123.jpg Mode=CREATE TRUNCATE WRITE lhr.33a8fb495ffb383b 닫기 경로=/버킷/사용자/123.jpg =3618546 BytesIn

작업	Amazon 로그 내의 해당 CloudWatch 로그
워크플로	<pre>{ "유형": " ", "세부 정보": { "입력": { "Execution Started ": { "백업 스토어": "EFS", "파일 시스템 ID": "fs-12345678", "initialFileLocation 경로": "/lhr/regex.py" } }, "워크플로 ID": "w-1111aa22bb3", "실행 ID": "1234abcd-12cd-127"4-efgh-5678-ijklmnopqr90", "전송 세부 정보": { "서버 ID": "s-zzzz11aaaa2223", "사용자 이름": "lhr", "세션 ID": "1234567890abcdef0" } } }</pre> <pre>{ "유형": " StepStarted ", "세부 정보": { "입력": { "파일 위치": { "백업 저장소": "EFS", "파일 시스템 ID": "fs-12345678", "경로": "/lhr/regex.py" } }, "단계 유형": "사용자 지정", "단계 이름": "efs-s3_copy_2", "워크플로우 ID": "w-9283e49d33297c3f7", "실행 ID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "전송 세부 정보": { "서버 ID": "s-18ca49dce5d842e0b", "사용자 이름": "lhr", "세션 ID": "1234567890abcdef0" } } }</pre>

CloudWatch 로그 항목 예

이 주제에서는 로그 항목의 예를 보여줍니다.

주제

- [전송 세션 로그 항목의 예](#)
- [SFTP 커넥터의 로그 항목 예](#)
- [키 교환 알고리즘 실패에 대한 로그 항목의 예](#)

전송 세션 로그 항목의 예

이 예제에서는 SFTP 사용자가 Transfer Family 서버에 연결하고 파일을 업로드한 다음 세션에서 연결을 끊습니다.

다음 로그 항목은 Transfer Family 서버에 연결하는 SFTP 사용자를 반영합니다.

```
{
  "role": "arn:aws:iam::500655546075:role/scooter-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": "/scooter-test/log-me",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

다음 로그 항목은 Amazon S3 버킷에 파일을 업로드하는 SFTP 사용자를 반영합니다.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/scooter-test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

다음 로그 항목은 SFTP 사용자의 SFTP 세션 연결을 끊는 사용자를 반영합니다. 먼저 클라이언트가 버킷에 대한 연결을 종료한 다음 클라이언트가 SFTP 세션 연결을 끊습니다.

```
{
  "path": "/scooter-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"
}
```

}

SFTP 커넥터의 로그 항목 예

이 섹션에는 성공적인 전송과 실패한 전송 모두에 대한 예제 로그가 포함되어 있습니다. 로그는 라는 로그 그룹에 생성됩니다/aws/transfer/*connector-id*. 여기서 *connector-id* 는 SFTP 커넥터의 식별자입니다.

Note

SFTP 커넥터의 로그 항목은 StartFileTransfer 명령을 실행할 때만 생성됩니다.

이 로그 항목은 성공적으로 완료된 전송을 위한 것입니다.

```
{
  "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-1:480351544584:connector/connector-id",
  "local-directory-path": "/connectors-localbucket"
}
```

이 로그 항목은 시간이 초과되어 성공적으로 완료되지 않은 전송을 위한 것입니다.

```
{
  "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-1:480351544584:connector/connector-id",
    "local-directory-path": "/connectors-localbucket"
  }

```

이전 로그 예제의 일부 키 필드에 대한 설명입니다.

- `timestamp` 는 로그가 에 추가되는 시기를 나타냅니다 CloudWatch. `start-time` 는 커넥터가 실제로 전송을 시작하고 완료하는 시기를 `end-time` 나타냅니다.
- `transfer-id` 는 각 `start-file-transfer` 요청에 할당된 고유 식별자입니다. 사용자가 한 번의 `start-file-transfer` API 호출로 여러 파일 경로를 전달하는 경우 모든 파일은 동일한 를 공유합니다 `transfer-id`.
- `file-transfer-id` 는 전송된 각 파일에 대해 생성된 고유한 값입니다. 의 초기 부분은 와 `file-transfer-id` 동일합니다 `transfer-id`.

키 교환 알고리즘 실패에 대한 로그 항목의 예

이 섹션에는 키 교환 알고리즘(KEX)이 실패한 예제 로그가 포함되어 있습니다. 다음은 구조화된 ERRORS 로그에 대한 로그 스트림의 예입니다.

이 로그 항목은 호스트 키 유형 오류가 있는 예제입니다.

```

{
  "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"
}

```

이 로그 항목은 KEX 불일치가 있는 예제입니다.

```

{
  "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"
}

```

Transfer Family에 대한 CloudWatch 지표 사용

Note

Transfer Family 콘솔 자체에서도 Transfer Family에 대한 지표를 가져올 수 있습니다. 자세한 내용은 [콘솔 내 사용량 모니터링](#)을 참조하세요.

CloudWatch 지표를 사용하여 서버에 대한 정보를 가져올 수 있습니다. 지표는 에 게시되는 시간 순서의 데이터 포인트 집합을 나타냅니다 CloudWatch. 지표를 사용할 때는 Transfer Family 네임스페이스, 지표 명칭 및 [차원](#)을 지정해야 합니다. 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [지표](#)를 참조하세요.

다음 표에서는 Transfer Family에 대한 CloudWatch 지표를 설명합니다.

네임스페이스	지표	설명
AWS/Transfer	BytesIn	서버로 전송된 총 바이트 수. 단위: 개 기간: 5분
	BytesOut	서버에서 전송된 총 바이트 수입니다. 단위: 개 기간: 5분
	FilesIn	서버로 전송된 총 파일 수. AS2 프로토콜을 사용하는 서버의 경우 이 지표는 수신된 메시지 수를 나타냅니다.

네임스페이스	지표	설명
		단위: 개 기간: 5분
	FilesOut	서버에서 전송된 총 파일 수. 단위: 개 기간: 5분
	InboundMessage	거래 파트너로부터 성공적으로 수신된 총 AS2 메시지 수입니다. 단위: 개 기간: 5분
	InboundFailedMessage	거래 파트너로부터 수신하지 못한 총 AS2 메시지 수입니다. 즉, 거래 파트너가 메시지를 보냈지만 Transfer Family 서버가 메시지를 성공적으로 처리하지 못했습니다. 단위: 개 기간: 5분
	OnPartialUploadExecutionsStarted	서버에서 시작된 총 워크플로 실행 수 on-partial-upload입니다. 단위: 개 기간: 1분
	OnPartialUploadExecutionsSuccess	서버에서 성공 on-partial-upload한 총 워크플로 실행 수입니다. 단위: 개 기간: 1분

네임스페이스	지표	설명
	OnPartialUploadExecutionsFailed	서버에서 실패한 on-partial-upload 총 워크플로 실행 수입니다. 단위: 개 기간: 1분
	OnUploadExecutionsStarted	서버에서 시작된 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분
	OnUploadExecutionsSuccess	서버에서 성공적인 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분
	OnUploadExecutionsFailed	서버에서 실패한 워크플로를 실행한 총 횟수. 단위: 개 기간: 1분

Transfer Family 크기

차원은 지표의 보안 인증에 속하는 명칭/값 쌍입니다. 차원에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [차원](#)을 참조하세요.

다음 표에서는 Transfer Family의 CloudWatch 차원을 설명합니다.

측정기준	설명
ServerId	사용자의 고유 ID입니다.

AWS 사용자 알림 와 함께 사용 AWS Transfer Family

AWS Transfer Family 이벤트에 대한 알림을 받으려면 [AWS 사용자 알림](#)를 사용하여 다양한 전송 채널을 설정할 수 있습니다. 이벤트가 지정한 규칙과 일치하면 알림을 받습니다.

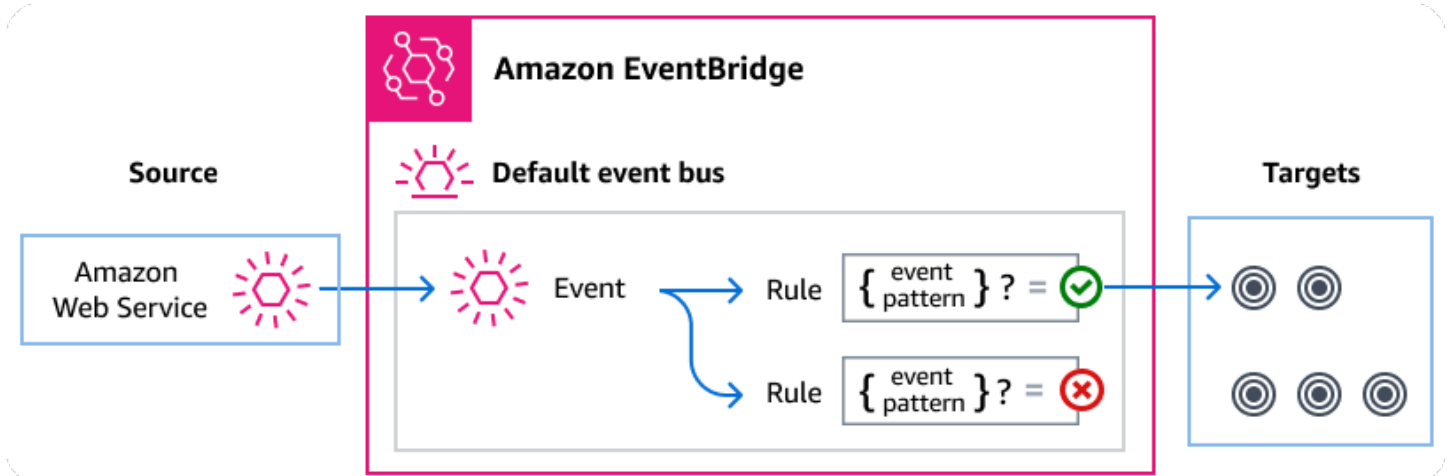
이메일, [채팅 애플리케이션 내 Amazon Q Developer](#) 채팅 알림 또는 [AWS Console Mobile Application](#) 푸시 알림을 비롯한 여러 채널을 통해 이벤트에 대한 알림을 받을 수 있습니다. [콘솔 알림 센터에서도 알림을 볼 수 있습니다](#). 사용자 알림 는 집계를 지원하므로 특정 이벤트 중에 수신하는 알림 수를 줄일 수 있습니다.

자세한 내용은 AWS 사용자 알림 사용 설명서의 [AWS Transfer Family 관리형 워크플로 블로그 게시물](#)을 사용하여 파일 전송 알림 사용자 지정 및 [란 무엇입니까 AWS 사용자 알림?](#)를 참조하세요.

를 사용하여 Transfer Family 이벤트 관리 Amazon EventBridge

Amazon EventBridge 는 이벤트를 사용하여 애플리케이션 구성 요소를 함께 연결하는 서버리스 서비스로, 확장 가능한 이벤트 기반 애플리케이션을 더 쉽게 구축할 수 있습니다. 이벤트 기반 아키텍처는 이벤트를 내보내고 대응하여 함께 작동하는 느슨하게 결합된 소프트웨어 시스템을 구축하는 스타일입니다. 이벤트는 리소스나 환경의 변화를 나타냅니다.

많은 AWS 서비스와 마찬가지로 는 이벤트를 Transfer Family 생성하고 EventBridge 기본 이벤트 버스로 전송합니다. 기본 이벤트 버스는 모든 AWS 계정에 자동으로 프로비저닝됩니다. 이벤트 버스는 이벤트를 수신하여 0개 이상의 목적지 또는 대상에 전달하는 라우터입니다. 이벤트가 도착할 때 이벤트를 평가하는 이벤트 버스에 대한 규칙을 지정합니다. 각 규칙은 이벤트가 규칙의 이벤트 패턴과 일치하는지 여부를 확인합니다. 이벤트가 일치하는 경우 이벤트 버스는 이벤트를 하나 이상의 지정된 대상으로 보냅니다.



주제

- [Transfer Family 이벤트](#)
- [EventBridge 규칙을 사용하여 Transfer Family 이벤트 전송](#)
- [Amazon EventBridge 권한](#)
- [추가 EventBridge 리소스](#)
- [Transfer Family 이벤트 세부 정보 참조](#)

Transfer Family 이벤트

Transfer Family 는 이벤트를 기본 이벤트 EventBridge 버스로 자동으로 전송합니다. 각 규칙에 이벤트 패턴과 하나 이상의 대상이 포함된 이벤트 버스에 규칙을 생성할 수 있습니다. 규칙의 이벤트 패턴과 일치하는 이벤트는 지정된 대상으로 [최선의 노력을 기울여](#) 전달되지만 일부 이벤트는 순서대로 전달되지 않을 수 있습니다.

다음 이벤트는 에서 생성됩니다 Transfer Family. 자세한 내용은 Amazon EventBridge 사용 설명서의 [EventBridge 이벤트를](#) 참조하세요.

SFTP, FTPS 및 FTP 서버 이벤트

이벤트 세부 정보 유형	설명
FTP 파일 서버 다운로드 완료	FTP 프로토콜에 대한 파일이 성공적으로 다운로드되었습니다.
FTP 파일 서버 다운로드 실패	FTP 프로토콜에 대한 파일 다운로드 시도가 실패했습니다.
FTP 파일 서버 업로드 완료	FTP 프로토콜에 대한 파일이 성공적으로 업로드되었습니다.
FTP 파일 서버 업로드 실패	FTP 프로토콜에 대한 파일 업로드 시도가 실패했습니다.
FTPS 파일 서버 다운로드 완료	FTPS 프로토콜에 대한 파일이 성공적으로 다운로드되었습니다.
FTPS 파일 서버 다운로드 실패	FTPS 프로토콜에 대한 파일 다운로드 시도가 실패했습니다.
FTPS 파일 서버 업로드 완료	FTPS 프로토콜에 대한 파일이 성공적으로 업로드되었습니다.
FTPS 파일 서버 업로드 실패	FTPS 프로토콜에 대한 파일 업로드 시도가 실패했습니다.
SFTP 서버 파일 다운로드 완료	SFTP 프로토콜에 대한 파일이 성공적으로 다운로드되었습니다.
SFTP 서버 파일 다운로드 실패	SFTP 프로토콜에 대한 파일 다운로드 시도가 실패했습니다.
SFTP 서버 파일 업로드 완료	SFTP 프로토콜에 대한 파일이 성공적으로 업로드되었습니다.
SFTP 서버 파일 업로드 실패	SFTP 프로토콜에 대한 파일 업로드 시도가 실패했습니다.

SFTP 커넥터 이벤트

이벤트 세부 정보 유형	설명
SFTP 커넥터 파일 전송 완료	커넥터에서 원격 SFTP 서버로의 파일 전송이 성공적으로 완료되었습니다.
SFTP 커넥터 파일 전송 실패	커넥터에서 원격 SFTP 서버로의 파일 전송이 실패했습니다.
SFTP 커넥터 파일 검색 완료	원격 SFTP 서버에서 커넥터로의 파일 전송이 성공적으로 완료되었습니다.
SFTP 커넥터 파일 검색 실패	원격 SFTP 서버에서 커넥터로의 파일 전송이 실패했습니다.

A2S 이벤트

이벤트 세부 정보 유형	설명
AS2 페이로드 수신 완료	AS2 메시지의 페이로드를 수신했습니다.
AS2 페이로드 수신 실패	AS2 메시지의 페이로드를 수신하지 못했습니다.
AS2 페이로드 전송 완료	AS2 메시지의 페이로드가 성공적으로 전송되었습니다.
AS2 페이로드 전송 실패	AS2 메시지의 페이로드가 전송되지 않았습니다.
AS2 MDN 수신 완료	메시지에 대한 AS2 메시지 처리 알림이 수신되었습니다.
AS2 MDN 수신 실패	메시지에 대한 AS2 메시지 처리 알림이 수신되지 않았습니다.
AS2 MDN 전송 완료	메시지에 대한 AS2 메시지 처리 알림이 성공적으로 전송되었습니다.
AS2 MDN 전송 실패	메시지에 대한 AS2 메시지 처리 알림이 전송되지 않았습니다.

EventBridge 규칙을 사용하여 Transfer Family 이벤트 전송

EventBridge 기본 이벤트 버스가 대상에 Transfer Family 이벤트를 보내도록 하려면 원하는 이벤트의 데이터와 일치하는 이벤트 패턴이 포함된 규칙을 생성해야 합니다 Transfer Family .

다음 일반 단계에 따라 규칙을 생성할 수 있습니다.

1. 다음을 지정하는 규칙의 이벤트 패턴을 생성합니다.

- Transfer Family 는 규칙에 의해 평가되는 이벤트의 소스입니다.
- (선택 사항) 일치하는 기타 이벤트 데이터입니다.

자세한 내용은 [??? 단원](#)을 참조하십시오.

2. (선택 사항) 가 정보를 규칙의 대상으로 EventBridge 보내기 전에 이벤트의 데이터를 사용자 지정하는 입력 변환기를 생성합니다.

자세한 내용은 EventBridge 사용 설명서의 [입력 변환](#)을 참조하세요.

3. 이벤트 패턴과 일치하는 이벤트를 EventBridge 전달할 대상을 지정합니다.

대상은 다른 AWS 서비스, 서비스형 소프트웨어(SaaS) 애플리케이션, API 대상 또는 기타 사용자 지정 엔드포인트일 수 있습니다. 자세한 내용은 EventBridge 사용 설명서의 [대상](#)을 참조하세요.

이벤트 버스 규칙 생성에 대해 자세히 알아보려면 EventBridge 사용 설명서의 [이벤트에 대응하는 규칙 생성](#)을 참조하세요.

이벤트에 대한 Transfer Family 이벤트 패턴 생성

가 이벤트를 기본 이벤트 버스로 Transfer Family 전달하는 경우는 각 규칙에 대해 정의된 이벤트 패턴을 EventBridge 사용하여 이벤트를 규칙의 대상으로 전달해야 하는지 여부를 결정합니다. 이벤트 패턴이 원하는 Transfer Family 이벤트의 데이터와 일치합니다. 각 이벤트 패턴은 다음을 포함하는 JSON 객체입니다.

- 이벤트를 전송하는 서비스를 식별하는 source 속성입니다. Transfer Family 이벤트의 경우 소스는 `aws.transfer`입니다.
- (선택 사항) 일치시킬 이벤트 유형의 배열이 포함된 detail-type 속성입니다.
- (선택 사항) 일치시킬 다른 이벤트 데이터를 포함하는 detail 속성입니다.

예를 들어 다음 이벤트 패턴은 의 모든 이벤트와 일치합니다 Transfer Family.

```
{
  "source": ["aws.transfer"]
}
```

다음 이벤트 패턴 예제는 모든 SFTP 커넥터 이벤트와 일치합니다.

```
{
  "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"]
}
```

다음 이벤트 패턴 예제는 모든 Transfer Family 실패 이벤트와 일치합니다.

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

다음 이벤트 패턴 예제는 사용자의 성공적인 SFTP 다운로드와 일치합니다. *username*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

자세한 내용은 EventBridge 사용 설명서의 [이벤트 패턴](#)을 참조하세요.

의 이벤트에 대한 Transfer Family 이벤트 패턴 테스트 EventBridge

EventBridge 샌드박스를 사용하면 규칙을 생성하거나 편집하는 광범위한 프로세스를 완료할 필요 없이 이벤트 패턴을 빠르게 정의하고 테스트할 수 있습니다. 샌드박스를 사용하여 이벤트 패턴을 정의하고 샘플 이벤트를 사용하여 패턴이 원하는 이벤트와 일치하는지 확인할 수 있습니다. EventBridge 샌드박스에서 직접 해당 이벤트 패턴을 사용하여 새 규칙을 생성할 수 있는 옵션을 제공합니다.

자세한 내용은 EventBridge 사용 설명서 [의 EventBridge Sandbox를 사용하여 이벤트 패턴 테스트를 참조](#) 하세요.

Amazon EventBridge 권한

Transfer Family 에서는 이 이벤트를 전달하는 데 추가 권한이 필요하지 않습니다 Amazon EventBridge.

지정하는 대상에는 특정 권한 또는 구성이 필요할 수 있습니다. 대상에 특정 서비스를 사용하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 [Amazon EventBridge 대상](#)을 참조하세요.

추가 EventBridge 리소스

를 사용하여 이벤트를 처리하고 관리하는 방법에 대한 자세한 내용은 [Amazon EventBridge 사용 설명서](#)의 다음 주제를 참조 EventBridge 하세요.

- 이벤트 버스의 작동 방식에 대한 자세한 내용은 [Amazon EventBridge 이벤트 버스](#)를 참조하세요.
- 이벤트 구조에 대해 자세히 알아보려면 [이벤트](#)를 참조하세요.
- 이벤트를 규칙과 일치 EventBridge 시킬 때 사용할 의 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 [이벤트 패턴 단원](#)을 참조하세요.
- EventBridge 에서 처리하는 이벤트를 지정하는 규칙을 생성하는 방법에 대한 자세한 내용은 [규칙](#)을 참조하세요.
- 가 일치하는 이벤트를 EventBridge 보내는 서비스 또는 기타 대상을 지정하는 방법에 대한 자세한 내용은 [대상](#)을 참조하세요.

Transfer Family 이벤트 세부 정보 참조

AWS 서비스의 모든 이벤트에는 이벤트에 대한 메타데이터가 포함된 공통 필드 세트가 있습니다. 이러한 메타데이터에는 이벤트의 소스인 AWS 서비스, 이벤트가 생성된 시간, 이벤트가 발생한 계정 및 리전 등이 포함될 수 있습니다. 이러한 일반 필드에 대한 정의는 Amazon EventBridge 사용 설명서의 [이벤트 구조 참조](#)를 참조하세요.

또한 각 이벤트에는 해당 특정 이벤트와 관련된 데이터를 포함하는 detail 필드가 있습니다. 다음 참조에서는 다양한 Transfer Family 이벤트에 대한 세부 정보 필드를 정의합니다.

EventBridge 를 사용하여 Transfer Family 이벤트를 선택하고 관리할 때는 다음을 고려하세요.

- 의 모든 이벤트에 대한 source 필드는 로 Transfer Family 설정됩니다aws.transfer.
- detail-type 필드는 이벤트 유형을 지정합니다.

예: FTP File Server Download Completed.

- detail 필드는 해당 특정 이벤트와 관련된 데이터를 포함합니다.

Transfer Family 이벤트와 일치하는 규칙을 활성화하는 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 안내서의 [이벤트 패턴](#)을 참조하세요.

이벤트 및 이벤트 EventBridge 처리 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 [Amazon EventBridge 이벤트를](#) 참조하세요.

주제

- [SFTP, FTPS 및 FTP 서버 이벤트](#)
- [SFTP 커넥터 이벤트](#)
- [AS2 이벤트](#)

SFTP, FTPS 및 FTP 서버 이벤트

다음은 SFTP, FTPS 및 FTP 서버 이벤트에 대한 세부 정보 필드입니다.

- FTP 파일 서버 다운로드 완료
- FTP 파일 서버 다운로드 실패
- FTP 파일 서버 업로드 완료
- FTP 파일 서버 업로드 실패
- FTPS 파일 서버 다운로드 완료
- FTPS 파일 서버 다운로드 실패
- FTPS 파일 서버 업로드 완료
- FTPS 파일 서버 업로드 실패
- SFTP 서버 파일 다운로드 완료
- SFTP 서버 파일 다운로드 실패
- SFTP 서버 파일 업로드 완료
- SFTP 서버 파일 업로드 실패

source 및 detail-type 필드는 Transfer Family 이벤트에 대한 특정 값을 포함하므로 아래에 포함되어 있습니다. 모든 이벤트에 포함된 다른 메타데이터 필드의 정의는 Amazon EventBridge 사용 설명서의 [이벤트 구조 참조](#)를 참조하세요.

```
{
  . . . ,
  "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",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

detail-type

이벤트의 유형을 식별합니다.

이 이벤트의 값은 이전에 나열된 SFTP, FTPS 또는 FTP 서버 이벤트 이름 중 하나입니다.

source

이벤트를 생성한 서비스를 식별합니다. Transfer Family 이벤트의 경우 이 값은 `aws.transfer`입니다.

detail

이벤트에 대한 정보가 포함된 JSON 객체입니다. 이벤트를 생성하는 서비스에 따라 이 필드의 내용이 결정됩니다.

이 이벤트의 경우 데이터에 다음이 포함됩니다.

failure-code

전송이 실패한 이유에 대한 범주입니다. 값: PARTIAL_UPLOAD | PARTIAL_DOWNLOAD | UNKNOWN_ERROR

status-code

전송 성공 여부. 값: COMPLETED | FAILED.

protocol

전송에 사용되는 프로토콜입니다. 값: SFTP | FTPS | FTP

bytes

전송되는 바이트 수입니다.

client-ip

전송과 관련된 클라이언트의 IP 주소

failure-message

실패한 전송의 경우 전송이 실패한 이유에 대한 세부 정보입니다.

end-timestamp

성공적인 전송을 위해 파일 처리가 완료될 때의 타임스탬프입니다.

etag

엔터티 태그(Amazon S3 파일에만 사용됨).

file-path

전송 중인 파일의 경로입니다.

server-id

Transfer Family 서버의 고유 ID입니다.

username

전송을 수행하는 사용자입니다.

session-id

전송 세션의 고유 식별자입니다.

start-timestamp

성공적인 전송을 위해 파일 처리가 시작될 때의 타임스탬프입니다.

Example SFTP 서버 파일 다운로드 실패 예제 이벤트

다음 예제는 SFTP 서버에서 다운로드가 실패한 이벤트를 보여줍니다(사용 중인 스토리지 Amazon EFS).

```
{
  "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 FTP 파일 서버 업로드 완료 예제 이벤트

다음 예제는 FTP 서버에서 업로드가 성공적으로 완료된 이벤트를 보여줍니다(사용 중인 스토리지 Amazon S3).

```
{
  "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": "/DOC-EXAMPLE-BUCKET/test/1mb_file",
        "server-id": "s-1111aaaa2222bbbb3",
        "username": "test",
        "session-id": "event-ID",
        "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
}

```

SFTP 커넥터 이벤트

다음은 SFTP 커넥터 이벤트에 대한 세부 필드입니다.

- SFTP 커넥터 파일 전송 완료
- SFTP 커넥터 파일 전송 실패
- SFTP 커넥터 파일 검색 완료
- SFTP 커넥터 파일 검색 실패

source 및 detail-type 필드는 Transfer Family 이벤트에 대한 특정 값을 포함하므로 아래에 포함되어 있습니다. 모든 이벤트에 포함된 다른 메타데이터 필드의 정의는 Amazon EventBridge 사용 설명서의 [이벤트 구조 참조](#)를 참조하세요.

```

{
    . . . ,
    "detail-type": "string",
    "source": "aws.transfer",
    . . . ,
    "detail": {
        "operation" : "string",
        "connector-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",
    "bytes" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
  }
}

```

detail-type

이벤트의 유형을 식별합니다.

이 이벤트의 경우 값은 이전에 나열된 SFTP 커넥터 이벤트 이름 중 하나입니다.

source

이벤트를 생성한 서비스를 식별합니다. 이벤트의 경우 Transfer Family 이 값은 `aws.transfer`입니다.

detail

이벤트에 대한 정보가 포함된 JSON 객체입니다. 이벤트를 생성하는 서비스는 이 필드의 내용을 결정합니다.

이 이벤트의 경우 데이터에 다음이 포함됩니다.

operation

StartFileTransfer 요청이 파일을 전송하고 있는지 아니면 검색하고 있는지 여부. 값: `SEND|RETRIEVE`.

connector-id

사용 중인 SFTP 커넥터의 고유 식별자입니다.

`transfer-id`

전송 이벤트(StartFileTransfer요청)의 고유 식별자입니다.

`file-transfer-id`

전송 중인 파일의 고유 식별자입니다.

`url`

파트너 AS2 또는 SFTP 엔드포인트URL의 .

`file-path`

전송 또는 검색되는 위치 및 파일입니다.

`status-code`

전송 성공 여부. 값: FAILED | COMPLETED.

`failure-code`

실패한 전송의 경우 전송이 실패한 이유 코드입니다.

`failure-message`

실패한 전송의 경우 전송이 실패한 이유에 대한 세부 정보입니다.

`start-timestamp`

성공적인 전송을 위해 파일 처리가 시작될 때의 타임스탬프입니다.

`end-timestamp`

성공적인 전송을 위해 파일 처리가 완료될 때의 타임스탬프입니다.

`local-directory-path`

RETRIEVE 요청의 경우 검색된 파일을 배치할 위치입니다.

`remote-directory-path`

SEND 요청의 경우 파트너의 SFTP 서버에 파일을 배치할 파일 디렉터리입니다. 사용자가 StartFileTransfer 요청에 전달RemoteDirectoryPath한 의 값입니다. 파트너의 서버에서 기본 디렉터리를 지정할 수 있습니다SFTP. 그렇다면 이 필드는 비어 있습니다.

`bytes`

전송 중인 바이트 수입니다. 실패한 전송의 값은 0입니다.

local-file-location

이 파라미터에는 AWS 스토리지 파일의 위치에 대한 세부 정보가 포함되어 있습니다.

domain

사용 중인 스토리지입니다. 현재 유일한 값은 `s3`입니다.

bucket

Amazon S3의 객체에 대한 컨테이너입니다.

key

Amazon S3의 객체에 할당된 이름입니다.

Example SFTP 커넥터 파일 전송 실패 예제 이벤트

다음 예제는 원격 SFTP 서버로 파일을 보내려고 시도하는 동안 SFTP 커넥터가 실패한 이벤트를 보여줍니다.

```
{
  "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": "/DOC-EXAMPLE-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": "DOC-EXAMPLE-BUCKET",
      "key": "testfile.txt"
    }
  }
}

```

Example SFTP 커넥터 파일 검색 완료 예제 이벤트

다음 예제는 SFTP 커넥터가 원격 SFTP 서버에서 전송된 파일을 성공적으로 검색한 이벤트를 보여줍니다.

```

{
  "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": "/DOC-EXAMPLE-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": "DOC-EXAMPLE-BUCKET",
      "key": "testfile.txt"
    }
  }
}

```



```
}
}
```

AS2 이벤트

다음은 AS2 이벤트의 세부 정보 필드입니다.

- AS2 페이로드 수신 완료
- AS2 페이로드 수신 실패
- AS2 페이로드 전송 완료
- AS2 페이로드 전송 실패
- AS2 MDN 수신 완료
- AS2 MDN 수신 실패
- AS2 MDN 전송 완료
- AS2 MDN 전송 실패

source 및 detail-type 필드는 Transfer Family 이벤트에 대한 특정 값을 포함하므로 아래에 포함되어 있습니다. 모든 이벤트에 포함된 다른 메타데이터 필드의 정의는 Amazon EventBridge 사용 설명서의 [이벤트 구조 참조](#)를 참조하세요.

```
{
  . . . ,
  "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

이벤트의 유형을 식별합니다.

이 이벤트의 경우 값은 이전에 나열된 AS2 이벤트 중 하나입니다.

source

이벤트를 생성한 서비스를 식별합니다. 이벤트의 경우 Transfer Family 이 값은 `aws.transfer`입니다.

detail

이벤트에 대한 정보가 포함된 JSON 객체입니다. 이벤트를 생성하는 서비스에 따라 이 필드의 내용이 결정됩니다.

s3-attributes

전송 중인 파일의 Amazon S3 버킷 및 키를 식별합니다. MDN 이벤트의 경우 MDN 파일의 버킷과 키도 식별합니다.

file-bucket

Amazon S3의 객체에 대한 컨테이너입니다.

file-key

Amazon S3의 객체에 할당된 이름입니다.

json-bucket

COMPLETED 또는 FAILED 전송의 경우 JSON 파일의 컨테이너입니다.

json-key

COMPLETED 또는 FAILED 전송의 경우 Amazon S3의 JSON 파일에 할당된 이름입니다.

mdn-bucket

MDN 이벤트의 경우 MDN 파일의 컨테이너입니다.

mdn-key

MDN 이벤트의 경우 Amazon S3의 MDN 파일에 할당된 이름입니다.

mdn-subject

MDN 이벤트의 경우 메시지 처리에 대한 텍스트 설명입니다.

mdn-message-id

MDN 이벤트의 경우 MDN 메시지의 고유 ID입니다.

disposition

MDN 이벤트의 경우 처리의 범주입니다.

bytes

메시지의 바이트 수입니다.

as2-from

메시지를 보내는 AS2 거래 파트너입니다.

as2-message-id

전송 중인 AS2 메시지의 고유 식별자입니다.

as2-to

메시지를 수신하는 AS2 거래 파트너입니다.

connector-id

Transfer Family 서버에서 거래 파트너로 전송되는 AS2 메시지의 경우 사용 중인 AS2 커넥터의 고유 식별자입니다.

client-ip

서버 이벤트(거래 파트너에서 Transfer Family 서버로 전송)의 경우 전송과 관련된 클라이언트의 IP 주소입니다.

agreement-id

서버 이벤트의 경우 AS2 계약의 고유 식별자입니다.

server-id

서버 이벤트의 경우 Transfer Family 서버에 대한 고유 ID만 해당됩니다.

requester-file-name

페이로드 이벤트의 경우 전송 중에 수신된 파일의 원래 이름입니다.

message-subject

메시지 제목에 대한 텍스트 설명입니다.

start-timestamp

성공적인 전송을 위해 파일 처리가 시작될 때의 타임스탬프입니다.

end-timestamp

성공적인 전송을 위해 파일 처리가 완료될 때의 타임스탬프입니다.

status-code

AS2 메시지 전송 프로세스의 상태에 해당하는 코드입니다. 유효한 값: COMPLETED | FAILED | PROCESSING.

failure-code

실패한 전송의 경우 전송이 실패한 이유의 범주입니다.

failure-message

실패한 전송의 경우 전송이 실패한 이유에 대한 세부 정보입니다.

transfer-id

전송 이벤트의 고유 식별자입니다.

Example AS2 페이로드 수신 완료된 예제 이벤트

```
{
```

```

    "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": "DOC-EXAMPLE-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 AS2 MDN 실패한 예제 이벤트 수신

```

{
  "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": "DOC-EXAMPLE-BUCKET1",
  "file-key": "/as2Integ/TestOutboundWrongCert.dat",
  "file-bucket": "DOC-EXAMPLE-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"
}
}
```

의 보안 AWS Transfer Family

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 범위](#) 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#) 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [의 보고서 다운로드 AWS Artifact](#).

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 AWS 서비스 결정됩니다. 는 규정 준수를 지원하는 다음 리소스를 AWS 제공합니다.

- [보안 및 규정 준수 빠른 시작 안내서](#) - 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 에 기존 환경을 배포 AWS 하기 위한 단계를 제공합니다.
- [Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 아키텍처](#) - 이 백서에서는 기업이 HIPAA 를 사용하여 적격 애플리케이션을 AWS 생성하는 방법을 설명합니다.

Note

모두 HIPAA 적합한 AWS 서비스 것은 아닙니다. 자세한 내용은 [HIPAA 적격 서비스 참조를](#) 참조하세요.

- [AWS 규정 준수 리소스](#) - 이 워크북 및 가이드 모음은 해당 산업 및 위치에 적용될 수 있습니다.
- [AWS 고객 규정 준수 가이드](#) - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(), 결제카드 산업보안표준위원회(NIST), PCI국제표준화 기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) - 이 AWS Config 서비스는 리소스 구성 이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) - AWS 서비스 에서 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub 는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하세요.

- [AWS Audit Manager](#) - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 규정 및 업계 표준 준수 및 위험을 관리하는 방법을 간소화할 수 있습니다.

이 설명서는 를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 AWS Transfer Family. 다음 주제에서는 보안 및 규정 준수 목표에 AWS Transfer Family 맞게 를 구성하는 방법을 보여줍니다. 또한 AWS Transfer Family 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- [에 대한 보안 정책 AWS Transfer Family](#)
- [AWS Transfer Family에서 하이브리드 포스트 쿼텀 키 교환 사용](#)
- [의 데이터 보호 AWS Transfer Family](#)
- [에 대한 자격 증명 및 액세스 관리 AWS Transfer Family](#)
- [에 대한 규정 준수 검증 AWS Transfer Family](#)
- [복원력 AWS Transfer Family](#)
- [의 인프라 보안 AWS Transfer Family](#)
- [웹 애플리케이션 방화벽 추가](#)
- [교차 서비스 혼동된 대리인 방지](#)
- [AWS Transfer Family에 대한 관리형 정책](#)

에 대한 보안 정책 AWS Transfer Family

의 서버 보안 정책을 AWS Transfer Family 사용하면 서버와 연결된 암호화 알고리즘(메시지 인증 코드 (MACs), 키 교환(KEXs) 및 암호 제품군) 세트를 제한할 수 있습니다. 지원되는 키 알고리즘 목록은 [암호화 알고리즘](#) 섹션을 참조하세요. 서버 호스트 키 및 서비스 관리 사용자 키와 함께 사용할 수 있는 지원되는 키 알고리즘 목록은 [사용자 및 서버 키에 지원되는 알고리즘](#)을 참조하세요.

Note

최신 보안 정책에 따라 서버를 업데이트하는 것이 좋습니다. 최신 보안 정책은 기본값입니다. 를 사용하여 CloudFormation Transfer Family 서버를 생성하고 기본 보안 정책을 수락하는 모든 고객에게는 최신 정책이 자동으로 할당됩니다. 클라이언트 호환성이 우려되는 경우 기본 정책을 사용하는 대신 서버를 생성하거나 업데이트할 때 사용하려는 보안 정책을 명확하게 명시하십시오. 기본 정책은 변경될 수 있습니다.

서버의 보안 정책을 변경하려면 섹션을 참조하세요 [보안 정책 편집](#).

Transfer Family의 보안에 대한 자세한 내용은 블로그 게시물, [Transfer Family가 안전하고 규정을 준수하는 관리형 파일 전송 솔루션을 구축하는 데 도움이 되는 방법](#) 섹션을 참조하세요.

주제

- [암호화 알고리즘](#)
- [TransferSecurityPolicy-2024년 1월](#)
- [TransferSecurityPolicy-2023년 5월](#)
- [TransferSecurityPolicy-2022년 3월](#)
- [TransferSecurityPolicy-2020년 6월](#)
- [TransferSecurityPolicy-2018년 11월](#)
- [TransferSecurityPolicy-FIPS-2024년 1월](#)
- [TransferSecurityPolicy-FIPS-2023년 5월](#)
- [TransferSecurityPolicy-FIPS-2020년 6월](#)
- [포스트 쿼텀 보안 정책](#)

Note

TransferSecurityPolicy-2024-01 는 콘솔, API 또는 를 사용하여 서버를 생성할 때 서버에 연결된 기본 보안 정책입니다CLI.

암호화 알고리즘

호스트 키의 경우 다음 알고리즘을 지원합니다.

- rsa-sha-256
- rsa-sha-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp512
- ssh-ed25519

또한 2018 및 2020 보안 정책은 를 허용합니다ssh-rsa.

 **Note**

RSA 키 유형, 즉 항상과 지원되는 알고리즘 중 하나일 수 있는 ssh-rsa RSA 호스트 키 알고리즘의 차이점을 이해하는 것이 중요합니다.

다음은 각 보안 정책에 지원되는 암호화 알고리즘 목록입니다.

 **Note**

다음 표 및 정책에서 알고리즘 유형의 다음 사용에 유의하세요.

- SFTP 서버는 SshCiphers, SshKexs및 SshMacs 섹션에서 알고리즘만 사용합니다.
- FTPS 서버는 TlsCiphers 섹션의 알고리즘만 사용합니다.
- FTP 서버는 암호화를 사용하지 않으므로 이러한 알고리즘을 사용하지 마세요.

보안 정 책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
SshCiphers								
aes128- ctr	◆			◆	◆		◆	◆
aes128- gc m@openssh .com	◆	◆	◆	◆	◆	◆	◆	◆
aes192- ctr	◆	◆	◆	◆	◆	◆	◆	◆
aes256- ctr	◆	◆	◆	◆	◆	◆	◆	◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
chacha20-poly1305@openssh.com				◆				◆
SshKexs								
curve25519-sha256	◆	◆	◆					◆
curve25519-sha256@libssh.org	◆	◆	◆					◆
diffie-hellman-group14-sha1								◆
diffie-hellman-group14-sha256				◆		◆		◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
diffie-hellman-group16-sha512	◆	◆	◆	◆	◆	◆	◆	◆
diffie-hellman-group18-sha512	◆	◆	◆	◆	◆	◆	◆	◆
diffie-hellman-group-exchange-sha256		◆	◆	◆		◆	◆	◆
ecdh-nist-p256-kurve512r3-sha256-d00@openquantumsafe.org	◆				◆			

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
ecdh-nistp384kyber-768r3-sha384-d00@openquantumsafe.org	◆				◆			
ecdh-nistp521kyber-1024r3-sha512-d00@openquantumsafe.org	◆				◆			
ecdh-sha2-nistp256	◆			◆	◆		◆	◆
ecdh-sha2-nistp384	◆			◆	◆		◆	◆
ecdh-sha2-nistp521	◆			◆	◆		◆	◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
x25519-kyber-512r3	◆							
sha256-d00@amazon.com								
SshMacs								
hmac-sha1								◆
hmac-sha1-etm@openssh.com								◆
hmac-sha2-256			◆	◆			◆	◆
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512			◆	◆			◆	◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com				◆				◆
umac-128@openssh.com				◆				◆
umac-64-etm@openssh.com								◆
umac-64@openssh.com								◆
TlsCiphers								
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		◆	◆	◆	◆	◆	◆	◆

보안 정책	2024-01	2023-05	2022-03	2020-06	FIPS-2024 년 1월	FIPS-2023 년 5월	FIPS-2020 년 6월	2018-11
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256								◆
TLS_RSA_WITH_AES_512_CBC_SHA256								◆

TransferSecurityPolicy-2024년 1월

다음은 TransferSecurityPolicy-2024-01 보안 정책을 보여줍니다.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "x25519-kyber-512r3-sha256-d00@amazon.com",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "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"
    ],
    "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-2023년 5월

다음은 TransferSecurityPolicy-2023-05 보안 정책을 보여줍니다.

```

{
  "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"
    ],
    "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-2022년 3월

다음은 TransferSecurityPolicy-2022-03 보안 정책을 보여줍니다.

```

{
  "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"
  ],
  "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-2020년 6월

다음은 TransferSecurityPolicy-2020-06 보안 정책을 보여줍니다.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "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"
  ],
  "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-2018년 11월

다음은 TransferSecurityPolicy-2018-11 보안 정책을 보여줍니다.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "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"
  ],
  "SshMac": [
    "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"
  ],
  "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"
  ]
}
}

```

TransferSecurityPolicy-FIPS-2024년 1월

다음은 TransferSecurityPolicy-FIPS-2024-01 보안 정책을 보여줍니다.

Note

FIPS 서비스 엔드포인트 및 TransferSecurityPolicy-FIPS-2024-01 보안 정책은 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요.

```
{
  "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-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "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"
    ],
    "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-2023년 5월

에 대한 FIPS 인증 세부 정보는 에서 확인할 AWS Transfer Family 수 있습니다. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

다음은 TransferSecurityPolicy-FIPS-2023-05 보안 정책을 보여줍니다.

Note

FIPS 서비스 엔드포인트 및 TransferSecurityPolicy-FIPS-2023-05 보안 정책은 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요.

```
{
  "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"
    ],
    "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-2020년 6월

에 대한 FIPS 인증 세부 정보는 에서 확인할 AWS Transfer Family 수 있습니다. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

다음은 TransferSecurityPolicy-FIPS-2020-06 보안 정책을 보여줍니다.

Note

FIPS 서비스 엔드포인트 및 TransferSecurityPolicy-FIPS-2020-06 보안 정책은 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요.

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

```

포스트 퀀텀 보안 정책

이 표에는 Transfer Family 포스트 퀀텀 보안 정책의 알고리즘이 나열되어 있습니다. 이러한 정책은 [AWS Transfer Family에서 하이브리드 포스트 퀀텀 키 교환 사용](#)에 자세히 설명되어 있습니다.

정책 목록은 표 뒤에 나와 있습니다.

보안 정책	TransferSecurityPolicy-PQ-S SH-Experimental-2023-04	TransferSecurityPolicy-PQ-S SH-FIPS-Experimental-2023-04
SSH ciphers		
aes128-ctr		◆
aes128-gcm@openssh.com	◆	◆
aes192-ctr	◆	◆
aes256-ctr	◆	◆
aes256-gcm@openssh.com	◆	◆
KEXs		

보안 정책	TransferSecurityPolicy-PQ-S SH-Experimental-2023-04	TransferSecurityPolicy-PQ-S SH-FIPS-Experimental-2023-04
ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org	◆	◆
ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org	◆	◆
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	◆	◆
x25519-kyber-512r3-sha256-d00@amazon.com	◆	
diffie-hellman-group14-sha256		◆
diffie-hellman-group16-sha512	◆	◆
diffie-hellman-group18-sha512	◆	◆
ecdh-sha2-nistp384		◆
ecdh-sha2-nistp521		◆
diffie-hellman-group-exchange-sha256	◆	◆
ecdh-sha2-nistp256		◆
curve25519-sha256@libssh.org	◆	
curve25519-sha256	◆	
MACs		

보안 정책	TransferSecurityPolicy-PQ-S SH-Experimental-2023-04	TransferSecurityPolicy-PQ-S SH-FIPS-Experimental-2023-04
hmac-sha2-256-etm@ openssh.com	◆	◆
hmac-sha2-256	◆	◆
hmac-sha2-512-etm@ openssh.com	◆	◆
hmac-sha2-512	◆	◆
TLS ciphers		
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

다음은 TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 보안 정책을 보여줍니다.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "x25519-kyber-512r3-sha256-d00@amazon.com",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "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"
    ],
    "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-PQ-SSH-FIPS-Experimental-2023-04

다음은 TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04 보안 정책을 보여줍니다.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.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"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "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"
    ]
  }
}
```

```
}
}
```

AWS Transfer Family에서 하이브리드 포스트 쿼텀 키 교환 사용

AWS Transfer Family 는 Secure Shell(SSH) 프로토콜에 대한 하이브리드 사후 양자 키 설정 옵션을 지원합니다. 이미 네트워크 트래픽을 기록하고 나중에 store-now-harvest-later 공격이라고 하는 양자 컴퓨터에 의한 복호화를 위해 저장할 수 있기 때문에 양자 후 키 설정이 필요합니다.

Amazon Simple Storage Service(Amazon S3) 스토리지 또는 Amazon Elastic File System(Amazon)으로 안전하게 파일을 전송하기 위해 Transfer Family에 연결할 때 이 옵션을 사용할 수 있습니다EFS. 이 포스트 쿼텀 하이브리드 키 설정에는 클래식 키 교환 알고리즘과 함께 사용하는 포스트 쿼텀 키 설정 메커니즘이 SSH 도입되었습니다. SSH 클래식 암호 제품군으로 생성된 키는 현재 기술을 사용한 무차별 공격으로부터 안전합니다. 그러나 향후 대규모 양자 컴퓨팅이 등장하더라도 기존 암호화는 보안을 유지하지 못할 것으로 예상됩니다.

Transfer Family 연결을 통해 전달되는 데이터의 장기 기밀 유지에 의존하는 조직의 경우, 대규모 양자 컴퓨터를 사용할 수 있게 되기 전에 포스트 쿼텀 암호화로 마이그레이션하는 계획을 고려해야 합니다.

현재 암호화된 데이터를 잠재적 향후 공격으로부터 보호하기 위해 AWS 는 양자 내성 또는 양자 후 알고리즘 개발에 암호화 커뮤니티에 참여하고 있습니다. Transfer Family에서 클래식 및 포스트 쿼텀 요소를 결합하는 하이브리드 포스트 쿼텀 키 교환 암호 제품군을 구현했습니다.

이러한 하이브리드 암호 제품군은 대부분의 AWS 지역에서 프로덕션 워크로드에 사용할 수 있습니다. 그러나 하이브리드 암호 제품군의 성능 특성 및 대역폭 요건은 클래식 키 교환 메커니즘의 해당 요건과 다르기 때문에 Transfer Family 연결에 대해 이 제품군을 테스트하는 것이 좋습니다.

[포스트 쿼텀 암호화](#) 보안 블로그 게시물에서 포스트 쿼텀 암호화에 대해 자세히 알아보세요.

목차

- [의 포스트 쿼텀 하이브리드 키 교환 정보 SSH](#)
- [Transfer Family에서 포스트 쿼텀 하이브리드 키 설정이 작동하는 방식](#)
 - [Kyber를 선택하는 이유는 무엇인가?](#)
 - [양자 사후 하이브리드 SSH 키 교환 및 암호화 요구 사항\(FIPS 140\)](#)
- [Transfer Family의 포스트 쿼텀 하이브리드 키 교환 테스트](#)
 - [SFTP 엔드포인트에서 쿼텀 후 하이브리드 키 교환 활성화](#)
 - [포스트 쿼텀 하이브리드 키 교환을 지원하는 SFTP 클라이언트 설정](#)

- [에서 쿼텀 후 하이브리드 키 교환 확인 SFTP](#)

의 포스트 쿼텀 하이브리드 키 교환 정보 SSH

Transfer Family는 클래식 [Elliptic Curve Diffie-Hellman\(ECDH\)](#) 키 교환 알고리즘과 CRYSTALS [Kyber](#) 를 모두 사용하는 양자 후 하이브리드 키 교환 암호 제품군을 지원합니다. Kyber는 [National Institute for Standards and Technology\(NIST\)](#)가 첫 번째 표준 사후 양자 키 계약 알고리즘으로 지정한 양자 후 퍼블릭 키 암호화 및 키 설정 알고리즘입니다.

클라이언트와 서버는 여전히 ECDH 키 교환을 수행합니다. 또한 서버는 클라이언트의 키 SSH 교환 메시지에 광고되는 클라이언트의 사후 양자 KEM 퍼블릭 키에 양자 공유 보안 암호를 캡슐화합니다. 이 전략은 고전 키 교환의 높은 보장과 제안된 양자 후 키 교환의 보안을 결합하여 ECDH 또는 양자 후 공유 보안 암호를 해제할 수 없는 한 핸드셰이크를 보호할 수 있도록 합니다.

Transfer Family에서 포스트 쿼텀 하이브리드 키 설정이 작동하는 방식

AWS 는 최근 에서 SFTP 파일 전송 시 양자 이후 키 교환에 대한 지원을 발표했습니다 AWS Transfer Family. Transfer Family는 business-to-business SFTP 및 기타 프로토콜을 사용하여 AWS 스토리지 서비스로 파일 전송을 안전하게 확장합니다. SFTP 는 를 통해 실행되는 파일 전송 프로토콜(FTP)의 보다 안전한 버전입니다 SSH. Transfer Family의 양자 후 키 교환 지원은 를 통한 데이터 전송에 대한 보안 기준을 높입니다 SFTP.

Transfer Family의 양자 후 하이브리드 키 교환 SFTP 지원에는 양자 후 알고리즘 Kyber-512, Kyber-768 및 Kyber-1024를 개 ECDH 이상의 P256, P384, P521 또는 Curve25519 곡선과 결합하는 것이 포함됩니다. 다음과 같은 해당 SSH 키 교환 방법은 [양자 후 하이브리드 SSH 키 교환 초안 에](#) 지정되어 있습니다.

- `ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org`
- `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`
- `ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org`
- `x25519-kyber-512r3-sha256-d00@amazon.com`

Note

이러한 새로운 키 교환 방법은 초안이 표준화로 발전하거나 Kyber 알고리즘을 NIST 비준할 때 변경될 수 있습니다.

Kyber를 선택하는 이유는 무엇인가?

AWS는 상호 운용 가능한 표준화된 알고리즘을 지원하기 위해 최선을 다하고 있습니다. Kyber는 Post-Quantum [NIST Cryptography 프로젝트](#)에서 표준화를 위해 선택한 첫 번째 포스트 양자 암호화 알고리즘입니다. 일부 표준 본문은 이미 Kyber를 프로토콜에 통합하고 있습니다. 일부 AWS API 엔드포인트에서 AWS 이미 KyberTLS를 지원합니다.

이 약속의 일환으로 AWS는 Kyber를 용 P256과 같은 NIST승인된 곡선과 결합하는 양자 후 암호화 IETF에 대한 초안 제안을 제출했습니다. SSH. 고객의 보안을 강화하기 위해 SFTP 및 에서 양자 후 키 교환을 AWS 구현하면 해당 초안이 SSH 적용됩니다. 에서 제안을 채택 IETF하고 표준이 될 때까지 향후 업데이트를 지원할 계획입니다.

초안이 표준화로 발전하거나 Kyber 알고리즘을 NIST 비준할 때 새로운 키 교환 방법(섹션에 나열됨 [Transfer Family에서 포스트 쿼텀 하이브리드 키 설정이 작동하는 방식](#))이 변경될 수 있습니다.

Note

양자 사후 알고리즘 지원은 현재 에서의 양자 사후 하이브리드 키 교환 TLS AWS KMS ([TLS로 하이브리드 사후 양자 사용 AWS KMS](#) 참조) AWS Certificate Manager 및 AWS Secrets Manager API 엔드포인트에 사용할 수 있습니다.

양자 사후 하이브리드 SSH 키 교환 및 암호화 요구 사항(FIPS 140)

FIPS 규정 준수가 필요한 고객을 위해 Transfer Family는 140 인증 오픈 소스 암호화 라이브러리인 FIPS- AWS LCSSH를 사용하여 AWS FIPS에서 승인된 암호화를 제공합니다. Transfer Family의 TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04에서 지원되는 양자 후 하이브리드 키 교환 방법은 [NIST의 SP 800-56Cr2\(섹션 2\)](#)에 따라 FIPS 승인되었습니다. 독일 연방 정보 보안 사무소([BSI](#))와 프랑스의 Agence nationale de la sécurité des systèmes d'information([ANSSI](#))도 이러한 양자 후 하이브리드 키 교환 방법을 권장합니다.

Transfer Family의 포스트 쿼텀 하이브리드 키 교환 테스트

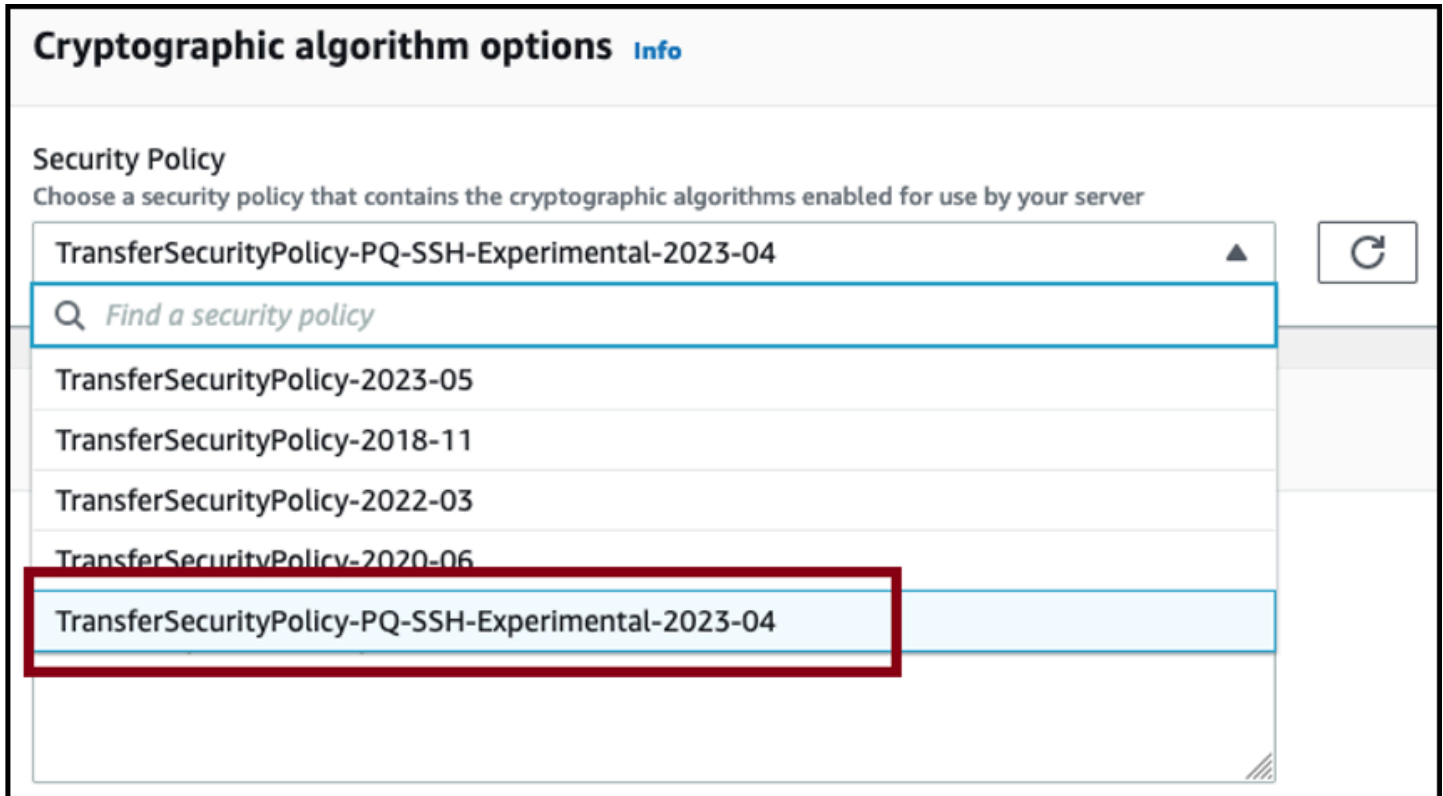
이 섹션에서는 포스트 쿼텀 하이브리드 키 교환을 테스트하기 위해 수행하는 단계를 설명합니다.

1. [SFTP 엔드포인트에서 쿼텀 후 하이브리드 키 교환 활성화](#).
2. 앞서 언급한 초안 사양의 지침에 따라 양자 후 하이브리드 키 교환을 지원하는 SFTP 클라이언트(예: [포스트 쿼텀 하이브리드 키 교환을 지원하는 SFTP 클라이언트 설정](#))를 사용합니다.
3. Transfer Family 서버를 사용하여 파일을 전송합니다.

4. [에서 쿼텀 후 하이브리드 키 교환 확인 SFTP.](#)

SFTP 엔드포인트에서 쿼텀 후 하이브리드 키 교환 활성화

Transfer Family에서 새 SFTP 서버 엔드포인트를 생성할 때 또는 기존 SFTP 엔드포인트에서 암호화 알고리즘 옵션을 편집하여 SSH 정책을 선택할 수 있습니다. 다음 스냅샷은 SSH 정책을 업데이트하는 AWS Management Console 의 예를 보여줍니다.



사후 양자 키 교환을 지원하는 SSH 정책 이름은 TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 및 TransferSecurityPolicy-PQ-SSHFIPS-Experimental-2023-04입니다. Transfer Family 정책에 대한 자세한 설명은 [에 대한 보안 정책 AWS Transfer Family](#)를 참조하세요.

포스트 쿼텀 하이브리드 키 교환을 지원하는 SFTP 클라이언트 설정

SFTP Transfer Family 엔드포인트에서 올바른 사후 양자 SSH 정책을 선택한 후 Transfer FamilySFTP에서 사후 양자로 실험할 수 있습니다. 앞서 언급한 초안 사양의 지침에 따라 양자 후 하이브리드 키 교환을 지원하는 SFTP 클라이언트(예: [OQS Open SSH](#))를 사용할 수 있습니다.

OQS OpenSSH은 를 사용하여 quantum-safe 암호화를 SSH에 추가하는 OpenSSH의 오픈 소스 포크입니다liboqs. liboqs는 양자 내성 암호화 알고리즘을 구현하는 오픈 소스 C 라이브러리입니다. OQS SSH와 liboqs는 Open Quantum Safe(OQS) 프로젝트의 일부입니다.

Transfer Family SFTP with OQS Open 에서 양자 후 하이브리드 키 교환을 테스트하려면 프로젝트의 [README](#)에 설명된 대로 OQS OpenSSH을 빌드SSH해야 합니다. OQS Open 을 빌드한 후 다음 명령과 같이 쿼텀 후 하이브리드 키 교환 방법을 사용하여 예제 SFTP 클라이언트를 실행하여 SFTP 엔드포인트(예: s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com)에 연결할 SSH수 있습니다.

```
./sftp -S ./ssh -v -o \
  KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

이전 명령에서 다음 항목을 자신의 정보로 바꿉니다.

- Replace *username_private_key_PEM_file* SFTP 사용자의 프라이빗 키 PEM인코딩 파일 사용
- Replace *username* SFTP 사용자 이름을 사용하여
- Replace *server-id* Transfer Family 서버 ID 사용
- Replace *region-id* Transfer Family 서버가 위치한 실제 리전

에서 쿼텀 후 하이브리드 키 교환 확인 SFTP

Transfer FamilySFTP에 대한 SSH 연결 중에 양자 후 하이브리드 키 교환이 사용되었는지 확인하려면 클라이언트 출력을 확인합니다. 선택적으로 패킷 캡처 프로그램을 사용할 수 있습니다. Open Quantum Safe OpenSSH 클라이언트를 사용하는 경우 출력은 다음과 비슷해야 합니다(간결성을 위해 관련 없는 정보 생략).

```
$. /sftp -S ./ssh -v -o KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-
d00@openquantumsafe.org -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_8.9-2022-01_p1, Open Quantum Safe 2022-08, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/lab/openssh/oqs-test/tmp/ssh_config
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xx.yy.zz..12] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_8.9-2022-01_
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 /home/lab/.ssh/known_hosts2: No such file or directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes192-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:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649
[...]
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 AWS.Transfer.PQ.SFTP.test-endpoint.aws.com ([xx.yy.zz..12]:22) using
"publickey".s
debug1: channel 0: new [client-session]
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>

```

출력은 양자 후 하이브리드 ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org 메서드를 사용하여 클라이언트 협상이 발생하고 SFTP 세션을 성공적으로 설정했음을 보여줍니다.

의 데이터 보호 AWS Transfer Family

AWS [공동 책임 모델](#) AWS Transfer Family (전송 패밀리)의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 사용하는 AWS 서비스에 대한 보안 구성 및 관리 작업이 포함됩니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 섹션](#)

을 [FAQ](#) 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management (IAM) ()를 사용하여 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. 1.2TLS를 지원합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- AWS 암호화 AWS 솔루션과 서비스 내 모든 기본 보안 제어를 사용합니다.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 FIPS 를 통해 에 액세스할 AWS 때 140-2 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#)를 참조하세요.

이름 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마십시오. 여기에는 콘솔, 또는 를 사용하여 Transfer Family 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다. API AWS CLI AWS SDKs. Transfer Family 서비스 구성에 입력하는 모든 구성 데이터 또는 다른 서비스의 구성이 진단 로그에 포함되도록 선택될 수 있습니다. 외부 서버에 URL을 제공하는 경우 해당 서버에 대한 요청을 검증 URL 하기 위해 에 보안 인증 정보를 포함하지 마세요.

반대로 Transfer Family 서버 내외로 업로드 및 다운로드 작업의 데이터는 완전히 비공개로 취급되며 SFTP 또는 FTPS 연결과 같은 암호화된 채널 외부에는 존재하지 않습니다. 이 데이터는 승인된 사람만 액세스할 수 있습니다.

주제

- [Amazon S3의 데이터 암호화](#)
- [키 관리](#)

Amazon S3의 데이터 암호화

AWS Transfer Family 는 Amazon S3 버킷에 대해 설정한 기본 암호화 옵션을 사용하여 데이터를 암호화합니다. 버킷에서 암호화를 활성화한 경우 모든 객체는 버킷에 저장될 때 암호화됩니다. 객체는

Amazon S3 관리형 키(SSE-S3) 또는 AWS Key Management Service () 관리형 키(SSE-AWS KMS)를 사용하여 서버 측 암호화를 사용하여 암호화됩니다. 자세한 설명은 Amazon Simple Storage Service 사용자 가이드의 [서버 측 암호화를 사용하여 데이터 보호](#)를 참조하세요.

다음 단계에서는 에서 데이터를 암호화하는 방법을 보여줍니다 AWS Transfer Family.

에서 암호화를 허용하려면 AWS Transfer Family

1. Amazon S3 버킷에 대한 기본 암호화를 활성화합니다. 자세한 설명은 Amazon Simple Storage Service 사용자 가이드의 [Amazon S3 버킷에 대한 Amazon S3 기본 암호화](#)를 참조하세요.
2. 사용자에게 연결된 AWS Identity and Access Management (IAM) 역할 정책을 업데이트하여 필요한 AWS Key Management Service (AWS KMS) 권한을 부여합니다.
3. 사용자에게 대해 세션 정책을 사용하는 경우 세션 정책에서 필요한 AWS KMS 권한을 부여해야 합니다.

다음 예제는 AWS KMS 암호화가 활성화된 Amazon S3 버킷과 AWS Transfer Family 함께 를 사용할 때 필요한 최소 권한을 부여하는 IAM 정책을 보여줍니다. 사용 중인 경우 사용자 IAM 역할 정책 및 세션 정책 모두에 이 예제 정책을 포함합니다.

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

이 정책에서 지정하는 KMS 키 ID는 1단계의 기본 암호화에 지정된 키 ID와 동일해야 합니다. 루트 또는 사용자에게 사용되는 IAM 역할은 키 정책에서 AWS KMS 허용되어야 합니다. AWS KMS 키 정책에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 [에서 키 정책 사용을 AWS KMS](#) 참조하세요.

키 관리

이 섹션에서는 키 생성 방법 및 키 교체 방법을 비롯한 SSH 키에 대한 정보를 찾을 수 있습니다. 에서 Transfer Family AWS Lambda 를 사용하여 키를 관리하는 방법에 대한 자세한 내용은 블로그 게시물 [A AWS Transfer Family 및 를 사용하여 사용자 셀프 서비스 키 관리 활성화 AWS Lambda](#)를 참조하세요.

Note

AWS Transfer Family 는 RSA, ECDSA 및 ED25519 키를 허용합니다.

이 섹션에서는 Pretty Good Privacy(PGP) 키를 생성하고 관리하는 방법도 다룹니다.

주제

- [사용자 및 서버 키에 지원되는 알고리즘](#)
- [서비스 관리 사용자를 위한 SSH 키 생성](#)
- [SSH 키 교체](#)
- [PGP 키 생성 및 관리](#)
- [지원되는 PGP 클라이언트](#)

사용자 및 서버 키에 지원되는 알고리즘

AWS Transfer Family 내에서 사용자 및 서버 키 쌍에 대해 다음과 같은 키 알고리즘이 지원됩니다.

Note

워크플로에서 PGP복호화에 사용할 알고리즘은 [PGP 키 페어에 지원되는 알고리즘을 참조하세요](#).

- 의 경우ED25519: ssh-ed25519
- 의 경우RSA:
 - rsa-sha2-256
 - rsa-sha2-512

- 의 경우 ECDSA:
 - `ecdsa-sha2-nistp256`
 - `ecdsa-sha2-nistp384`
 - `ecdsa-sha2-nistp521`

Note

이전 보안 정책에 SHA1 대해 `ssh-rsa` 를 지원합니다. 세부 정보는 [암호화 알고리즘](#) 을 참조하세요.

서비스 관리 사용자를 위한 SSH 키 생성

서비스 내에 사용자 이름과 SSH 키가 저장되는 서비스 관리형 인증 방법을 사용하여 사용자를 인증하도록 서버를 설정할 수 있습니다. 사용자의 퍼블릭 SSH 키는 사용자의 속성으로 서버에 업로드됩니다. 이 키는 서버에서 표준 키 기반 인증 프로세스의 일부로 사용됩니다. 각 사용자는 개별 서버가 있는 파일에 여러 퍼블릭 SSH 키를 가질 수 있습니다. 사용자당 저장할 수 있는 키 수에 대한 제한은 Amazon Web Services 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#) 을 참조하세요.

서비스 관리형 인증 방법의 대안으로 사용자 지정 자격 증명 공급자 또는 를 사용하여 사용자를 인증할 수 있습니다 AWS Directory Service for Microsoft Active Directory. 자세한 내용은 [사용자 지정 자격 증명 공급자와 작업](#) 또는 [AWS 디렉터리 서비스 자격 증명 공급자 사용](#) 을 참조하세요.

서버는 한 가지 방법 (서비스 관리형, 디렉터리 서비스 또는 맞춤 ID 제공자)을 사용해서만 사용자를 인증할 수 있으며, 서버를 만든 후에는 이 방법을 변경할 수 없습니다.

주제

- [macOS, Linux 또는 Unix에서 SSH 키 생성](#)
- [Microsoft Windows에서 SSH 키 생성](#)
- [SSH2 퍼블릭 키를 PEM 형식으로 변환](#)

macOS, Linux 또는 Unix에서 SSH 키 생성

macOS , Linux 또는 Unix 운영 체제에서는 `ssh-keygen` 명령을 사용하여 SSH 퍼블릭 키와 키 페어라고도 하는 SSH 프라이빗 키를 생성합니다.

macOS , Linux 또는 Unix 운영 체제에서 SSH 키를 생성하려면

1. macOS, Linux 또는 Unix 작동 시스템에서는 명령 터미널을 엽니다.
2. AWS Transfer Family 는 RSA-, ECDSA- 및 ED25519-형식의 키를 허용합니다. 생성하려는 키 쌍의 타입에 따라 적절한 명령을 선택합니다.

Note

다음 예에서는 패스프레이즈를 지정하지 않았는데, 이 경우 도구에서 패스프레이즈를 입력한 다음 반복하여 확인하도록 요청합니다. 패스프레이즈를 만들면 프라이빗 키를 더 잘 보호할 수 있고 전반적인 시스템 보안도 향상될 수 있습니다. 패스프레이즈는 복구할 수 없습니다: 암호를 잊은 경우 새 키를 생성해야 합니다.

그러나 Transfer Family 서버는 시작 시 패스프레이즈를 요청할 수 없으므로 서버 호스트 키를 생성하는 경우 명령에서 `-N ""` 옵션을 지정하거나 메시지가 표시되면 **Enter**을 두 번 눌러 빈 암호를 지정해야 합니다.

- RSA 4096비트 키 페어를 생성하려면:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- ECDSA 521비트 키 페어를 생성하려면(ECDSA비트 크기가 256, 384 및 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- ED25519 키 페어를 생성하려면:

```
ssh-keygen -t ed25519 -f key_name
```

Note

key_name 는 SSH 키 페어 파일 이름입니다.

다음은 ssh-keygen 출력의 예입니다.

```
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]-----+

```

Note

앞의 예처럼 `ssh-keygen` 명령을 실행하면, 현재 디렉터리에 퍼블릭 및 프라이빗 키가 파일로 생성됩니다.

이제 SSH 키 페어를 사용할 준비가 되었습니다. 3단계와 4단계를 따라 서비스 관리형 사용자의 SSH 퍼블릭 키를 저장합니다. 이러한 사용자는 Transfer Family 서버 엔드포인트에서 파일을 전송할 때 키를 사용합니다.

3. `key_name.pub` 파일로 이동하여 엽니다.
4. 텍스트를 복사하여 서비스 관리형 사용자의 SSH 퍼블릭 키에 붙여 넣습니다.
 - a. 에서 AWS Transfer Family 콘솔을 연 <https://console.aws.amazon.com/transfer/> 다음 탐색 창에서 서버를 선택합니다.
 - b. 서버 페이지에서 업데이트하려는 사용자가 포함된 서버의 서버 ID를 선택합니다.
 - c. 퍼블릭 키를 추가할 사용자를 선택합니다.
 - d. SSH 퍼블릭 키 창에서 SSH 퍼블릭 키 추가를 선택합니다.

Transfer Family > Servers > s- > User: OneUser

User: OneUser

[View logs](#) [Delete](#)

User configuration

[Edit](#)

Role

[Role](#)

Posix Profile

User ID

2001

Group ID

2001

Secondary Group IDs

-

Policy

[View](#)

Home directory

/fs- /

Restricted

SSH public keys (1)

[Delete](#) [Add SSH public key](#)

< 1 >

☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256:-

- e. 생성한 퍼블릭 키의 텍스트를 SSH 퍼블릭 키 텍스트 상자에 붙여 넣은 다음 키 추가를 선택합니다.

Transfer Family > Servers > s- > OneUser > Add key

Add key

SSH public keys

SSH public key [Info](#)

Paste the contents of SSH public key

Enter SSH public key

[Cancel](#) [Add key](#)

새 키는 SSH 퍼블릭 키 창에 나열됩니다.

SSH public keys (2)			Delete	Add SSH public key
			< 1 >	
☐	Date imported	Fingerprint		
☐	6/14/2022, 12:53:34 PM	SHA256:-		
☐	10/20/2022, 4:26:51 PM	SHA256:-		

Microsoft Windows에서 SSH 키 생성

Windows는 약간 다른 SSH 키 페어 형식을 사용합니다. 퍼블릭 키는 PUB 형식이어야 하고, 프라이빗 키는 PPK 형식이어야 합니다. Windows에서는 PuTTYgen 를 사용하여 적절한 형식으로 SSH 키 페어를 생성할 수 있습니다. PuTTYgen 를 사용하여 생성된 프라이빗 키를 .ppk 파일로 변환할 수도 있습니다.

Note

.ppk 형식이 아닌 프라이빗 키 파일과 함께 WinSCP를 제공하는 경우 해당 클라이언트는 키를 .ppk 형식으로 변환하도록 제안합니다.

Windows PuTTYgen 에서 P를 사용하여 SSH 키를 생성하는 방법에 대한 자습서는 [SSH.com 웹 사이트](https://www.ssh.com/ssh-keygen/)를 참조하세요.

SSH2 퍼블릭 키를 PEM 형식으로 변환

AWS Transfer Family 는 PEM 형식이 지정된 퍼블릭 키만 허용합니다. SSH2 퍼블릭 키가 있는 경우 이를 변환해야 합니다. SSH2 퍼블릭 키의 형식은 다음과 같습니다.

```
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
----- END SSH2 PUBLIC KEY -----
```

PEM 퍼블릭 키의 형식은 다음과 같습니다.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

다음 명령을 실행하여 SSH2형식이 지정된 퍼블릭 키를 PEM형식이 지정된 퍼블릭 키로 변환합니다. Replace *ssh2-key* SSH2 키 이름을 사용하여 *PEM-key* PEM 키의 이름이 표시됩니다.

```
ssh-keygen -i -f ssh2-key.pub > PEM-key.pub
```

SSH 키 교체

보안을 위해 SSH 키를 교체하는 모범 사례를 권장합니다. 일반적으로 이러한 교체는 보안 정책의 일부로 지정되며, 자동화된 방식으로 구현됩니다. 보안 수준에 따라 매우 민감한 통신의 경우 SSH 키 페어를 한 번만 사용할 수 있습니다. 이렇게 하면 저장된 키 때문에 발생하는 모든 위험을 제거할 수 있습니다. 그러나 일정 기간 동안 SSH 보안 인증 정보를 저장하고 사용자에게 과도한 부담을 주지 않는 간격을 설정하는 것이 훨씬 더 일반적입니다. 가장 일반적인 주기는 3개월입니다.

SSH 키 교체를 수행하는 데 사용되는 두 가지 방법이 있습니다.

- 콘솔에서 새 SSH 퍼블릭 키를 업로드하고 기존 SSH 퍼블릭 키를 삭제할 수 있습니다.
- 를 사용하여 [DeleteSshPublicKey](#) API를 사용하여 사용자의 Secure Shell(SSH) 퍼블릭 키를 삭제하고 [ImportSshPublicKey](#) API를 사용하여 새 Secure Shell(SSH) 퍼블릭 키를 사용자 계정에 추가하여 기존 사용자를 업데이트할 API 수 있습니다.

Console

콘솔에서 키 로테이션을 수행하려면

1. 에서 AWS Transfer Family 콘솔을 엽니다 <https://console.aws.amazon.com/transfer/>.
2. 서버 페이지로 이동합니다.
3. 서버 ID 옆에서 식별자를 선택하여 서버 세부 정보 페이지를 표시합니다.
4. 사용자 에서 퍼블릭 SSH 키를 교체하려는 사용자의 확인란을 선택한 다음 작업을 선택한 다음 키 추가를 선택하여 키 추가 페이지를 확인합니다.

또는

사용자 이름을 선택하여 사용자 세부 정보 페이지를 확인한 다음 SSH 퍼블릭 키 추가를 선택하여 키 추가 페이지를 확인합니다.

5. 새 SSH 퍼블릭 키를 입력하고 키 추가를 선택합니다.

⚠ Important

SSH 퍼블릭 키의 형식은 생성한 키 유형에 따라 다릅니다.

- RSA 키의 형식은 `ssh-rsa string`.
- ED25519 키의 형식은 `ssh-ed25519 string`.
- ECDSA 키의 경우 키는 생성한 키의 크기에 따라 `ecdsa-sha2-nistp521`, `ecdsa-sha2-nistp256` 또는 `ecdsa-sha2-nistp384`로 시작합니다. 그런 다음 다른 키 타입과 마찬가지로 시작 문자열 뒤에 *string*(가) 옵니다.

사용자 세부 정보 페이지로 돌아가고 방금 입력한 새 SSH 퍼블릭 키가 SSH 퍼블릭 키 섹션에 나타납니다.

6. 삭제할 보안 인증 옆의 확인란을 선택하고 삭제를 선택합니다.
7. 단어 `delete`를 입력하여 삭제 작업을 확인한 다음 삭제를 선택합니다.

API

를 사용하여 키 교체를 수행하려면 API

1. macOS, Linux 또는 Unix 작동 시스템에서는 명령 터미널을 엽니다.
2. 다음 명령을 입력하여 삭제하려는 SSH 키를 검색합니다. 이 명령을 사용하려면, *serverID*를 Transfer Family 서버의 서버 ID로 바꾸고 *username*를 사용자 이름으로 바꾸세요.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

이 명령은 사용자에게 대한 세부 정보를 반환합니다. "SshPublicKeyId": 필드 내용을 복사합니다. 이 값은 이 절차의 뒷부분에서 입력해야 합니다.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. 그런 다음 사용자의 새 SSH 키를 가져옵니다. 프롬프트에 다음 명령을 입력합니다. 이 명령을 사용하려면 *serverID*를 Transfer Family 서버의 서버 ID로 바꾸고 *username*를 사용자 이름으로 바꾸고 *public-key*를 새 퍼블릭 키의 지문으로 바꾸세요.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'
--ssh-public-key-body='public-key'
```

이 명령이 성공하면 출력이 반환되지 않습니다.

4. 마지막으로 다음 명령을 실행하여 이전 키를 삭제합니다. 이 명령을 사용하려면 *serverID*를 Transfer Family 서버의 서버 ID로 바꾸고 *username*를 사용자 이름으로 바꾸고 *keyID-from-step-2*를 이 절차의 2단계에서 복사한 키 ID 값으로 바꾸세요.

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'
--ssh-public-key-id='keyID-from-step-2'
```

5. (옵션) 이전 키가 더 이상 존재하지 않는지 확인하려면 2단계를 반복합니다.

PGP 키 생성 및 관리

Transfer Family가 워크플로로 처리하는 파일에 Pretty Good Privacy(PGP) 복호화를 사용할 수 있습니다. 워크플로 단계에서 복호화를 사용하려면 PGP 키를 제공해야 합니다.

AWS 스토리지 블로그에는 [PGP 및 를 사용하여 파일을 암호화 및 복호화하고 파일을 암호화 및 복호화 AWS Transfer Family](#)하는 방법을 설명하는 게시물이 있습니다.

PGP 키 생성

PGP 키를 생성하는 데 사용하는 방법은 운영 체제와 사용 중인 키 생성 소프트웨어의 버전에 따라 다릅니다.

Linux 또는 Unix를 사용하는 경우 패키지 설치 프로그램을 사용하여 gpg를 설치하세요. Linux 배포판에 따라 다음 명령 중 하나를 사용할 수 있습니다.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Windows 또는 macOS의 경우, <https://gnupg.org/download/>에서 필요한 것을 다운로드할 수 있습니다.

PGP 키 생성기 소프트웨어를 설치한 후 `gpg --full-gen-key` 또는 `gpg --gen-key` 명령을 실행하여 키 페어를 생성합니다.

 Note

GnuPG 버전 2.3.0 이상을 사용하는 경우 `gpg --full-gen-key`를 실행해야 합니다. 생성할 키 유형에 대한 메시지가 표시되면 RSA 또는 `l`를 선택합니다 ECC. 그러나 `l`를 선택하는 경우 ECC다음 중 하나를 선택해야 합니다.NIST 또는 BrainPool 타원 곡선의 경우. 선택 안 함 Curve 25519.

PGP 키 페어에 지원되는 알고리즘

PGP 키 페어에 지원되는 알고리즘은 다음과 같습니다.

- RSA
- Elgamal
- ECC:
 - NIST
 - BrainPool

 Note

Curve25519 키는 지원되지 않습니다.

유용한 **gpg** 하위 명령

다음은 gpg에 유용한 몇 가지 하위 명령입니다:

- `gpg --help` – 이 명령에는 사용 가능한 옵션이 나열되며 몇 가지 예가 포함될 수 있습니다.
- `gpg --list-keys` – 이 명령은 생성한 모든 키 쌍에 대한 세부 정보를 나열합니다.
- `gpg --fingerprint` – 이 명령은 각 키의 지문을 포함하여 모든 키 쌍에 대한 세부 정보를 나열합니다.
- `gpg --export -a user-name` – 이 명령은 키가 생성될 때 사용된 *user-name* 키의 퍼블릭 키 부분을 내보냅니다.

PGP 키 관리

PGP 키를 관리하려면 `l`를 사용해야 합니다 AWS Secrets Manager.

Note

비밀 명칭에는 Transfer Family 서버 ID가 포함됩니다. 즉, 이 PGP 키 정보를 저장하기 전에 서버를 이미 식별했거나 생성했어야 합니다 AWS Secrets Manager.

모든 사용자에게 대해 하나의 키와 암호를 사용하려면 PGP 키 블록 정보를 보안 암호 이름 아래에 저장할 수 있습니다. `aws/transfer/server-id/@pgp-default` 여기서 *server-id*는 Transfer Family 서버의 ID입니다. 이 기본 키는 *user-name*가 워크플로를 실행하는 사용자와 일치하는 키가 없는 경우에 사용됩니다.

또는 특정 사용자의 키를 생성할 수 있습니다. 이 경우 암호 명칭의 형식은 `aws/transfer/server-id/user-name`입니다. 여기서 *user-name*는 Transfer Family 서버의 워크플로를 실행하는 사용자와 일치합니다.

Note

Transfer Family 서버당 사용자당 최대 3개의 PGP 프라이빗 키를 저장할 수 있습니다.

복호화에 사용할 PGP 키를 구성하려면

1. 사용 GPG 중인 버전에 따라 다음 명령 중 하나를 실행하여 Curve 25519 암호화 알고리즘을 사용하지 않는 PGP 키 페어를 생성합니다.

- **GnuPG** 버전 2.3.0 이상을 사용하는 경우, 다음 명령을 실행합니다.

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

RSA를 선택할 수도 있고, **ECC**를 선택할 경우 **NIST** 또는 **BrainPool** 하나를 타원 곡선으로 선택할 수 있습니다. `gpg --gen-key` 대신 `gpg --full-gen-key`를 실행하면 현재 키에 대해 지원되지 않는 ECC Curve 25519 암호화 알고리즘을 사용하는 PGP 키 페어를 생성합니다.

- 2.3.0 **GnuPG** 이전 버전의 경우 RSA가 기본 암호화 유형이므로 다음 명령을 사용할 수 있습니다.

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

⚠ Important

키 생성 프로세스 중에 패스프레이즈와 이메일 주소를 제공해야 합니다. 이러한 값을 기록해 두세요. 이 절차의 AWS Secrets Manager 뒷부분에서 키의 세부 정보를 입력할 때 패스프레이즈를 제공해야 합니다. 그리고 다음 단계에서 프라이빗 키를 내보내려면 동일한 이메일 주소를 제공해야 합니다.

2. 프라이빗 키를 내보내려면 다음 명령을 실행합니다. 이 명령을 사용하려면 *private.pgp*를 프라이빗 키 블록을 저장할 파일 명칭으로, *marymajor@example.com*를 키 쌍을 생성할 때 사용한 이메일 주소로 바꾸세요.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. PGP 키를 저장하는 AWS Secrets Manager 데 사용합니다.
 - a. 에 로그인 AWS Management Console 하고 에서 AWS Secrets Manager 콘솔을 엽니다 <https://console.aws.amazon.com/secretsmanager/>.
 - b. 왼쪽 탐색 창에서 암호를 선택합니다.
 - c. 암호 페이지에서 새 암호 저장을 선택합니다.
 - d. 암호 타입 선택 페이지의 암호 타입에 대해 다른 타입의 암호를 선택합니다.
 - e. 키/값 쌍 섹션에서 키/값 탭을 선택합니다.
 - 키 – **PGPPrivateKey**를 입력합니다.

i Note

PGPPrivateKey 문자열을 정확히 입력해야 합니다: 문자 앞이나 사이에 공백을 추가하지 마세요.

- 값 — 프라이빗 키의 텍스트를 값 필드에 붙여넣습니다. 이 절차의 앞부분에서 키를 내보낼 때 지정한 파일 (예: *private.pgp*) 에서 프라이빗 키의 텍스트를 찾을 수 있습니다. 키는 -----BEGIN PGP PRIVATE KEY BLOCK----- (으)로 시작하고 -----END PGP PRIVATE KEY BLOCK----- (으)로 끝납니다.

Note

텍스트 블록에는 프라이빗 키만 포함되고 퍼블릭 키는 포함되지 않는지 확인하세요.

f. 행 추가를 선택하고 키/값 쌍 섹션에서 키/값 탭을 선택합니다.

- 키 - **PGPPassphrase**를 입력합니다.

Note

PGPPassphrase 문자열을 정확히 입력해야 합니다: 문자 앞이나 사이에 공백을 추가하지 마세요.

- 값 - PGP 키 페어를 생성할 때 사용한 암호를 입력합니다.

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	
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	my passphrase	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.

aws/secretsmanager [Add new key](#)

Note

최대 3세트의 키와 패스프레이즈를 추가할 수 있습니다. 두 번째 세트를 추가하려면 새 행 두 개를 추가하고 키에 **PGPPrivateKey2**와(과) **PGPPassphrase2**를 입력한 다음 다른 프라이빗 키와 패스프레이즈를 붙여넣습니다. 세 번째 세트를 추가하려면 키 값이 **PGPPrivateKey3** 및 **PGPPassphrase3**여야 합니다.

- g. Next(다음)를 선택합니다.
- h. 암호 구성 페이지에 암호를 위한 명칭과 설명을 입력합니다.
 - 기본 키, 즉 모든 Transfer Family 사용자가 사용할 수 있는 키를 만들려면 다음을 입력하세요 **aws/transfer/*server-id*/epgp-default**. *server-id*를 복호화 단계가 있는 워크플로가 포함된 서버의 ID로 바꾸세요.
 - 특정 Transfer Family 사용자가 사용할 키를 만들려면 **aws/transfer/*server-id*/*user-name***를 입력하세요. *server-id*를 복호화 단계가 있는 워크플로가 포함된 서버의 ID로 바꾸고 *user-name*를 워크플로를 실행하는 사용자 이름으로 바꾸세요. *user-name*은(는) Transfer Family 서버가 사용하는 ID 제공자에 저장됩니다.
- i. 다음을 선택하고 순환 구성 페이지의 기본값을 그대로 사용합니다. 그 다음 다음을 선택합니다.
- j. 검토 페이지에서 저장을 선택하여 암호를 만들고 저장합니다.

다음 스크린샷은 특정 Transfer Family 서버의 사용자 **marymajor**의 세부 정보를 보여줍니다. 이 예에서는 세 개의 키와 해당 패스프레이즈를 보여줍니다.

/ aws/transfer/s- / marymajor
Replicate secret to other Regions

Secret details
Actions

Encryption key
aws/secretsmanager

Secret name
/ aws/transfer/s- / marymajor

Secret ARN
arn:aws:secretsmanager:us-east-2:-:secret:/aws/transfer/s- / marymajor-

Secret description
Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-

Secret value Info
Close Edit

Retrieve and view the secret value.

Key/value Plaintext

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase	my passphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase2	my passphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase3	my passphrase3

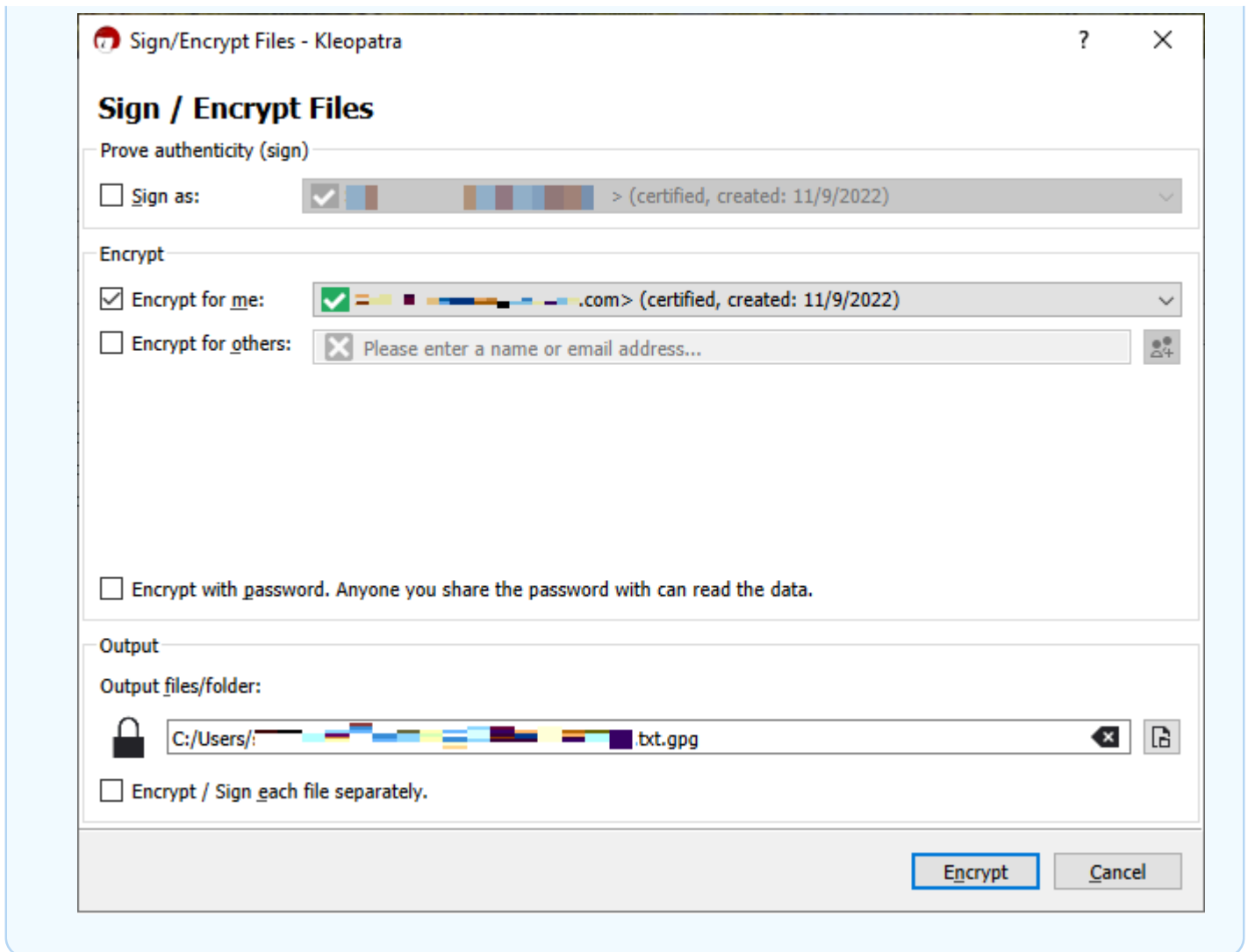
지원되는 PGP 클라이언트

다음 클라이언트는 Transfer Family로 테스트되었으며 PGP 키를 생성하고 워크플로를 사용하여 복호화하려는 파일을 암호화하는 데 사용할 수 있습니다.

- Gpg4win + Kleopatra.

Note

파일 서명/암호화를 선택할 때는 서명 주체 선택을 취소해야 합니다: 현재 암호화된 파일에 대한 서명은 지원하지 않습니다.



- 주요 GnuPG 버전: 2.4, 2.3, 2.2, 2.0, 1.4.

다른 PGP 클라이언트도 작동할 수 있지만 여기에 언급된 클라이언트만 Transfer Family로 테스트되었습니다.

에 대한 자격 증명 및 액세스 관리 AWS Transfer Family

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 AWS Transfer Family 누가 리소스를 사용할 수 있도록 인증(로그인) 및 권한 부여(권한 부여)를 받을 수 있는지 제어합니다. IAM 는 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [고객](#)

- [ID를 통한 인증](#)
- [정책을 사용한 액세스 관리](#)
- [에서 AWS Transfer Family 를 사용하는 방법 IAM](#)
- [AWS Transfer Family 자격 증명 기반 정책 예제](#)
- [AWS Transfer Family 태그 기반 정책 예제](#)
- [AWS Transfer Family 자격 증명 및 액세스 문제 해결](#)

고객

AWS Identity and Access Management (IAM) 사용 방법은 에서 수행하는 작업에 따라 다릅니다 AWS Transfer Family.

서비스 사용자 - AWS Transfer Family 서비스를 사용하여 작업을 수행하는 경우 관리자는 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Transfer Family 기능을 사용하여 작업을 수행하면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Transfer Family의 기능에 액세스할 수 없는 경우 [AWS Transfer Family 자격 증명 및 액세스 문제 해결](#)을 참조하세요.

서비스 관리자 - 회사에서 AWS Transfer Family 리소스를 담당하는 경우 에 대한 전체 액세스 권한이 있을 수 있습니다 AWS Transfer Family. 서비스 사용자가 액세스해야 하는 AWS Transfer Family 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 이해합니다 IAM. 회사에서 IAM를 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Transfer Family참조하세요 [에서 AWS Transfer Family 를 사용하는 방법 IAM](#).

IAM 관리자 - IAM 관리자인 경우 에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다 AWS Transfer Family. 에서 사용할 수 있는 자격 AWS Transfer Family 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요 [AWS Transfer Family 자격 증명 기반 정책 예제](#).

ID를 통한 인증

인증은 자격 증명 AWS 으로 에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자로 또는 IAM 역할을 수입하여 인증(에 로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 에 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션 자격 증명으로 로

그인하면 관리자가 이전에 IAM 역할을 사용하여 자격 증명 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수입하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [에 로그인하는 방법을 AWS 계정 AWS참조하세요.](#)

AWS 프로그래밍 방식으로 에 액세스하는 경우는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [요청 서명을 AWS API](#) 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [다중 인증](#) 및 사용 설명서의 [다중 인증 사용\(MFA\) AWS](#)을 참조하세요IAM.

AWS 계정 루트 사용자

를 생성하면 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업을](#) 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, , AWS Directory Service Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스하면 역할을 AWS 계정수입하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [IAM Identity Center란 무엇입니까?](#)를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례에 대한 액세스 키 정기적으로 교체](#)를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 라는 이름의 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수입할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 [\(역할 대신\) IAM 사용자를 생성할 시기](#)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 비슷하지만 특정 사용자와는 관련이 없습니다. IAM 역할을 전한 AWS Management Console 하에서 역할을 일시적으로 수입할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수입할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 역할 사용](#)을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 [타사 자격 증명 공급자에 대한 역할 생성](#)을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 세트](#)를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 다른 권한을 일시적으로 맡을 IAM 역할을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다.

그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스도 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [리소스 기반 정책과 IAM 역할이 어떻게 다른지](#) 참조하세요.

- 교차 서비스 액세스 - 일부 는 다른 에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와 의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [액세스 세션 전달](#)을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수입하는 [IAM 역할](#)입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 [에 권한을 위임할 역할 생성을 AWS 서비스](#) 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서[EC2의 IAM 역할 사용을 참조하세요](#).

IAM 역할 또는 IAM 사용자를 사용할지 여부를 알아보려면 IAM 사용 설명서의 [IAM 역할 생성 시기\(사용자 대신\)](#)를 참조하세요.

정책을 사용한 액세스 관리

정책을 AWS 생성하고 AWS 자격 증명 또는 리소스에 연결하여 의 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 AWS 때 권한을 정의하는 의 객체입니다. 는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나

거부되는 지를 결정합니다. 대부분의 정책은 에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM 사용 설명서 [의 JSON 정책 개요](#)를 참조하세요.

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, iam:GetRole 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI 또는 에서 역할 정보를 가져올 수 있습니다 AWS API.

보안 인증 기반 정책

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 선택](#)을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책IAM에서는 의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

Amazon S3 AWS WAF 및 Amazon VPC은 를 지원하는 서비스의 예입니다. ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 [액세스 제어 목록\(ACL\) 개요](#)를 ACLs 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- **권한 경계** - 권한 경계는 자격 증명 기반 정책이 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 엔터티에 대한 권한 경계](#)를 참조하세요.
- **서비스 제어 정책(SCPs)** - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 SCPs JSON 정책입니다. AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여려 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 모든 계정에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다. AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [SCPs 작동 방식](#)을 SCPs 참조하세요.
- **세션 정책** - 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. AWS 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

에서 AWS Transfer Family 를 사용하는 방법 IAM

AWS Identity and Access Management (IAM)를 사용하여 에 대한 액세스를 관리하기 전에 에서 사용할 수 있는 IAM 기능을 이해해야 AWS Transfer Family합니다 AWS Transfer Family. AWS Transfer Family 및 기타 AWS 서비스가 에서 작동하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 [AWS 에서 작업하는 서비스를 IAM](#) IAM참조하세요.

주제

- [AWS Transfer Family ID 기반 정책](#)
- [AWS Transfer Family 리소스 기반 정책](#)
- [AWS Transfer Family 태그 기반 인증](#)
- [AWS Transfer Family IAM 역할](#)

AWS Transfer Family ID 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부된 작업 및 리소스와 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. AWS Transfer Family 는 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 AWS Identity and Access Management 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

작업

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

의 정책 작업은 작업 앞에 다음 접두사를 AWS Transfer Family 사용합니다transfer:. 예를 들어 Transfer Family CreateServer API 작업을 사용하여 서버를 생성할 수 있는 권한을 부여하려면 정책에 transfer:CreateServer 작업을 포함시킵니다. 정책 명령문에는 Action 또는 NotAction 요소가 포함되어야 합니다. AWS Transfer Family 는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 집합을 정의합니다.

명령문 하나에 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
    "transfer:action1",
    "transfer:action2"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "transfer:Describe*"
```

AWS Transfer Family 작업 목록을 보려면 서비스 승인 참조의 에서 [정의한 작업을 AWS Transfer Family](#) 참조하세요.

리소스

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문장에는 Resource 또는 NotResource 요소가 반드시 추가되어야 합니다. 가장 좋은 방법은 [Amazon 리소스 이름\(ARN\)을 사용하여 리소스를](#) 지정하는 것입니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"

```

Transfer Family 서버 리소스에는 다음과 같은 이 있습니다ARN.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

예를 들어 명령문에서 s-01234567890abcdef Transfer Family 서버를 지정하려면 다음 를 사용합니다ARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

형식에 대한 자세한 ARNs내용은 서비스 승인 참조 또는 IAM 사용 설명서 [IAM ARNs](#)의 [Amazon 리소스 이름\(ARNs\)](#)을 참조하세요.

특정 계정에 속하는 모든 인스턴스를 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

일부 AWS Transfer Family 작업은 IAM 정책에 사용되는 리소스와 같은 여러 리소스에서 수행됩니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

Transfer Family 서버 및 사용자에게 대한 액세스를 허용하는 정책을 만드는 경우와 같이 둘 이상의 리소스 타입을 지정해야 하는 경우도 있습니다. 단일 문에서 여러 리소스를 지정하려면 쉼표ARNs로 를 구분합니다.

```
"Resource": [
    "resource1",
    "resource2"
]
```

AWS Transfer Family 리소스 목록을 보려면 서비스 승인 참조의 [에 정의된 리소스 유형을 AWS Transfer Family](#) 참조하세요.

조건 키

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 IAM 리소스에 사용자 IAM 이름으로 태그가 지정된 경우에만 사용자에게 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS 는 전역 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

AWS Transfer Family 는 자체 조건 키 세트를 정의하고 일부 전역 조건 키 사용을 지원합니다. AWS Transfer Family 조건 키 목록을 보려면 서비스 승인 참조의 [에 대한 조건 키를 AWS Transfer Family](#) 참조하세요.

예시

AWS Transfer Family 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Transfer Family 자격 증명 기반 정책 예제](#).

AWS Transfer Family 리소스 기반 정책

리소스 기반 정책은 지정된 보안 주체가 AWS Transfer Family 리소스에서 수행할 수 있는 작업과 조건을 지정하는 JSON 정책 문서입니다. Amazon S3는 Amazon S3에 대한 리소스 기반 권한 정책을 지원합니다. *buckets*. 리소스 기반 정책을 사용하면 리소스별로 다른 계정에 사용 권한을 부여할 수 있습니다. 리소스 기반 정책을 사용하여 AWS 서비스가 Amazon S3에 액세스하도록 허용할 수도 있습니다. *buckets*.

교차 계정 액세스를 활성화하려면 리소스 기반 정책 에서 전체 계정 또는 다른 계정의 IAM 엔터티를 보안 주체로 지정할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우 보안 주체에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 보안 인증 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [리소스 기반 정책과 IAM 역할의 차이점](#)을 참조하세요.

Amazon S3 서비스는 *bucket* 정책, 에 연결된 *bucket*. 이 정책은 객체에 대해 작업을 수행할 수 있는 보안 주체(계정, 사용자, 역할 및 페더레이션 사용자)를 정의합니다.

예시

AWS Transfer Family 리소스 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Transfer Family 태그 기반 정책 예제](#).

AWS Transfer Family 태그 기반 인증

에 대한 요청에서 태그를 AWS Transfer Family 리소스에 연결하거나 전달할 수 있습니다 AWS Transfer Family. 태그에 근거하여 액세스를 제어하려면 `transfer:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정

보를 제공합니다. 태그를 사용하여 AWS Transfer Family 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AWS Transfer Family 태그 기반 정책 예제](#).

AWS Transfer Family IAM 역할

[IAM 역할은](#) AWS 계정 내에서 특정 권한이 있는 엔터티입니다.

에서 임시 자격 증명 사용 AWS Transfer Family

임시 자격 증명을 사용하여 페더레이션으로 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. [AssumeRole](#) 또는 와 같은 작업을 호출 AWS STS API하여 임시 보안 자격 증명을 얻을 수 있습니다 [GetFederationToken](#).

AWS Transfer Family 는 임시 자격 증명 사용을 지원합니다.

AWS Transfer Family 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할에는 AWS Transfer Family 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS 를 사용하여 작업을 수행할 수 없습니다 API. IAM 관리자는 사용자 및 역할에 필요한 지정된 리소스에 대해 특정 API 작업을 수행할 수 있는 권한을 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 해당 정책을 연결해야 합니다.

이러한 예제 정책 문서를 사용하여 IAM 자격 증명 기반 JSON 정책을 생성하는 방법을 알아보려면 AWS Identity and Access Management 사용 설명서 [의 JSON 탭에서 정책 생성을](#) 참조하세요.

주제

- [정책 모범 사례](#)
- [AWS Transfer Family 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)

정책 모범 사례

자격 증명 기반 정책은 계정에서 AWS Transfer Family 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용

할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [관리AWS 형 정책](#) 또는 [AWS 작업 함수에 대한 관리형 정책을](#) 참조하세요.

- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 [에서 정책 및 권한을 IAM](#) 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 정책 조건을 작성하여 를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다SSL. AWS 서비스와 같은 특정 를 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건을](#) 참조하세요.
- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer 정책 검증](#)을 참조하세요.
- 다중 인증 필요(MFA) - 에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해 를 AWS 계정칩니다. API 작업을 호출할 MFA 때 를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA-보호된 API 액세스 구성을](#) 참조하세요.

의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [의 보안 모범 사례를 IAM](#) 참조하세요.

AWS Transfer Family 콘솔 사용

AWS Transfer Family 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 AWS 계정의 AWS Transfer Family 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 생성하는 경우 콘솔은 해당 정책이 있는 엔터티(IAM 사용자 또는 역할)에 대해 의도한 대로 작동하지 않습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [사용자에게 권한 추가](#)를 참조하십시오.

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 허용합니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다 AWS API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Transfer Family 태그 기반 정책 예제

다음은 태그를 기반으로 AWS Transfer Family 리소스에 대한 액세스를 제어하는 방법의 예입니다.

태그를 사용하여 AWS Transfer Family 리소스에 대한 액세스 통제

IAM 정책의 조건은 AWS Transfer Family 리소스에 대한 권한을 지정하는 데 사용하는 구문의 일부입니다. 리소스의 태그를 기반으로 AWS Transfer Family 리소스(예: 사용자, 서버, 역할 및 기타 엔터티)에 대한 액세스를 제어할 수 있습니다. 태그는 키/값 쌍입니다. 리소스 태그 지정에 대한 자세한 내용은 [AWS 리소스 태그 지정](#)을 참조하세요. AWS 일반 참조.

에서 AWS Transfer Family 리소스에는 태그가 있을 수 있으며 일부 작업에는 태그가 포함될 수 있습니다. IAM 정책을 생성할 때 태그 조건 키를 사용하여 다음을 제어할 수 있습니다.

- AWS Transfer Family 리소스에 있는 태그를 기반으로 리소스에 대해 작업을 수행할 수 있는 사용자입니다.
- 어떤 태그가 작업의 요청에서 전달될 수 있는지 통제합니다.
- 요청에서 특정 키를 사용할 수 있는지 여부를 통제합니다.

태그 기반 액세스 제어를 사용하면 API 수준보다 더 미세한 제어를 적용할 수 있습니다. 또한 리소스 기반 액세스 통제를 사용하는 것보다 더 동적인 통제를 적용할 수 있습니다. 요청에 제공된 태그(요청 태그)를 기반으로 작업을 허용하거나 거부하는 IAM 정책을 생성할 수 있습니다. 또한 (리소스 태그)에서 운영 중인 리소스의 태그를 기반으로 IAM 정책을 생성할 수 있습니다. 일반적으로 리소스 태그는 리소스에 이미 있는 태그용이고, 요청 태그는 리소스에 태그를 추가하거나 리소스에서 태그를 제거할 때 사용됩니다.

태그 조건 키의 전체 구문 및 의미 체계는 IAM 사용 설명서의 [AWS 리소스 태그를 사용하여 리소스에 대한 액세스 제어](#)를 참조하세요. API Gateway를 사용하여 IAM 정책을 지정하는 방법에 대한 자세한 내용은 API Gateway 개발자 안내서의 [IAM 권한을 API 사용하여 에 대한 액세스 제어](#)를 참조하세요.

예 1: 리소스 태그 기반 작업 거부

태그를 기반으로 리소스에서 수행할 작업을 거부할 수 있습니다. 다음 예 정책은 사용자 또는 서버 리소스에 키 stage와(과) 값 prod이(가) 태그 지정된 경우 TagResource, UntagResource, StartServer, StopServer, DescribeServer, DescribeUser 작업을 거부합니다.

```
{
  "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"
        }
    }
}
]
}

```

예 2: 리소스 태그 기반 작업 허용

태그를 기반으로 리소스에서 작업을 수행하도록 허용할 수 있습니다. 다음 예 정책은 사용자 또는 서버 리소스에 키 stage와(과) 값 prod이(가) 태그 지정된 경우 TagResource, UntagResource, StartServer, StopServer, DescribeServer, DescribeUser 작업을 거부합니다.

```

{
    "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"
                }
            }
        }
    ]
}

```

```
}

```

예 3: 요청 태그에 따른 사용자 또는 서버 생성 거부

다음의 정책 예에는 명령문이 2개입니다. 첫 번째 명령문은 태그의 코스트 센터 키에 값이 없는 경우 모든 리소스에 대한 `CreateServer` 작업을 거부합니다.

두 번째 명령문은 태그의 코스트 센터 키에 1, 2 또는 3을 제외한 다른 값이 포함된 경우 `CreateServer` 작업을 거부합니다.

Note

이 정책은 1, 2, 또는 3 라는 `costcenter` 키와 값을 포함하는 리소스를 만들거나 삭제할 수 있도록 허용합니다.

```
{
  "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"
  ]
}
}
}
]
}

```

AWS Transfer Family 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AWS Transfer Family 및 작업 시 발생할 수 있는 일반적인 문제를 진단하고 해결할 수 있습니다IAM.

주제

- [에서 작업을 수행할 권한이 없습니다.AWS Transfer Family](#)
- [iam을 수행할 권한이 없습니다.PassRole](#)
- [내 AWS 계정 외부의 사람들이 내 AWS Transfer Family 리소스에 액세스하도록 허용하고 싶습니다.](#)

에서 작업을 수행할 권한이 없습니다.AWS Transfer Family

에 작업을 수행할 권한이 없다고 AWS Management Console 표시되면 관리자에게 문의하여 지원을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 에 대한 세부 정보를 보려고 할 때 발생합니다.*widget*에는 *transfer:GetWidget* 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
transfer:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *my-example-widget* 작업을 사용하여 *transfer::GetWidget* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam을 수행할 권한이 없습니다.PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Transfer Family에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있도록 AWS 서비스 허용합니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이름이 인 IAM 사용자가 콘솔을 사용하여 에서 작업을 수행하려고 marymajor 할 때 발생합니다 AWS Transfer Family. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

다음 예 정책에는 역할을 AWS Transfer Family에 전달할 권한이 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "iam:PassRole",
      "Resource": "arn:aws::iam::123456789012:role/*",
      "Effect": "Allow"
    }
  ]
}
```

내 AWS 계정 외부의 사람들이 내 AWS Transfer Family 리소스에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 가 이러한 기능을 AWS Transfer Family 지원하는지 알아보려면 섹션을 참조하세요 [에서 AWS Transfer Family 를 사용하는 방법 IAM](#).
- 소유 AWS 계정 한 의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [소유 AWS 계정 한 다른 의 IAM 사용자에게 액세스 권한 제공을 참조하세요](#).

- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유에 대한 액세스 권한 제공](#)을 AWS 계정참조하세요.
- 자격 증명 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부 인증 사용자\(자격 증명 페더레이션\)에 대한 액세스 제공](#)을 참조하세요.
- 교차 계정 액세스에 역할 및 리소스 기반 정책을 사용하는 차이점을 알아보려면 IAM 사용 설명서의 [리소스 기반 정책과 IAM 역할이 어떻게 다른지](#) 참조하세요.

에 대한 규정 준수 검증 AWS Transfer Family

타사 감사자는 여러 규정 준수 프로그램의 AWS Transfer Family 일환으로 의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, HIPAA, 및 기타PCI가 포함됩니다. 전체 목록은 [AWS 규정 준수 프로그램의 범위 내 서비스를 참조하세요](#).

특정 규정 준수 프로그램의 범위에 속하는 AWS 서비스 목록은 [AWS 규정 준수 프로그램별 범위 내 서비스를 참조하세요](#). 일반 정보는 [AWS 규정 준수 프로그램](#)을 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [의 보고서 다운로드를 참조하세요 AWS Artifact](#).

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. AWS Transfer Family 는 규정 준수를 지원하는 다음 리소스를 AWS 제공합니다.

- [보안 및 규정 준수 빠른 시작 가이드](#) - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 에서 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- [HIPAA 보안 및 규정 준수를 위한 아키텍처 백서](#) - 이 백서는 기업이 HIPAA규정을 준수하는 애플리케이션을 생성하는 AWS 데 를 사용할 수 있는 방법을 설명합니다.
- [AWS 규정 준수 리소스](#) - 사용자의 업계와 위치에 해당할 수 있는 워크북 및 가이드 모음입니다.
- [AWS Config](#) - 이 AWS 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) - 이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수를 확인하는 데 도움이 되는 의 보안 상태를 포괄적으로 보여줍니다.

복원력 AWS Transfer Family

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. AWS 리전은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워크와 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 제

공합니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS Transfer Family 는 최대 3개의 가용 영역을 지원하며 연결 및 전송 요청을 위한 자동 조정, 중복 플릿을 지원합니다.

유의할 사항:

- 퍼블릭 엔드포인트의 경우:
 - 가용 영역 수준의 이중화가 서비스에 내장되어 있습니다.
 - 각 AZ에는 중복 플릿이 있습니다.
 - 이 중복성은 자동으로 제공됩니다.
- Virtual Private Cloud(VPC)의 엔드포인트는 섹션을 참조하세요 [Virtual Private Cloud\(VPC\)에 서버 생성](#).

참고 항목

- AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라 섹션](#)을 참조하세요.
- 지연 시간 기반 라우팅을 사용하여 중복성을 높이고 네트워크 지연 시간을 최소화하는 방법에 대한 예제는 블로그 게시물 [AWS Transfer Family 서버로 네트워크 지연 시간 최소화를 참조하세요](#).

의 인프라 보안 AWS Transfer Family

관리형 서비스인 AWS Transfer Family 는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및 가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 [AWS 클라우드 보안 섹션](#)을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 [인프라 보호](#)를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 AWS Transfer Family 통해 에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- DHE (Ephemeral Diffie-HellmanPFS) 또는 (Elliptic Curve Ephemeral Diffie-Hellman)과 같은 완벽한 순방향 보안ECDHE()이 포함된 Cipher 제품군입니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 IAM 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 보안 인증을 생성하여 요청에 서명할 수 있습니다.

웹 애플리케이션 방화벽 추가

AWS WAF 는 웹 애플리케이션과 를 공격APIs으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 사용하여 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 웹 액세스 제어 목록(웹 ACL)이라고 하는 규칙 세트를 구성할 수 있습니다. 자세한 내용은 [를 보호하기 AWS WAF 위해 사용을 참조하세요APIs](#).

추가하려면 AWS WAF

1. 에서 API 게이트웨이 콘솔을 엽니다<https://console.aws.amazon.com/apigateway/>.
2. APIs 탐색 창에서 사용자 지정 자격 증명 공급자 템플릿을 선택합니다.
3. 단계를 선택합니다.
4. 단계(Stages) 창에서 단계 명칭을 선택합니다.
5. Stage Editor(단계 편집기) 창에서 설정 탭을 선택합니다.
6. 다음 중 하나를 수행합니다.
 - 웹 애플리케이션 방화벽(WAF)의 웹 ACL에서 이 단계에 연결할 웹ACL을 선택합니다.
 - ACL 필요한 웹이 없는 경우 다음을 수행하여 웹을 생성해야 합니다.
 1. 웹 생성을 ACL선택합니다.
 2. 서비스 홈페이지에서 AWS WAF 웹 생성을 ACL선택합니다.
 3. 웹 ACL 세부 정보 의 이름 에 웹 의 이름을 입력합니다ACL.
 4. 규칙에서 규칙 추가를 선택한 다음 나만의 규칙 및 규칙 그룹 추가를 선택합니다.
 5. 규칙 타입에서 IP 세트를 선택하여 특정 IP 주소 목록을 식별합니다.
 6. 규칙에는 규칙 명칭을 입력합니다.
 7. IP 세트의 경우 기존 IP 세트를 선택합니다. IP 집합을 생성하려면 [IP 세트 생성](#)을 참조하세요.
 8. 기원 주소로 사용할 IP 주소의 경우 헤더의 IP 주소를 선택합니다.
 9. 헤더 필드 명칭에 SourceIP를 입력합니다.
 - 10.헤더 내 위치의 경우 첫 번째 IP 주소를 선택합니다.

11. 누락된 IP 주소를 위한 대처를 위해, 헤더에서 유효하지 않거나 누락된 IP 주소를 처리하려는 방법에 따라 일치 또는 불일치를 선택합니다.
12. 조치에서 IP 세트 조치를 선택합니다.
13. 규칙과 일치하지 않는 요청에 대한 기본 웹 ACL 작업 에서 허용 또는 차단을 선택한 다음 다음을 클릭합니다.
14. 단계와 5단계에서 다음을 선택합니다.
15. 검토 및 생성에서 선택 사항을 검토한 다음 웹 생성 ACL을 선택합니다.

7. 변경 사항 저장을 선택합니다.
8. 리소스를 선택합니다.
9. 작업 에서 배포를 API 선택합니다.

AWS 웹 애플리케이션 방화벽 AWS Transfer Family 으로 보안하는 방법에 대한 자세한 내용은 AWS 스토리지 블로그의 [AWS 애플리케이션 방화벽 및 Amazon API Gateway AWS Transfer Family 로 보안을 참조하세요.](#)

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 서비스 AWS간 사칭은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다. 이 문제에 대한 자세한 설명은 IAM 사용 설명서 [의 혼동된 대리자 문제를 참조하세요.](#)

리소스 정책에서 [aws:SourceArn](#) 및 [aws:SourceAccount](#) 전역 조건 컨텍스트 키를 사용하여 AWS Transfer Family가 리소스에 대해 갖는 권한을 제한하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문서에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 허용하려는 리소스의 정확한 Amazon 리소스 이름(ARN)을 사용하는 것입니다. 여러 리소스를 지정하는 경우 의 알 수 없는 부분에 와일드카드 문자(*)가 있는 `aws:SourceArn` 전역 컨텍스트 조건 키를 사용합니다. 예: `arn:aws:transfer::region::account-id:server/*`.

AWS Transfer Family는 다음과 같은 유형의 역할을 사용합니다.

- 사용자 역할 - 서비스 관리형 사용자가 필요한 Transfer Family 리소스에 액세스할 수 있도록 허용합니다. AWS Transfer Family는 Transfer Family 사용자 의 맥락에서 이 역할을 말합니다ARN.
- 액세스 역할 - 전송 중인 Amazon S3 파일에만 액세스할 수 있습니다. 인바운드 AS2 전송의 경우 액세스 역할은 계약에 Amazon 리소스 이름(ARN)을 사용합니다. 아웃바운드 AS2 전송의 경우 액세스 역할은 커넥터에 ARN 를 사용합니다.
- 호출 역할 - 서버의 사용자 지정 자격 증명 공급자로 Amazon API Gateway와 함께 사용됩니다. Transfer Family는 Transfer Family 서버 의 컨텍스트에서 이 역할을 말합니다ARN.
- 로깅 역할 - Amazon 에 항목을 로깅하는 데 사용됩니다 CloudWatch. Transfer Family는 이 역할을 사용하여 File Transfer에 대한 정보와 함께 성공 및 실패 세부 정보를 기록합니다. Transfer Family는 Transfer Family 서버 의 컨텍스트에서 이 역할을 말합니다ARN. 아웃바운드 AS2 전송의 경우 로깅 역할은 커넥터 를 사용합니다ARN.
- 실행 역할 - Transfer Family 사용자가 전화를 걸어 워크플로를 시작할 수 있습니다. Transfer Family는 Transfer Family 워크플로의 맥락에서 이 역할을 말합니다ARN.

자세한 내용은 IAM 사용 설명서의 [에서 정책 및 권한을 IAM](#) 참조하세요.

Note

다음 예에서는 각각을 바꿉니다.*user input placeholder* 자신의 정보를 사용합니다.

Note

이 예에서는 ArnLike 및 ArnEquals 모두를 사용합니다. 기능적으로 동일하므로 정책을 구성할 때 둘 중 하나를 사용할 수 있습니다. Transfer Family 설명서에서는 조건에 와일드 카드 문자가 포함된 경우에는 ArnLike를 사용하고, 정확한 일치 조건을 나타내기 위해서는 ArnEquals를 사용합니다.

AWS Transfer Family 사용자 역할 교차 서비스 혼동 대리자 방지

다음 예 정책은 계정에 있는 모든 서버의 모든 사용자가 역할을 수임하도록 허용합니다.

```
{
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": {
          "Service": "transfer.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "account-id"
          },
          "ArnLike": {
            "aws:SourceArn": "arn:aws:transfer:region:account-id:user/*"
          }
        }
      }
    ]
  }

```

다음 예 정책은 특정 서버의 모든 사용자가 역할을 수임하도록 허용합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
        }
      }
    }
  ]
}

```

```
}

```

다음 예 정책은 특정 서버의 특정 사용자가 역할을 수임하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-
id/user-name"
        }
      }
    }
  ]
}
```

AWS Transfer Family 워크플로 역할 교차 서비스 혼동 대리자 방지

다음 예 정책은 계정의 모든 워크플로가 역할을 수임하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

```

        "ArnLike": {
            "aws:SourceArn": "arn:aws:transfer:region:account-id:workflow/*"
        }
    }
}

```

다음 예 정책은 특정 워크플로가 역할을 가정하도록 허용합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:workflow/workflow-id"
        }
      }
    }
  ]
}

```

AWS Transfer Family 로깅 및 호출 역할 교차 서비스 혼동 대리자 방지

Note

다음 예는 로깅 및 호출 역할 모두에 사용할 수 있습니다.
이 예제에서는 서버에 연결된 워크플로가 없는 경우 워크플로의 ARN 세부 정보를 제거할 수 있습니다.

다음 예제 로깅/인보이스 정책을 사용하면 계정의 모든 서버(및 워크플로)가 역할을 수임할 수 있습니다.


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:region:account-id:server/*",
            "arn:aws:transfer:region:account-id:workflow/*"
          ]
        }
      }
    }
  ]
}
```

다음 예제 로깅/인보이스 정책을 사용하면 특정 서버(및 워크플로)가 역할을 수임할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnEquals": {
          "aws:SourceArn": [

```

```
    "arn:aws:transfer:region:account-id:server/server-id",
    "arn:aws:transfer:region:account-id:workflow/workflow-id"
  ]
}
}
```

AWSAWS Transfer Family에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 [AWS Identity and Access Management \(IAM\) 고객 관리형 정책을 생성하는](#) 데는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책을](#) 참조하세요. 모든 AWS 관리형 정책의 자세한 목록은 [AWS 관리형 정책 참조 가이드](#) 섹션을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책의 권한은 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트가 기존 권한을 손상시키지 않습니다.

또한 여러 서비스에 걸쳐 있는 작업 함수에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 작업 함수 정책의 목록 및 설명은 IAM 사용 설명서의 [AWS 작업 함수에 대한 관리형 정책](#)을 참조하세요.

AWS 관리형 정책: AWSTransferConsoleFullAccess

이 `AWSTransferConsoleFullAccess` 정책은 AWS 관리 콘솔을 통해 Transfer Family에 대한 전체 액세스 권한을 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `acm:ListCertificates` - 각 의 인증서 Amazon 리소스 이름(ARNs) 및 도메인 이름 목록을 검색할 수 있는 권한을 부여합니다ARN.
- `ec2:DescribeAddresses` - 하나 이상의 탄력적 IP 주소를 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeAvailabilityZones` - 사용 가능한 하나 이상의 가용 영역을 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeNetworkInterfaces` - 하나 이상의 네트워크 인터페이스를 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeSecurityGroups` - 하나 이상의 보안 그룹을 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeSubnets` - 하나 이상의 서브넷을 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeVpcs` - 하나 이상의 가상 프라이빗 클라우드()를 설명할 수 있는 권한을 부여합니다 VPCs.
- `ec2:DescribeVpcEndpoints` - 하나 이상의 VPC 엔드포인트를 설명할 수 있는 권한을 부여합니다.
- `health:DescribeEventAggregates` - 각 이벤트 타입(문제, 예약된 변경 및 계정 알림)의 이벤트 수를 반환합니다.
- `iam:GetPolicyVersion` - 정책 설명서를 포함하여 지정된 관리형 정책의 버전에 대한 정보를 검색할 권한을 부여합니다.
- `iam:ListPolicies` - 모든 관리형 정책을 나열할 권한을 부여합니다.
- `iam:ListRoles` - 지정된 경로 접두사가 있는 IAM 역할을 나열할 수 있는 권한을 부여합니다.
- `iam:PassRole` - Transfer Family에 IAM 역할을 전달할 수 있는 권한을 부여합니다. 자세한 내용은 [에 역할을 전달할 수 있는 사용자 권한 부여를 참조하세요 AWS 서비스](#).
- `route53:ListHostedZones` - 현재 AWS 계정와(과) 연계된 퍼블릭 및 프라이빗 호스팅 영역의 목록을 가져올 수 있는 권한을 부여합니다.
- `s3:ListAllMyBuckets` - 요청의 인증된 발신자가 소유한 모든 버킷을 나열할 수 있는 권한을 부여합니다.
- `transfer:*` - Transfer Family 리소스에 대한 액세스 권한을 부여합니다. 별표(*)는 모든 리소스에 대한 액세스 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "transfer.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "acm:ListCertificates",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "health:DescribeEventAggregates",
      "iam:GetPolicyVersion",
      "iam:ListPolicies",
      "iam:ListRoles",
      "route53:ListHostedZones",
      "s3:ListAllMyBuckets",
      "transfer:*"
    ],
    "Resource": "*"
  }
]
}

```

AWS 관리형 정책: AWSTransferFullAccess

또한 AWSTransferFullAccess 정책은 Transfer Family 서비스에 대한 전체 액세스 권한을 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- **transfer:*** – Transfer Family 리소스에 대한 액세스 권한을 부여합니다. 별표(*)는 모든 리소스에 대한 액세스 권한을 부여합니다.

- `iam:PassRole` – Transfer Family에 IAM 역할을 전달할 수 있는 권한을 부여합니다. 자세한 내용은 [에 역할을 전달할 수 있는 사용자 권한 부여를 참조하세요 AWS 서비스](#).
- `ec2:DescribeAddresses` – 하나 이상의 탄력적 IP 주소를 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeNetworkInterfaces` – 하나 이상의 네트워크 인터페이스를 설명할 수 있는 권한을 부여합니다.
- `ec2:DescribeVpcEndpoints` - 하나 이상의 VPC 엔드포인트를 설명할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "transfer:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AWSTransferLoggingAccess

AWSTransferLoggingAccess 정책은 AWS Transfer Family에 로그 스트림 및 그룹을 생성하고 로그 이벤트를 계정에 넣을 수 있는 전체 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 에 대한 다음 권한이 포함됩니다 Amazon CloudWatch Logs.

- `CreateLogStream` – 보안 주체에게 로그 스트림을 생성할 수 있는 권한을 부여합니다.
- `DescribeLogStreams` – 주도자에게 로그 그룹의 로그 스트림을 나열할 수 있는 권한을 부여합니다.
- `CreateLogGroup` – 보안 주체에게 로그 스트림을 생성할 수 있는 권한을 부여합니다.
- `PutLogEvents` – 보안 주체가 로그 이벤트의 배치를 로그 스트림에 업로드할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AWSTransferReadOnlyAccess

AWSTransferReadOnlyAccess 정책은 Transfer Family 서비스에 대한 읽기 전용 액세스를 제공합니다.

권한 세부 정보

이 정책에는 Transfer Family에 대한 다음 권한이 포함되어 있습니다.

- `DescribeUser` – 주도자에게 사용자의 설명을 볼 수 있는 권한을 부여합니다.
- `DescribeServer` – 주도자에게 서버에 대한 설명을 볼 수 있는 권한을 부여합니다.
- `ListUsers` – 주도자에게 서버의 사용자를 나열할 수 있는 권한을 부여합니다.
- `ListServers` – 주도자에게 계정의 서버를 나열할 수 있는 권한을 부여합니다.
- `TestIdentityProvider` – 보안 주체에게 구성된 ID 제공자가 올바르게 설정되었는지 테스트할 수 있는 권한을 부여합니다.
- `ListTagsForResource` – 주도자에게 리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSAWS 관리형 정책에 패밀리 업데이트 전송

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS Transfer Family의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 페이지의 RSS 피드를 구독하세요 [에 대한 문서 기록 AWS Transfer Family](#).

변경 사항	설명	날짜
설명서 업데이트	Transfer Family 관리 정책 각각에 대한 섹션이 추가되었습니다.	2022년 1월 27일
AWSTransferReadOnlyAccess -기존 정책 업데이트	AWS Transfer Family는 정책을 읽을 수 있는 새 권한을 추가했습니다 AWS Managed Microsoft AD.	2021년 9월 30일
AWS Transfer Family에서 변경 사항 추적 시작	AWS Transfer Family는 AWS 관리형 정책에 대한 변경 사항을 추적하기 시작했습니다.	2021년 6월 15일

문제 해결 AWS Transfer Family

다음 정보를 사용하여 로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결할 수 있습니다 AWS Transfer Family.

Transfer FamilyIAM의 와 관련된 문제는 섹션을 참조하세요 [AWS Transfer Family 자격 증명 및 액세스 문제 해결](#).

주제

- [서비스 관리 사용자 문제 해결](#)
- [Amazon API Gateway 문제 해결](#)
- [암호화된 Amazon S3 버킷에 대한 정책 문제 해결](#)
- [인증 문제 해결](#)
- [관리형 워크플로 문제 해결](#)
- [워크플로 복호화 문제 해결](#)
- [Amazon EFS 문제 해결](#)
- [ID 제공자 테스트 문제 해결](#)
- [SFTP 커넥터에 대해 신뢰할 수 있는 호스트 키 추가 문제 해결](#)
- [파일 업로드 문제 해결](#)
- [ResourceNotFound 예외 문제 해결](#)
- [SFTP 커넥터 문제 해결](#)
- [AS2 문제 해결](#)

서비스 관리 사용자 문제 해결

이 섹션에서는 다음 문제에 대한 가능한 해결 방법을 설명합니다.

주제

- [Amazon EFS 서비스 관리형 사용자 문제 해결](#)
- [퍼블릭 키 본문이 너무 긴 문제 해결](#)
- [SSH 퍼블릭 키를 추가하지 못한 문제 해결](#)

Amazon EFS 서비스 관리형 사용자 문제 해결

설명

sftp 명령을 실행하면 프롬프트가 나타나지 않고 대신 다음 메시지가 표시됩니다:

```
Couldn't canonicalize: Permission denied
Need cwd
```

원인

AWS Identity and Access Management (IAM) 사용자의 역할에 Amazon Elastic File System(Amazon)에 액세스할 수 있는 권한이 없습니다EFS.

솔루션

사용자 역할에 대한 정책 권한을 늘리세요. 와 같은 AWS 관리형 정책을 추가할 수 있습니다AmazonElasticFileSystemClientFullAccess.

퍼블릭 키 본문이 너무 긴 문제 해결

설명

서비스 관리 사용자를 생성하려고 하면 다음 오류가 발생합니다:

```
Failed to create user (1 validation error detected:
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or
equal to 2048)
```

원인

퍼블릭 PGP 키 본문에 키를 입력하는 중일 수 있으며 AWS Transfer Family 는 서비스 관리형 사용자에 대한 PGP 키를 지원하지 않습니다.

솔루션

PGP 키가 RSA기반인 경우 PEM 형식으로 변환할 수 있습니다. 예를 들어 Ubuntu는 <https://manpages.ubuntu.com/manpages/xenial/man1/openpgp2ssh.1.html>에서 변환 도구를 제공합니다.

SSH 퍼블릭 키를 추가하지 못한 문제 해결

설명

서비스 관리 사용자에게 대한 퍼블릭 키를 추가하려고 하면 다음 오류가 발생합니다:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

원인

SSH2형식이 지정된 퍼블릭 키를 가져오려고 할 수 있으며 서비스 관리형 사용자에게는 SSH2형식이 지정된 퍼블릭 키를 지원하지 AWS Transfer Family 않습니다.

솔루션

키를 OpenSSH 형식으로 변환해야 합니다. 이 과정은 [SSH2 퍼블릭 키를 PEM 형식으로 변환](#)에 설명되어 있습니다.

Amazon API Gateway 문제 해결

이 섹션에서는 다음 API Gateway 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [인증 오류가 너무 많음](#)
- [연결 종료](#)

인증 오류가 너무 많음

설명

Secure Shell(SSH) 파일 전송 프로토콜()을 사용하여 서버에 연결하려고 SFTP하면 다음 오류가 발생합니다.

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

원인

잘못된 데이터베이스 사용자 암호를 입력했을 수 있습니다. 올바른 암호를 다시 입력해 보세요.

암호가 올바른 경우 유효하지 않은 Amazon 리소스 이름(ARN) 역할로 인해 문제가 발생할 수 있습니다. 이것이 문제인지 확인하려면 서버의 ID 공급자를 테스트하세요. 다음과 유사한 응답이 표시되는 경우 역할은 모든 0의 역할 ID 값으로 표시되는 ARN 자리 표시자만 됩니다.

```
{
  "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\"
}
```

솔루션

자리 표시자 역할을 서버에 액세스할 수 있는 권한이 있는 ARN 실제 역할로 바꿉니다.

역할을 업데이트하려면

1. <https://console.aws.amazon.com/cloudformation>에서 AWS CloudFormation 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 스택을 선택합니다.
3. 스택 목록에서 스택을 선택한 다음 파라미터 탭을 선택합니다.
4. 업데이트를 선택합니다. 업데이트 스택 페이지에서 현재 템플릿 사용을 선택하고 다음을 선택합니다.
5. Transfer Family 서버에 액세스할 수 있는 충분한 권한이 ARN 있는 역할UserRoleArn로 를 바꿉니다.

Note

필요한 권한을 부여하려면 AmazonAPIGatewayAdministrator 및 AmazonS3FullAccess 관리형 정책을 역할에 추가할 수 있습니다.

6. 다음을 선택하고 다시 다음을 선택합니다. 검토에서 **stack** 페이지에서 이 IAM 리소스를 생성할 AWS CloudFormation 수 있음을 인정함을 선택한 다음 스택 업데이트를 선택합니다.

연결 종료

설명

Secure Shell(SSH) 파일 전송 프로토콜()을 사용하여 서버에 연결하려고 SFTP하면 다음 오류가 발생합니다.

Connection closed

원인

이 문제의 가능한 원인 중 하나는 Amazon CloudWatch 로깅 역할이 Transfer Family와 신뢰 관계가 없기 때문입니다.

솔루션

서버의 로깅 역할이 Transfer Family와 신뢰 관계를 맺고 있는지 확인하세요. 자세한 내용은 [신뢰 관계를 구축하기 위해](#)를 참조하세요.

암호화된 Amazon S3 버킷에 대한 정책 문제 해결

설명

Transfer Family 서버의 스토리지로 사용하고 있는 암호화된 Amazon S3 버킷이 있습니다. 서버에 파일을 업로드하려고 하면 오류 Couldn't close file: Permission denied가 발생합니다.

그리고 서버 로그를 보면 다음과 같은 오류가 표시됩니다:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

원인

IAM 사용자의 정책에는 암호화된 버킷에 액세스할 수 있는 권한이 없습니다.

솔루션

요구되는 AWS Key Management Service (AWS KMS) 권한을 부여하려면 정책에 추가 권한을 지정해야 합니다. 자세한 내용은 [Amazon S3의 데이터 암호화](#)를 참조하세요.

인증 문제 해결

이 섹션에서는 다음 인증 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [인증 실패—SSH/SFTP](#)

- [관리형 AD 불일치 영역 문제](#)
- [기타 인증 문제](#)

인증 실패—SSH/SFTP

설명

Secure Shell(SSH) 파일 전송 프로토콜()을 사용하여 서버에 연결하려고 SFTP하면 다음과 비슷한 메시지가 표시됩니다.

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

API 게이트웨이를 사용하고 있고 이 오류가 발생하는 경우 섹션을 참조하세요 [인증 오류가 너무 많음](#).

원인

사용자를 위한 RSA 키 페어를 추가하지 않았으므로 대신 암호를 사용하여 인증해야 합니다.

솔루션

sftp 명령은 -o PubkeyAuthentication=no 옵션을 지정할 때 실행됩니다. 이 옵션을 선택하면 시스템에서 강제로 암호를 요청합니다. 예:

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

관리형 AD 불일치 영역 문제

설명

사용자의 영역과 그룹 영역이 일치해야 합니다. 둘 다 기본 영역에 있거나 둘 다 신뢰할 수 있는 영역에 있어야 합니다.

원인

사용자와 그룹이 일치하지 않는 경우 Transfer Family에서 사용자를 인증할 수 없습니다. 사용자의 ID 공급자를 테스트하면 사용자 그룹에 연결된 액세스 권한을 찾을 수 없음이라는 오류 메시지가 표시됩니다.

솔루션

사용자 영역에서 그룹 영역(기본값 또는 신뢰할 수 있음)과 일치하는 그룹을 참조합니다.

기타 인증 문제

설명

인증 오류가 발생했지만 다른 문제 해결은 작동하지 않습니다.

원인

선행 또는 후행 슬래시(/)가 포함된 논리 디렉터리의 대상을 지정했을 수 있습니다.

솔루션

논리적 디렉터리 대상을 업데이트하여 슬래시로 시작하고 후행 슬래시를 포함하지 않도록 하세요. 예를 들어 `/DOC-EXAMPLE-BUCKET/images`는 허용되지만 `DOC-EXAMPLE-BUCKET/images /DOC-EXAMPLE-BUCKET/images/`는 허용되지 않습니다.

관리형 워크플로 문제 해결

이 섹션에서는 다음 워크플로 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [Amazon을 사용하여 워크플로 관련 오류 해결 CloudWatch](#)
- [워크플로 복사 오류 문제 해결](#)

Amazon을 사용하여 워크플로 관련 오류 해결 CloudWatch

설명

워크플로에 문제가 있는 경우 Amazon CloudWatch 을 사용하여 원인을 조사할 수 있습니다.

원인

원인은 여러 가지가 있을 수 있습니다. Amazon CloudWatch Logs를 사용하여 조사합니다.

솔루션

Transfer Family는 워크플로 실행 상태를 CloudWatch 로그로 내보냅니다. CloudWatch 로그에는 다음과 같은 유형의 워크플로 오류가 나타날 수 있습니다.

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

다양한 필터 및 패턴 구문을 사용하여 워크플로의 실행 로그를 필터링할 수 있습니다. 예를 들어 CloudWatch 로그에 로그 필터를 생성하여 ExecutionErrored 메시지가 포함된 워크플로 실행 로그를 캡처할 수 있습니다. 자세한 내용은 Amazon [Logs 사용 설명서의 구독 및 필터 및 패턴 구문을 사용한 로그 데이터의 실시간 처리](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html)를 참조하세요. <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html> CloudWatch

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"}
```

여기서 StepErrored는 워크플로 내의 한 단계에서 오류가 발생했음을 나타냅니다. 단일 워크플로에서 여러 단계를 구성할 수 있습니다. 이 오류는 오류가 발생한 단계를 알려주고 오류 메시지를 제공합니다. 이 특정 예제에서는 단계에 파일에 태그를 지정하도록 구성되었지만 Amazon EFS 파일 시스템에서 파일에 태그를 지정하면 지원되지 않으므로 단계에서 오류가 발생했습니다.

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"}}
```

워크플로에서 어떤 단계도 실행할 수 없는 경우 `ExecutionErrored` 메시지가 생성됩니다. 예를 들어, 특정 워크플로에서 단일 단계를 구성했는데 해당 단계를 실행할 수 없는 경우 전체 워크플로가 실패합니다.

Executionthrottled

시스템에서 지원할 수 있는 속도보다 빠른 속도로 워크플로가 트리거되면 실행이 제한됩니다. 이 로그 메시지는 워크플로의 실행 속도를 늦춰야 함을 나타냅니다. 워크플로 실행 속도를 축소할 수 없는 경우 [문의 AWS](#) AWS Support 로 문의하세요.

워크플로 시작 시 서비스 실패

서버에서 워크플로를 제거하고 새 워크플로로 바꾸거나 워크플로의 실행 역할에 영향을 미치는 서버 구성을 업데이트할 때마다 새 워크플로를 실행하기 전에 약 10분을 기다려야 합니다. Transfer Family 서버는 워크플로 세부 정보를 캐시하며 서버가 캐시를 새로 고치는 데 10분이 걸립니다.

또한 활성 SFTP 세션에서 로그아웃한 다음 10분 대기 기간 후에 다시 로그인하여 변경 사항을 확인해야 합니다.

워크플로 복사 오류 문제 해결

설명

업로드된 파일을 복사하는 단계가 포함된 워크플로를 실행하는 경우 다음 오류가 발생할 수 있습니다:

```
{
  "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"
    }
  }
}
```

원인

소스 파일은 대상 버킷과 다른 Amazon S3 버킷 AWS 리전 에 있습니다.

솔루션

복사 단계가 포함된 워크플로를 실행하는 경우, 소스 버킷과 목적지 버킷이 동일한 AWS 리전안에 있는지 확인하세요.

워크플로 복호화 문제 해결

설명

복호화 워크플로가 실패하고 로그 메시지가 다음과 비슷합니다:

```
{
  "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"
  }
}
```

원인

Transfer Family 서버에 FIPS 모드가 활성화되어 있고 관련 복호화 워크플로 단계가 있습니다.

Transfer Family 서버에 업로드하기 전에 파일을 암호화할 때 암호화 클라이언트는 승인되지FIPS 않은 대칭 암호화 알고리즘을 사용하는 암호화된 파일을 생성할 수 있습니다. 이러한 시나리오에서는 워크플로에서 파일을 해독할 수 없습니다. 다음 예제에서 GnuPG 버전 2.4.0은 OCB (비FIPS 블록 암호 모드)를 사용하여 파일을 암호화합니다. 이렇게 하면 워크플로가 실패합니다.

솔루션

파일을 암호화하는 데 사용한 GPG 키를 편집한 다음 다시 암호화해야 합니다. 다음 절차는 취해야 하는 단계를 설명합니다.

PGP 키를 편집하려면

1. `gpg --list-keys`를 실행하여 편집해야 하는 키를 식별합니다.

그러면 키 목록이 반환됩니다. 각 키에는 다음과 유사한 세부 정보가 있습니다.

```
pub   ed25519 2022-07-07 [SC]
      wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
uid           [ultimate] Mary Major <marymajor@example.com>
sub   cv25519 2022-07-07 [E]
```

2. 편집할 키를 식별합니다. 이전 단계에 표시된 예에서 ID는 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`입니다.
3. `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`를 실행합니다.

시스템은 GnuPG 프로그램 및 지정된 키에 대한 세부 정보로 응답합니다.

4. `gpg>` 프롬프트에서 `showpref`를 입력합니다. 다음과 같은 세부 정보가 반환됩니다:

```
[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
```

참고로, 키에 저장된 선호 알고리즘이 나열되어 있습니다.

5. 키를 편집하여 를 제외한 모든 알고리즘을 유지하려고 합니다OCB. `setpref` 명령을 실행하여 유지할 모든 알고리즘을 지정합니다:

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
      BZIP2, ZIP, Uncompressed
```

그러면 다음 세부 사항이 반환됩니다:

```
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. y를 입력하여 업데이트한 다음, 변경을 확인하라는 메시지가 표시되면 암호를 입력합니다.
7. 변경 사항을 저장합니다.

```
gpg> save
```

복호화 워크플로를 다시 실행하기 전에 편집한 키를 사용하여 파일을 다시 암호화해야 합니다.

Amazon EFS 문제 해결

이 섹션에서는 다음 Amazon EFS 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [누락된 POSIX 프로파일 문제 해결](#)
- [Amazon을 사용한 논리적 디렉터리 문제 해결 EFS](#)

누락된 POSIX 프로파일 문제 해결

설명

서버에 Amazon EFS 스토리지를 사용하고 사용자 지정 자격 증명 공급자를 사용하는 경우 AWS Lambda 함수에 POSIX 프로파일을 제공해야 합니다.

원인

가능한 한 가지 원인은 AWS Lambda지원되는 Amazon API Gateway 메서드를 생성하기 위해 제공하는 템플릿에 현재 POSIX 정보가 포함되어 있지 않기 때문입니다.

POSIX 정보를 제공한 경우 정보를 제공하는 데 사용한 형식이 Transfer Family에서 올바르게 구문 분석되지 않을 POSIX 수 있습니다.

솔루션

PosixProfile 파라미터의 Transfer Family에 JSON 요소를 제공하는지 확인합니다.

예를 들어, Python을 사용하는 경우 PosixProfile 파라미터를 파싱하는 위치에 다음 줄을 추가할 수 있습니다.

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

또는 에서 다음 줄을 추가할 JavaScript수 있습니다. 여기서 *uid-value* 및 *gid-value*는 각각 사용자 ID(UID) 및 그룹 ID(GID)를 나타내는 0 이상의 정수입니다.

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

이러한 코드 예제는 PosixProfile 파라미터를 문자열이 아닌 JSON 객체로 Transfer Family에 전송합니다.

또한 내에서 다음과 같이 PosixProfile 파라미터를 저장 AWS Secrets Manager해야 합니다. *your-uid* 및 *your-gid* 를 GID 및 의 실제 값으로 바꿉니다UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Amazon을 사용한 논리적 디렉터리 문제 해결 EFS

설명

사용자의 홈 디렉터리가 존재하지 않고 사용자가 `ls` 명령을 실행하면 시스템은 다음과 같이 응답합니다:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

원인

Transfer Family 서버가 Amazon 를 사용하는 경우 사용자가 논리적 EFS홈 디렉터리에서 작업하기 전에 읽기 및 쓰기 액세스 권한으로 사용자의 홈 디렉터리를 생성해야 합니다. 사용자는 논리적 홈 디렉터리 상의 `mkdir`에 대한 권한이 없기 때문에 이 디렉터리를 직접 만들 수는 없습니다.

솔루션

상위 디렉터리에 대한 관리 액세스 권한이 있는 사용자는 사용자의 논리적 홈 디렉터리를 생성해야 합니다.

ID 제공자 테스트 문제 해결

설명

콘솔 또는 TestIdentityProvider API 호출을 사용하여 자격 증명 공급자를 테스트하면 Response 필드가 비어 있습니다. 예:

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

원인

가장 가능성이 높은 원인은 잘못된 사용자 이름이나 암호로 인해 인증이 실패했기 때문입니다.

솔루션

사용자에 대한 올바른 자격 증명을 사용하고 있는지 확인하고 필요한 경우 사용자 이름 또는 암호를 업데이트하세요.

SFTP 커넥터에 대해 신뢰할 수 있는 호스트 키 추가 문제 해결

설명

SFTP 커넥터를 생성하거나 편집하고 신뢰할 수 있는 호스트 키를 추가하면 다음 오류가 발생합니다. Failed to edit connector details (Invalid host key format.)

원인

올바른 퍼블릭 키에 붙여넣는 경우 키의 comment 일부를 포함했다는 문제가 발생할 수 있습니다. 현재 키의 주석 부분을 수락하지 AWS Transfer Family 않습니다.

솔루션

키를 텍스트 필드에 붙여넣을 때 키의 설명 부분을 삭제하세요. 예를 들어, 키는 다음과 비슷할 것입니다:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

== 문자 뒤에 오는 텍스트를 제거하고, 키에서 == 문자 앞까지 오는 부분만 붙여넣습니다.

```
ssh-rsa AAAA...==
```

파일 업로드 문제 해결

이 섹션에서는 다음 파일 업로드 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [Amazon S3 파일 업로드 오류 문제 해결](#)
- [읽을 수 없는 파일 명칭 문제 해결](#)

Amazon S3 파일 업로드 오류 문제 해결

설명

Transfer Family를 사용하여 Amazon S3 스토리지에 파일을 업로드하려고 하면 다음과 같은 오류 메시지가 나타납니다: AWS Transfer는 S3 객체에 대한 임의 액세스 쓰기를 지원하지 않음.

원인

Amazon S3를 서버 스토리지로 사용하는 경우 Transfer Family는 단일 전송에 대한 복수 연결을 지원하지 않습니다.

솔루션

Transfer Family 서버가 Amazon S3를 스토리지로 사용하는 경우 단일 전송에 복수 연결을 사용한다고 언급하는 클라이언트 소프트웨어 옵션을 비활성화하세요.

읽을 수 없는 파일 명칭 문제 해결

설명

업로드한 파일 중 일부에 손상된 파일 명칭이 있습니다. 사용자는 umlauts, 악센트가 지정된 문자 또는 중국어나 아랍어와 같은 특정 스크립트와 같은 파일 이름의 특정 문자를 왜곡하는 FTP와 SFTP 전송에 문제가 발생하는 경우가 있습니다.

원인

FTP 및 SFTP 프로토콜을 사용하면 클라이언트가 파일 이름을 문자 인코딩할 수 있지만 Amazon S3와 AmazonEFS는 협상하지 않습니다. 대신 UTF-8자 인코딩이 필요합니다. 따라서 특정 문자가 제대로 렌더링되지 않습니다.

솔루션

이 문제를 해결하려면 클라이언트 애플리케이션에서 파일 이름 문자 인코딩을 검토하고 UTF-8로 설정되어 있는지 확인합니다.

ResourceNotFound 예외 문제 해결

설명

리소스를 찾을 수 없는 오류가 발생합니다. 예를 들어 UpdateServer를 실행하면 다음과 같은 오류가 발생할 수 있습니다:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:
Unknown server
```

원인

ResourceNotFoundException 메시지를 수신하는 데는 여러 가지 이유가 있습니다. 대부분의 경우 API 명령에 지정한 리소스가 존재하지 않습니다. 기존 리소스를 지정한 경우 가장 가능성이 높은 원인은 기본 지역이 리소스의 지역과 다르기 때문입니다. 예를 들어 기본 지역이 us-east-1이고 Transfer Family 서버가 us-east-2에 있는 경우 알 수 없는 리소스 예외가 발생합니다.

기본 지역 설정에 대한 자세한 설명은 [aws configure를 통한 빠른 구성](#)을 참조하세요.

솔루션

API 명령에 리전 파라미터를 추가하여 특정 리소스를 찾을 위치를 명시적으로 지정합니다.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

SFTP 커넥터 문제 해결

이 섹션에서는 다음 SFTP 커넥터 문제에 대해 가능한 해결 방법을 설명합니다.

주제

- [키 협상 실패](#)
- [기타 SFTP 커넥터 문제](#)

키 협상 실패

설명

키 교환 협상이 실패하는 오류가 발생합니다. 예:

```
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]
```

원인

이 오류는 서버에서 지원하는 호스트 키 알고리즘과 커넥터에서 지원하는 호스트 키 알고리즘이 겹치지 않기 때문입니다.

솔루션

원격 서버가 오류 메시지에 나열된 클라이언트 호스트 키 알고리즘 중 하나 이상을 지원하는지 확인하세요. 지원되는 키 알고리즘 목록은 [SFTP 커넥터 알고리즘](#) 섹션을 참조하세요.

기타 SFTP 커넥터 문제

설명

를 실행한 후 오류가 발생StartFileTransfer하지만 문제의 원인을 알 수 없으며 API 호출 후에는 커넥터 ID만 반환됩니다.

원인

이 오류에는 여러 원인이 있을 수 있습니다. 문제를 해결하려면 커넥터를 테스트하고 CloudWatch 로그를 검색하는 것이 좋습니다.

솔루션

- 커넥터 테스트: 단원을 참조하세요[SFTP 커넥터 테스트](#). 테스트가 실패하면 시스템은 테스트 실패 이유를 기반으로 오류 메시지를 제공합니다. 이 섹션에서는 콘솔에서 또는 를 사용하여 커넥터를 테스트하는 방법을 설명합니다. [TestConnection](#) API 명령.

- 커넥터에 대한 CloudWatch 로그 보기: 참조[SFTP 커넥터의 로그 항목 예](#). 이 주제에서는 SFTP 커넥터 로그 항목에 대한 예제와 적절한 로그를 찾는 데 도움이 되는 명령 규칙을 제공합니다.

AS2 문제 해결

적용 설명서 2(AS2) 지원 서버에 대한 오류 메시지 및 문제 해결 팁은 [여기](#)에 설명되어 있습니다.[AS2 오류 코드](#).

API 참조

다음 섹션에서는 서비스 호출, 데이터 유형, 파라미터 및 오류를 문서화합니다 AWS Transfer Family API.

주제

- [에 오신 것을 환영합니다. AWS Transfer Family API](#)
- [작업](#)
- [데이터 유형](#)
- [API 요청 만들기](#)
- [공통 파라미터](#)
- [일반적인 오류](#)

에 오신 것을 환영합니다. AWS Transfer Family API

AWS Transfer Family 는 다음 프로토콜을 통해 Amazon Simple Storage Service(Amazon S3) 스토리지로 파일을 송수신하는 데 사용할 수 있는 보안 전송 서비스입니다.

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP)
- 파일 전송 프로토콜 보안(FTPS)
- 파일 전송 프로토콜(FTP)
- 적용 가능성 설명 2(AS2)

파일 전송 프로토콜은 금융 서비스, 의료, 광고, 소매 등 다양한 산업의 데이터 교환 워크플로에 사용됩니다. AWS Transfer Family 는 파일 전송 워크플로를 로 마이그레이션하는 것을 간소화합니다 AWS.

AWS Transfer Family 서비스를 사용하려면 선택한 AWS 리전에서 서버를 인스턴스화합니다. 서버를 생성하고, 가용 서버를 나열하고, 서버를 업데이트하고 삭제할 수 있습니다. 서버는 에서 파일 작업을 요청하는 엔터티입니다 AWS Transfer Family. 서버에는 수많은 중요 속성이 존재합니다. 서버는 시스템이 할당한 ServerId 식별자로 확인하는 이름이 지정된 인스턴스입니다. 옵션으로, 서버에 호스트 이름을 할당할 수 있습니다. 사용자 지정 호스트 이름도 가능합니다. 이 서비스는 인스턴스화한 서버(심지어 OFFLINE 서버 포함)와 전송한 데이터 양에 대한 요금을 청구합니다.

사용자는 파일 작업을 요청하는 서버가 알고 있어야 합니다. 사용자 이름으로 식별한 사용자가 서버에 할당됩니다. 사용자 이름은 요청을 인증할 때 사용됩니다. 서버는 인증 메서드로

AWS_DIRECTORY_SERVICE, SERVICE_MANAGED, AWS_LAMBDA, 또는 API_GATEWAY 중 오직 하나만 사용할 수 있습니다.

다음과 같은 ID 제공자 타입을 사용하여 사용자를 인증할 수 있습니다.

- 의 경우 SERVICE_MANAGED SSH 퍼블릭 키는 서버의 사용자 속성과 함께 저장됩니다. 사용자는 SERVICE_MANAGED 인증 방법에 대한 SSH 퍼블릭 키를 파일에 하나 이상 보유할 수 있습니다. 클라이언트가 SERVICE_MANAGED 메서드에 대한 파일 작업을 요청하면 클라이언트는 인증된 사용자 이름과 SSH 프라이빗 키를 제공하고 액세스 권한이 제공됩니다.
- AWS_DIRECTORY_SERVICE 인증 방법을 선택하여 Microsoft Active Directory 그룹을 사용하여 사용자 인증 및 액세스를 관리할 수 있습니다.
- 를 사용하여 사용자 지정 자격 증명 공급자에 연결할 수 있습니다 AWS Lambda. AWS_LAMBDA 인증 방법을 선택합니다.
- 사용자 인증과 액세스를 모두 제공하는 사용자 지정 인증 메서드를 이용해 사용자 요청을 인증할 수도 있습니다. 이 방법은 Amazon API Gateway를 사용하여 자격 증명 공급자의 API 호출을 사용하여 사용자 요청을 검증합니다. 이 메서드는 API 호출 API_GATEWAY에서 로, 콘솔에서 사용자 지정으로 지칭됩니다. 이 사용자 지정 메서드를 이용해 디렉터리 서비스, 데이터베이스 이름과 암호 쌍 또는 기타 메커니즘에 대해 사용자를 인증할 수도 있습니다.

사용자에는 사용자 자신과 Amazon S3 버킷 간의 신뢰 관계를 제공하는 정책이 할당됩니다. 사용자는 버킷 전체 또는 일부에 액세스할 수 있습니다. 서버가 사용자를 대신해 작동하려면, 서버는 사용자로부터 신뢰 관계를 상속받아야 합니다. 신뢰 관계가 포함된 AWS Identity and Access Management (IAM) 역할이 생성되고 해당 역할에 AssumeRole 작업이 할당됩니다. 그런다음 서버는 마치 사용자인 것처럼 파일 작업을 수행할 수 있습니다.

home 디렉터리 속성을 설정한 사용자는 해당 디렉터리(또는 폴더)가 파일 작업의 대상 및 원본으로 작동하게 해야 합니다. home 디렉터리가 설정되지 않았다면, 버킷의 root 디렉터리가 랜딩 디렉터리가 됩니다.

서버, 사용자 및 역할은 모두 Amazon 리소스 이름()으로 식별됩니다ARN. 키-값 페어인 태그를 가 있는 엔터티에 할당할 수 있습니다ARN. 태그는 이러한 개체(entity)를 그룹화하고 검색하는 데 사용할 수 있는 메타데이터입니다. 태그를 유용하게 사용할 수 있는 대표적인 분야는 회계입니다.

다음 규칙은 AWS Transfer Family ID 형식으로 관찰됩니다.

- s-01234567890abcdef 양식에서 얻은 ServerId 값
- key-01234567890abcdef 양식에서 얻은 SshPublicKeyId 값

Amazon 리소스 이름(ARN) 형식은 다음 형식을 따릅니다.

- 서버의 경우 양식을 ARNs 사용합니다 `arn:aws:transfer:region:account-id:server/server-id`.

서버의 예는 ARN입니다 `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- 사용자의 경우 양식을 ARNs 가져옵니다 `arn:aws:transfer:region:account-id:user/server-id/username`.

예를 들면, `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`입니다.

DNS 사용 중인 항목(평가변수)은 다음과 같습니다.

- API 엔드포인트는 양식을 사용합니다 `transfer.region.amazonaws.com`.
- `server.transfer.region.amazonaws.com` 형식을 취하는 서버 엔드포인트

AWS 리전별 Transfer Family 엔드포인트 목록은 의 [AWS Transfer Family 엔드포인트 및 할당량을 참조하세요](#) AWS 일반 참조.

에 대한 이 API 인터페이스 참조에는 를 관리하는 데 사용할 수 있는 프로그래밍 인터페이스에 대한 설명서가 AWS Transfer Family 포함되어 있습니다 AWS Transfer Family. 참조 구조는 다음과 같습니다.

- API 작업의 알파벳순 목록은 섹션을 참조하세요. [Actions](#).
- 데이터 유형의 알파벳순 목록은 섹션을 참조하세요. [Data Types](#).
- 공통 쿼리 파라미터 목록은 [공통 파라미터](#)를 참조하세요.
- 오류 코드에 대한 설명은 [공통 오류](#)를 참조하세요.

Tip

실제로 명령을 실행하는 대신 API 호출과 함께 `--generate-cli-skeleton` 파라미터를 사용하여 파라미터 템플릿을 생성하고 표시할 수 있습니다. 그런 다음 생성된 템플릿을 사용하여 사용자 정의하고 이후 명령의 입력으로 사용할 수 있습니다. 자세한 내용은 [파라미터 스켈레톤 파일 생성 및 사용](#)을 참조하세요.

작업

다음 작업이 지원됩니다.

- [CreateAccess](#)
- [CreateAgreement](#)
- [CreateConnector](#)
- [CreateProfile](#)
- [CreateServer](#)
- [CreateUser](#)
- [CreateWorkflow](#)
- [DeleteAccess](#)
- [DeleteAgreement](#)
- [DeleteCertificate](#)
- [DeleteConnector](#)
- [DeleteHostKey](#)
- [DeleteProfile](#)
- [DeleteServer](#)
- [DeleteSshPublicKey](#)
- [DeleteUser](#)
- [DeleteWorkflow](#)
- [DescribeAccess](#)
- [DescribeAgreement](#)
- [DescribeCertificate](#)
- [DescribeConnector](#)
- [DescribeExecution](#)
- [DescribeHostKey](#)
- [DescribeProfile](#)
- [DescribeSecurityPolicy](#)
- [DescribeServer](#)
- [DescribeUser](#)

- [DescribeWorkflow](#)
- [ImportCertificate](#)
- [ImportHostKey](#)
- [ImportSshPublicKey](#)
- [ListAccesses](#)
- [ListAgreements](#)
- [ListCertificates](#)
- [ListConnectors](#)
- [ListExecutions](#)
- [ListHostKeys](#)
- [ListProfiles](#)
- [ListSecurityPolicies](#)
- [ListServers](#)
- [ListTagsForResource](#)
- [ListUsers](#)
- [ListWorkflows](#)
- [SendWorkflowStepState](#)
- [StartFileTransfer](#)
- [StartServer](#)
- [StopServer](#)
- [TagResource](#)
- [TestConnection](#)
- [TestIdentityProvider](#)
- [UntagResource](#)
- [UpdateAccess](#)
- [UpdateAgreement](#)
- [UpdateCertificate](#)
- [UpdateConnector](#)
- [UpdateHostKey](#)
- [UpdateProfile](#)

- [UpdateServer](#)
- [UpdateUser](#)

CreateAccess

관리자가 디렉터리에서 `를 사용하여 활성화된 프로토콜을 통해 파일을 업로드하고 다운로드할 수 있는 액세스 권한을 가질 그룹을 선택하는 데 사용됩니다` AWS Transfer Family. 예를 들어, Microsoft Active Directory에는 50,000명의 사용자가 있을 수 있지만 서버에 파일을 전송할 수 있는 기능은 극히 일부만 필요할 수 있습니다. 관리자는 `CreateAccess`를 필요로 하는 올바른 사용자 집합으로 액세스를 제한하는 데 사용할 수 있습니다.

구문 요청

```
{
  "ExternalId": "string",
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ExternalId

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자는 `를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다`

다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

이 명령에서 YourGroupName 를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =, ., @, /, - 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 예

[HomeDirectory](#)

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

[HomeDirectoryMappings](#)

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서는

경로가 어떻게 표시되는 Entry지, 는 실제 Amazon S3 또는 Amazon EFS 경로 Target입니다. 대상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할 이 의 경로에 대한 액세스를 제공하는지 확인해야 합니다 Target. 이 값은 이 로 설정된 경우에만 HomeDirectoryType 설정할 수 있습니다 LOGICAL.

다음은 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

대부분의 경우 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리("chroot")로 제한할 수 있습니다. 이렇게 하려면 Entry을 /로 설정하고, Target을 HomeDirectory 파라미터 값으로 설정하면 됩니다.

다음은 chroot에 대한 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

타입: [HomeDirectoryMapEntry](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

[HomeDirectoryType](#)

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시하는 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

Policy

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 하는 사용자에게 대한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

Note

이 정책은 `ServerId`의 도메인이 Amazon S3인 경우에만 적용됩니다. AmazonEFS은 세션 정책을 사용하지 않습니다.

세션 정책의 경우 는 정책의 Amazon 리소스 이름(ARN) 대신 정책을 JSON 블록으로 AWS Transfer Family 저장합니다. 정책을 JSON blob으로 저장하고 Policy 인수에 전달합니다. 세션 정책의 예는 [세션 정책 예](#)를 참조하세요.

자세한 내용은 참조 [AssumeRole](#)의 섹션을 참조하세요. AWS Security Token Service API

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

PosixProfile

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정

책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

Pattern: `arn:.*role/\S+`

필수 여부: 예

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이 항목은 사용자를 추가한 특정 서버입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `s-([0-9a-f]{17})`

필수 여부: 예

응답 구문

```
{
  "ExternalId": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ExternalId

를 사용하여 활성화된 프로토콜을 통해 사용자가 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있는 그룹의 외부 식별자입니다 AWS Transfer Family.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

ServerId

사용자가 연결된 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateAgreement

계약을 생성합니다. 계약은 AWS Transfer Family 서버와 AS2 프로세스 간의 양자 거래 파트너 계약 또는 파트너십입니다. 계약은 서버와 AS2 프로세스 간의 파일 및 메시지 전송 관계를 정의합니다. 계약을 정의하기 위해 Transfer Family는 서버, 로컬 프로필, 파트너 프로필, 인증서 및 기타 속성을 결합합니다.

파트너는 로 식별PartnerProfileId되고 AS2 프로세스는 로 식별됩니다LocalProfileId.

구문 요청

```
{
  "AccessRole": "string",
  "BaseDirectory": "string",
  "Description": "string",
  "LocalProfileId": "string",
  "PartnerProfileId": "string",
  "ServerId": "string",
  "Status": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[AccessRole](#)

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출StartFileTransfer하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2수 있습니다SendFilePaths. 파일의 상위 디렉터리(예: 의 경우 --send-file-

`paths /bucket/dir/file.txt` 상위 디렉터리는 `/bucket/dir/`를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 `AccessRole`은(는) `StartFileTransfer` 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 `StartFileTransfer`와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 `secretsmanager:GetSecretValue` 권한이 필요합니다. Secrets Manager의 AWS 관리형 키 대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 `kms:Decrypt` 권한이 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 `StartFileTransfer` 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 `secretsmanager:GetSecretValue` 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

Pattern: `arn:.*role/\S+`

필수 여부: 예

[BaseDirectory](#)

AS2 프로토콜을 사용하여 전송된 파일의 랜딩 디렉터리(폴더)입니다.

`BaseDirectory`의 예: `/DOC-EXAMPLE-BUCKET/home/mydirectory`

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

Pattern: `(|/.*)`

필수 여부: 예

[Description](#)

계약을 식별하는 데 사용되는 명칭 또는 간단한 설명입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: `[\p{Graph}]+`

Required: No

LocalProfileId

AS2 로컬 프로필의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `p-([0-9a-f]{17})`

필수 여부: 예

PartnerProfileId

계약에 사용되는 파트너 프로필의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `p-([0-9a-f]{17})`

필수 여부: 예

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이는 계약에서 사용하는 특정 서버를 나타냅니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `s-([0-9a-f]{17})`

필수 여부: 예

Status

구성 요소의 상태입니다. 계약은 ACTIVE 또는 INACTIVE 둘 중 하나일 수 있습니다.

타입: 문자열

유효 값: ACTIVE | INACTIVE

필수 여부: 아니요

Tags

계약을 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

응답 구문

```
{
  "AgreementId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[AgreementId](#)

계약의 고유 식별자입니다. 이 ID를 사용하여 계약을 삭제하거나 업데이트할 뿐만 아니라 계약 ID를 지정해야 하는 다른 API 모든 통화에서도 이 ID를 사용합니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: a-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 계약을 생성하고 계약 ID를 반환합니다.

```
aws transfer create-agreement --server-id s-021345abcdef6789 --local-profile-id p-1234567890abcdef0 --partner-profile-id p-abcdef01234567890 --base-folder /DOC-EXAMPLE-BUCKET/AS2-files --access-role arn:aws:iam::111122223333:role/AS2-role
```

샘플 응답

API 호출은 새 계약의 계약 ID를 반환합니다.

```
{
  "AgreementId": "a-11112222333344444"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateConnector

AS2 또는 SFTP 프로토콜에 대한 연결 파라미터를 캡처하는 커넥터를 생성합니다. AS2의 경우 외부 호스팅 AS2 서버로 파일을 전송하려면 커넥터가 필요합니다. 이 경우 SFTP서버로 파일을 보내거나 SFTP 서버에서 파일을 수신할 때 커넥터가 필요합니다. 커넥터에 대한 자세한 내용은 [AS2 커넥터 구성](#) 및 [SFTP 커넥터 생성 단원](#)을 참조하세요.

Note

(As2Config) 또는 AS2 ()에 대해 구성 객체를 정확히 하나 지정해야 합니다 SFTPSftpConfig.

구문 요청

```
{
  "AccessRole": "string",
  "As2Config": {
    "BasicAuthSecretId": "string",
    "Compression": "string",
    "EncryptionAlgorithm": "string",
    "LocalProfileId": "string",
    "MdnResponse": "string",
    "MdnSigningAlgorithm": "string",
    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "LoggingRole": "string",
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Url": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

AccessRole

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출 StartFileTransfer하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2수 있습니다 SendFilePaths. 파일의 상위 디렉터리(예: 의 경우 --send-file-paths /bucket/dir/file.txt상위 디렉터리는 /bucket/dir/)를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 AccessRole은(는) StartFileTransfer 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 StartFileTransfer와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 secretsmanager:GetSecretValue 권한이 필요합니다. Secrets Manager의 AWS 관리형 키 대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 kms:Decrypt 권한도 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 에 대한 secretsmanager:GetSecretValue 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

Pattern: arn:.*role/\S+

필수 여부: 예

As2Config

AS2 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [As2ConnectorConfig](#) 객체

필수 여부: 아니요

LoggingRole

커넥터가 Amazon S3 이벤트에 대한 CloudWatch 로깅을 켤 수 있도록 허용하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. Amazon S3 설정하면 CloudWatch 로그에서 커넥터 활동을 볼 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

SftpConfig

SFTP 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [SftpConnectorConfig](#) 객체

필수 여부: 아니요

Tags

커넥터를 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다. 태그는 어떠한 목적으로 사용자에게 연결되는 메타데이터입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Url

파트너 AS2 또는 SFTP 엔드포인트 URL의 .

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

필수 여부: 예

응답 구문

```
{
  "ConnectorId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[ConnectorId](#)

API 호출이 성공한 후 반환되는 커넥터의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: c-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예제에서는 AS2 커넥터를 생성합니다. 명령에서 다음과 같이 항목을 바꿉니다.

- `url`: 거래 파트너의 AS2 서버에 URL 대한 를 제공합니다.
- `your-IAM-role-for-bucket-access`: 파일을 저장하는 데 사용하는 Amazon S3 버킷에 액세스할 수 있는 IAM 역할입니다.
- AWS 계정 ID가 포함된 로깅 역할에 ARN 를 사용합니다.
- AS2 커넥터 구성 파라미터가 포함된 파일의 경로를 제공합니다. AS2 커넥터 구성 객체는 [As2ConnectorConfig](#)에 설명되어 있습니다.

```
// Listing for testAs2Config.json
{
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "partner-profile-id",
```

```

"MdnResponse": "SYNC",
"Compression": "ZLIB",
"EncryptionAlgorithm": "AES256_CBC",
"SigningAlgorithm": "SHA256",
"MdnSigningAlgorithm": "DEFAULT",
"MessageSubject": "Your Message Subject"
}

```

```

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

```

예

다음 예제에서는 SFTP 커넥터를 생성합니다. 명령에서 다음과 같이 항목을 바꿉니다.

- `sftp-server-url`: 파일을 교환하는 SFTP 서버에 URL 대한 를 제공합니다.
- `your-IAM-role-for-bucket-access`: 파일을 저장하는 데 사용하는 Amazon S3 버킷에 액세스 할 수 있는 IAM 역할입니다.
- AWS 계정 ID가 포함된 로깅 역할에 ARN 를 사용합니다.
- SFTP 커넥터 구성 파라미터가 포함된 파일의 경로를 제공합니다. SFTP 커넥터 구성 객체는 에 설명 되어 있습니다 [SftpConnectorConfig](#).

```

// 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="
  ]
}

```

```

aws transfer create-connector --url "sftp://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
```

예

API 호출은 새 커넥터의 커넥터 ID를 반환합니다.

샘플 응답

```
{  
  "ConnectorId": "a-11112222333344444"  
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateProfile

AS2 전송에 사용할 로컬 또는 파트너 프로파일을 생성합니다.

구문 요청

```
{
  "As2Id": "string",
  "CertificateIds": [ "string" ],
  "ProfileType": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

As2Id

As2Id 는 [RFC4130](#)에 정의된 AS2-name입니다. 인바운드 전송의 경우 파트너에서 보낸 AS2 메시지의 AS2-From 헤더입니다. 아웃바운드 커넥터의 경우 작업을 사용하여 파트너에게 전송되는 AS2 메시지의 AS2-To 헤더입니다. 이 ID는 공백을 포함할 수 없습니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

Pattern: [\p{Print}\s]*

필수 여부: 예

CertificateIds

가져온 인증서의 식별자 배열입니다. 프로파일 및 파트너 프로파일 작업에 이 식별자를 사용합니다.

타입: 문자열 배열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

필수 여부: 아니요

ProfileType

생성할 프로파일 타입을 결정합니다.

- 로컬 프로 파일을 LOCAL 생성하도록 지정합니다. 로컬 프로 파일은 AS2활성화된 Transfer Family 서버 조직 또는 당사자를 나타냅니다.
- 파트너 프로 파일을 생성하도록 PARTNER를 지정하세요. 파트너 프로 파일은 Transfer Family 외부의 원격 조직을 나타냅니다.

타입: 문자열

유효 값: LOCAL | PARTNER

필수 사항 여부: 예

Tags

AS2 프로 파일을 그룹화하고 검색하는 데 사용할 수 있는 키-값 페어입니다.

유형: [Tag](#) 객체 어레이

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

응답 구문

```
{
  "ProfileId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ProfileId

API 호출이 성공한 후 반환되는 AS2 프로필의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 프로필을 생성하고 프로필 ID를 반환합니다.

인증서는 `import-certificate`를 실행할 때 생성IDs되며, 하나는 서명 인증서용이고 다른 하나는 암호화 인증서용입니다.

```
aws transfer create-profile --as2-id MYCORP --certificate-ids c-abcdefgh123456hijk  
c-987654aaaa321bbbb
```

샘플 응답

API 호출은 새 프로파일의 프로파일 ID를 반환합니다.

```
{  
  "ProfileId": "p-11112222333344444"  
}
```

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateServer

AWS에서 선택한 파일 전송 프로토콜을 기반으로 자동 조정 가상 서버를 인스턴스화합니다. 파일 전송 프로토콜 사용 서버를 업데이트하거나 사용자와 작업할 때 새로 생성된 서버에 할당된 서비스 생성 ServerId 속성을 사용합니다.

구문 요청

```
{
  "Certificate": "string",
  "Domain": "string",
  "EndpointDetails": {
    "AddressAllocationIds": [ "string" ],
    "SecurityGroupIds": [ "string" ],
    "SubnetIds": [ "string" ],
    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKey": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "IdentityProviderType": "string",
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
  "StructuredLogDestinations": [ "string" ],
```

```

"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"WorkflowDetails": {
  "OnPartialUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ],
  "OnUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ]
}
}

```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Certificate

(ARN) 인증서의 Amazon 리소스 이름 AWS Certificate Manager (ACM)입니다. Protocols이(가) FTPS(으)로 설정된 경우에 필요합니다.

새 퍼블릭 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [퍼블릭 인증서 요청](#)을 참조하세요.

기존 인증서를 로 가져오려면 AWS Certificate Manager 사용 설명서의 [로 인증서 가져오기](#)ACM를 ACM참조하세요.

프라이빗 IP 주소를 FTPS 통해 사용할 프라이빗 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [프라이빗 인증서 요청](#)을 참조하세요.

다음 암호화 알고리즘 및 키 크기를 사용하는 인증서가 지원됩니다:

- 2048비트RSA(RSA_2048)
- 4096비트RSA(RSA_4096)
- 타원 프라임 곡선 256비트(EC_prime256v1)
- 타원 프라임 곡선 384 비트(EC_secp384r1)
- 타원 프라임 곡선 521비트(EC_secp521r1)

Note

인증서는 지정된 FQDN 또는 IP 주소와 발급자에 대한 정보가 있는 유효한 SSL/TLS X.509 버전 3 인증서여야 합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1600입니다.

필수 여부: 아니요

Domain

파일 전송에 사용되는 스토리지 시스템의 도메인을 지정합니다. Amazon Simple Storage Service(Amazon S3)와 Amazon Elastic File System(Amazon)의 두 가지 도메인을 사용할 수 있습니다. EFS. 기본값은 S3입니다.

Note

서버가 생성된 후에는 도메인을 변경할 수 없습니다.

타입: 문자열

유효 값: S3 | EFS

필수 여부: 아니요

EndpointDetails

서버에 대해 구성된 가상 프라이빗 클라우드(VPC) 엔드포인트 설정입니다. 내에서 엔드포인트를 호스팅할 때 엔드포인트를 내 리소스에만 액세스하도록 하거나 VPC탄력적 IP 주소를 연결하고 인터넷을 통해 클라이언트가 엔드포인트에 액세스할 VPC수 있도록 할 수 있습니다. VPC의 기본 보안 그룹은 엔드포인트에 자동으로 할당됩니다.

유형: [EndpointDetails](#) 객체

필수 여부: 아니요

[EndpointType](#)

서버에서 사용할 엔드포인트 타입입니다. 서버의 엔드포인트에 공개적으로 액세스(PUBLIC)하거나에서 호스팅하도록 선택할 수 있습니다VPC. 에서 호스팅되는 엔드포인트를 사용하면 내에서만 서버 및 리소스에 대한 액세스를 제한VPC하거나 탄력적 IP 주소를 직접 연결하여 인터넷에 연결하도록 선택할 VPC수 있습니다.

Note

2021년 5월 19일 이후에는 계정이 2021년 5월 19일 이전에 아직 생성되지 않은 AWS 계정 경우 EndpointType=VPC_ENDPOINT 에서 를 사용하여 서버를 생성할 수 없습니다. 2021년 5월 19일 AWS 계정 또는 그 이전에 EndpointType=VPC_ENDPOINT 에서 를 사용하여 서버를 이미 생성한 경우 영향을 받지 않습니다. 이 날짜 이후에는 EndpointType=VPC를 사용하세요.

자세한 내용은 [VPC_사용 중단ENDPOINT](#)를 참조하세요.

VPC를 EndpointType(으)로 사용하는 것이 좋습니다. 이 엔드포인트 유형을 사용하면 최대 3개의 탄력적 IPv4 주소(BYOIP 포함)를 서버의 엔드포인트와 직접 연결하고 VPC 보안 그룹을 사용하여 클라이언트의 퍼블릭 IP 주소로 트래픽을 제한할 수 있습니다.

EndpointType를 VPC_ENDPOINT(으)로 설정하면 이 작업을 할 수 없습니다.

타입: 문자열

유효 값: PUBLIC | VPC | VPC_ENDPOINT

필수 여부: 아니요

[HostKey](#)

SFTP사용 가능한 서버에 사용할 RSAECDSA, 또는 ED25519 프라이빗 키입니다. 키를 교체하거나 다른 알고리즘을 사용하는 활성 키 집합이 있는 경우, 여러 호스트 키를 추가할 수 있습니다.

다음 명령을 사용하여 암호 없이 RSA 2048비트 키를 생성합니다.

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

-b 옵션에는 최소값인 2048을 사용합니다. 3072 또는 4096을 사용하여 더 강력한 키를 만들 수 있습니다.

다음 명령을 사용하여 암호 없이 ECDSA 256비트 키를 생성합니다.

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

에 대한 -b 옵션의 유효한 값은 256, 384 및 521ECDSA입니다.

다음 명령을 사용하여 암호가 없는 ED25519 키를 생성합니다.

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

이러한 모든 명령의 경우 를 원하는 문자열my-new-server-key로 바꿀 수 있습니다.

Important

기존 사용자를 기존 SFTP지원 서버에서 새 서버로 마이그레이션할 계획이 없는 경우 호스트 키를 업데이트하지 마세요. 실수로 서버의 호스트 키를 변경하면 작업에 영향을 줄 수 있습니다.

자세한 내용은 AWS Transfer Family 사용 설명서의 [SFTP사용 가능한 서버의 호스트 키 업데이트를 참조하세요](#).

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096입니다.

필수 여부: 아니요

[IdentityProviderDetails](#)

IdentityProviderType이(가) AWS_DIRECTORY_SERVICE, AWS_LAMBDA 또는 API_GATEWAY(으)로 설정된 경우 필수입니다. 에서 디렉터리를 사용하거나 API Gateway 를 API 포함하여 고객 제공 인증을 AWS_DIRECTORY_SERVICE 호출하는 데 필요한 모든 정보가 포함된 배열을 허용합니다URL. IdentityProviderType이 SERVICE_MANAGED로 설정된 경우에 필요합니다.

타입: [IdentityProviderDetails](#) 객체

필수 여부: 아니요

[IdentityProviderType](#)

서버 인증 모드. 기본값은 이며SERVICE_MANAGED, 이를 통해 AWS Transfer Family 서비스 내에서 사용자 자격 증명을 저장하고 액세스할 수 있습니다.

AWS_DIRECTORY_SERVICE 를 사용하여 온프레미스 환경에서 AWS Directory Service for Microsoft Active Directory 또는 Microsoft Active Directory의 Active Directory 그룹에 대한 액세스를 제공하거나 AD Connector를 AWS 사용할 수 있습니다. 또한 이 옵션을 사용하려면 IdentityProviderDetails 파라미터를 사용하여 디렉터리 ID를 제공해야 합니다.

API_GATEWAY 값을 사용하여 선택하는 자격 증명 제공자와 통합합니다. 이 API_GATEWAY 설정을 수행하려면 IdentityProviderDetails 파라미터를 사용하여 인증을 호출URL할 Amazon API Gateway 엔드포인트를 제공해야 합니다.

AWS_LAMBDA 값을 사용하여 AWS Lambda 함수를 자격 증명 공급자로 직접 사용합니다. 이 값을 선택하는 경우 IdentityProviderDetails 데이터 유형의 Function 파라미터에 ARN Lambda 함수에 대해 를 지정해야 합니다.

타입: 문자열

유효 값: SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

필수 여부: 아니요

[LoggingRole](#)

서버가 Amazon S3 또는 Amazon 에 대한 Amazon CloudWatch 로깅을 켤 수 있도록 허용하는 () 역할ARN의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다EFSevents. 설정하면 CloudWatch 로그에서 사용자 활동을 볼 수 있습니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2,048.

패턴: (|arn:.*role/\S+)

필수 여부: 아니요

[PostAuthenticationLoginBanner](#)

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증한 후에 표시됩니다.

Note

SFTP 프로토콜은 인증 후 표시 배너를 지원하지 않습니다.

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: `[\x09-\x0D\x20-\x7E]*`

필수 여부: 아니요

[PreAuthenticationLoginBanner](#)

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증하기 전에 표시됩니다. 예를 들어 다음 배너는 시스템 사용에 대한 세부 정보를 표시합니다.

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

타입: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: `[\x09-\x0D\x20-\x7E]*`

필수 여부: 아니요

[ProtocolDetails](#)

서버에 대해 구성된 프로토콜 설정입니다.

- 패시브 모드(FTP 및 FTPS 프로토콜용)를 표시하려면 `PassiveIp` 파라미터를 사용합니다. 방화벽, 라우터 또는 로드 밸런서의 외부 IP IPv4 주소와 같은 단일 점 쿼드 주소를 입력합니다.
- Amazon S3 버킷에 업로드하는 파일에 대해 클라이언트가 `SETSTAT` 명령을 사용하려 할 때 생성되는 오류를 무시하려면 `SetStatOption` 파라미터를 사용합니다. AWS Transfer Family 서버가 SFTP 클라이언트를 변경할 필요 없이 `SETSTAT` 명령을 무시하고 파일을 업로드하도록 하려면 값을 `ENABLE_NO_OP`로 설정합니다. `SetStatOption` 파라미터를 `ENABLE_NO_OP`로 설정하면 AWS Transfer Family가 Amazon CloudWatch Logs에 로그 항목을 생성하여 클라이언트가 `SETSTAT` 전화를 거는 시기를 확인할 수 있습니다.
- AWS Transfer Family 서버가 고유한 세션 ID를 통해 최근 협상된 세션을 재개하는지 확인하려면 `TlsSessionResumptionMode` 파라미터를 사용합니다.
- `As2Transports`는 AS2 메시지의 전송 방법을 나타냅니다. 현재 HTTP만 지원됩니다.

유형: [ProtocolDetails](#) 객체

필수 여부: 아니요

Protocols

파일 전송 프로토콜 클라이언트가 서버의 엔드포인트에 연결할 수 있는 파일 전송 프로토콜을 지정합니다. 사용 가능한 프로토콜은 다음과 같습니다:

- SFTP (Secure Shell (SSH) 파일 전송 프로토콜): 파일 전송 SSH
- FTPS (파일 전송 프로토콜 보안): TLS 암호화를 사용한 파일 전송
- FTP (File Transfer Protocol): 암호화되지 않은 파일 전송
- AS2 (적용 설명 2): 구조화된 business-to-business 데이터 전송에 사용

Note

- 를 선택하는 경우 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용되는 AWS Certificate Manager (ACM)에 저장된 인증서를 선택해야 FTPS합니다FTPS.
- Protocol에 FTP 또는 FTPS이(가) 포함된 경우 EndpointType은(는) VPC이고 IdentityProviderType은(는) AWS_DIRECTORY_SERVICE, AWS_LAMBDA 또는 API_GATEWAY여야 합니다.
- Protocol에 FTP이(가) 포함된 경우 AddressAllocationIds를 연결할 수 없습니다.
- Protocol이 SFTP로만 설정된 경우 EndpointType을 PUBLIC으로 설정하고 IdentityProviderType을 지원되는 ID 타입(SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA, API_GATEWAY) 중 하나로 설정할 수 있습니다.
- Protocol에 AS2이(가) 포함된 경우 EndpointType은(는) VPC여야 하고, 도메인은 Amazon S3여야 합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 4개입니다.

유효 값: SFTP | FTP | FTPS | AS2

필수 여부: 아니요

S3StorageOptions

Amazon S3 디렉터리의 성능 최적화 여부를 지정합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

기본적으로 홈 디렉터리 매핑의 는 TYPE입니다 DIRECTORY. 이 옵션을 활성화하면 매핑에 파일 대상이 포함되도록 HomeDirectoryMapEntry Type FILE 하려면 를 로 명시적으로 설정해야 합니다.

유형: [S3StorageOptions](#) 객체

필수 여부: 아니요

[SecurityPolicyName](#)

서버에 연결된 보안 정책의 명칭을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

패턴: TransferSecurityPolicy-.*

필수 여부: 아니요

[StructuredLogDestinations](#)

사용자의 서버 로그가 전송될 로그 그룹을 지정합니다.

로그 그룹을 지정하려면 기존 로그 그룹에 ARN 대해 를 제공해야 합니다. 이 경우, 로그 그룹의 형식은 다음과 같습니다:

arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*

예제: arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*

이전에 서버의 로그 그룹을 지정한 경우, update-server 호출 시 이 파라미터에 빈 값을 제공하여 로그 그룹을 지우고 사실상 구조화된 로깅을 끌 수 있습니다. 예:

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

타입: 문자열 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 1개입니다.

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

필수 여부: 아니요

Tags

서버의 그룹화 및 검색에 사용될 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

WorkflowDetails

할당할 워크플로의 워크플로 ID와 워크플로 실행에 사용되는 실행 역할을 지정합니다.

파일이 완전히 업로드될 때 실행되는 워크플로 외에도 WorkflowDetails에는 부분 업로드 시 실행할 워크플로의 워크플로 ID와 실행 역할이 포함될 수 있습니다. 파일이 업로드되는 동안 서버 세션 연결이 끊기면 부분 업로드가 수행됩니다.

타입: [WorkflowDetails](#) 객체

필수 항목 여부: 아니요

응답 구문

```
{
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ServerId

생성되는 서버의 서비스 할당 ID입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 VPC_ENDPOINT를 사용하여 새 표를 만듭니다.

샘플 요청

```
{
  "EndpointType": "VPC",
  "EndpointDetails": ...,
  "HostKey": "Your RSA private key",
  "IdentityProviderDetails": "IdentityProvider",
  "IdentityProviderType": "SERVICE_MANAGED",
  "LoggingRole": "CloudWatchLoggingRole",
  "Tags": [
    {
      "Key": "Name",
      "Value": "MyServer"
    }
  ]
}
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "ServerId": "s-01234567890abcdef"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)

- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateUser

사용자를 생성하고 기존 File Transfer 프로토콜 지원 서버와 연결합니다.

IdentityProviderType이(가) SERVICE_MANAGED(으)로 설정된 서버와만 사용자를 생성하여 연결할 수 있습니다. 에 대한 파라미터를 사용하여 사용자 이름을 지정하고, 홈 디렉터리를 설정하고, 사용자의 퍼블릭 키를 저장하고, 사용자의 AWS Identity and Access Management (IAM) 역할을 할당할 CreateUser수 있습니다. 또한 세션 정책을 선택적으로 추가하고 사용자 그룹화 및 검색에 사용될 수 있는 태그가 포함된 메타데이터를 할당할 수 있습니다.

구문 요청

```
{
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string",
  "SshPublicKeyBody": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "UserName": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

HomeDirectory

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: `/bucket_name/home/mydirectory`

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `(|/.*)`

Required: No

HomeDirectoryMappings

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 는 경로가 Entry 어떻게 표시되는지, Target 는 실제 Amazon S3 또는 Amazon EFS 경로입니다. 대상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할 이 의 경로에 대한 액세스를 제공하는지 확인해야 합니다Target. 이 값은 이 로 설정된 경우에만 HomeDirectoryType 설정할 수 있습니다LOGICAL.

다음은 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

대부분의 경우 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리('chroot')로 제한할 수 있습니다. 이렇게 하려면 Entry를 /(으)로 설정하고 사용자가 로그인할 때 홈 디렉터리에 대해 확인해야 하는 값을 Target(으)로 설정할 수 있습니다.

다음은 chroot에 대한 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

타입: [HomeDirectoryMapEntry](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

[HomeDirectoryType](#)

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH 파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL 제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

[Policy](#)

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 사용자를 위한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

Note

이 정책은 ServerId의 도메인이 Amazon S3인 경우에만 적용됩니다. AmazonEFS은 세션 정책을 사용하지 않습니다.
세션 정책의 경우는 정책의 Amazon 리소스 이름(ARN) 대신 정책을 JSON 블록으로 AWS Transfer Family 저장합니다. 정책을 JSON blob으로 저장하고 Policy 인수에 전달합니다.

세션 정책의 예는 [세션 정책 예](#)를 참조하세요.

자세한 내용은 보안 토큰 서비스 참조 [AssumeRole](#)의 섹션을 참조하세요. AWS API

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

[PosixProfile](#)

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명을 지정합니다. Amazon의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 EFS 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

[Role](#)

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

Pattern: arn:.*role/\S+

필수 여부: 예

[ServerId](#)

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이 항목은 사용자를 추가한 특정 서버입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

SshPublicKeyBody

사용자를 서버에 인증하는 데 사용되는 Secure Shell(SSH) 키의 퍼블릭 부분입니다.

세 가지 표준 SSH 퍼블릭 키 형식 요소는 각 요소 사이에 공백이 <comment>있는 <key type><body base64>, 및 선택적입니다.

AWS Transfer Family 는 RSA, ECDSA 및 ED25519 키를 허용합니다.

- RSA 키의 경우 키 유형은 ssh-rsa.
- ED25519 키의 경우 키 유형은 ssh-ed25519.
- ECDSA 키의 경우 키 유형은 생성한 키의 크기에 따라 ecdsa-sha2-nistp521, ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 또는입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

Tags

사용자의 그룹화 및 검색에 사용될 수 있는 키-값 쌍입니다. 태그는 어떠한 목적으로 사용자에게 연결되는 메타데이터입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

UserName

사용자를 식별하고 ServerId와 연결되는 고유한 문자열입니다. 이 사용자 이름은 3~100자여야 합니다. a-z, A-Z, 0-9, _(밑줄), -(하이픈), .(마침표) 및 @ 기호를 유효한 문자로 사용할 수 있습니다. 사용자 이름은 하이픈, 마침표 및 @ 기호로 시작할 수 없습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: `[\w][\w@.-]{2,99}`

필수 여부: 예

응답 구문

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ServerId

사용자가 연결된 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: `s-([0-9a-f]{17})`

UserName

Transfer Family 사용자를 식별하는 고유한 문자열입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: `[\w][\w@.-]{2,99}`

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

사용자를 생성하려면 먼저 파라미터를 JSON 파일, 예를 들어 예 저장createUserParameters한 다음 create-user API 명령을 실행할 수 있습니다.

```
{
  "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
  "HomeDirectoryType": "PATH",
  "Role": "arn:aws:iam::111122223333:role/bob-role",
  "ServerId": "s-1111aaaa2222bbbb3",
  "SshPublicKeyBody": "ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA...
bobusa@mycomputer.us-east-1.amazon.com",
  "UserName": "bobusa-API"
```

```
}
```

샘플 요청

```
aws transfer create-user --cli-input-json file://createUserParameters
```

샘플 응답

```
{
  "ServerId": "\"s-1111aaaa2222bbbb3\"",
  "UserName": "bobusa-API"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

CreateWorkflow

파일 전송이 완료된 후 워크플로가 호출하는 지정된 단계 및 단계 세부 정보를 사용하여 워크플로를 생성할 수 있습니다. 워크플로를 생성한 후 CreateServer 및 UpdateServer 작업에서 workflow-details 필드를 지정하여 생성된 워크플로를 전송 서버와 연결할 수 있습니다.

구문 요청

```
{
  "Description": "string",
  "OnExceptionSteps": [
    {
      "CopyStepDetails": {
        "DestinationFileLocation": {
          "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
          },
          "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
          }
        },
        "Name": "string",
        "OverwriteExisting": "string",
        "SourceFileLocation": "string"
      },
      "CustomStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Target": "string",
        "TimeoutSeconds": number
      },
      "DecryptStepDetails": {
        "DestinationFileLocation": {
          "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
          },
          "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
          }
        }
      }
    }
  ]
}
```

```

    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string",
    "Type": "string"
  },
  "DeleteStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string"
  },
  "TagStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  "Type": "string"
}
],
"Steps": [
  {
    "CopyStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string"
    },
    "CustomStepDetails": {
      "Name": "string",
      "SourceFileLocation": "string",
      "Target": "string",

```

```

    "TimeoutSeconds": number
  },
  "DecryptStepDetails": {
    "DestinationFileLocation": {
      "EfsFileLocation": {
        "FileSystemId": "string",
        "Path": "string"
      },
      "S3FileLocation": {
        "Bucket": "string",
        "Key": "string"
      }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string",
    "Type": "string"
  },
  "DeleteStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string"
  },
  "TagStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  "Type": "string"
}
],
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
]
}

```


요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Description

워크플로에 대한 텍스트 설명입니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `[\w- ]*`

Required: No

OnExceptionSteps

워크플로를 실행하는 동안 오류가 발생할 경우 수행할 단계(작업)를 지정합니다.

Note

사용자 지정 단계의 경우 Lambda 함수는 예외 단계를 시작하려면 FAILURE 콜백API으로 보내야 합니다. 또한 Lambda가 제한 시간이 초과되기 전에 SUCCESS를 전송하지 않는 경우 예외 단계가 실행됩니다.

타입: [WorkflowStep](#) 객체 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 8개입니다.

필수 여부: 아니요

Steps

지정된 워크플로에 있는 단계에 대한 세부 정보를 지정합니다.

TYPE이(가) 다음 중 이 단계에서 취해야 할 작업을 지정합니다.

- **COPY** - 다른 위치에 파일을 복사합니다.
- **CUSTOM** - AWS Lambda 함수 대상으로 사용자 지정 단계를 수행합니다.
- **DECRYPT** - 업로드되기 전에 암호화된 파일을 복호화합니다.

- **DELETE** - 파일을 삭제합니다.
- **TAG** - 파일에 태그를 추가합니다.

 Note

현재 복사 및 태그 지정은 S3에서만 지원됩니다.

파일 위치의 경우 Amazon S3 버킷 및 키 또는 Amazon EFS 파일 시스템 ID 및 경로를 지정합니다.

유형: [WorkflowStep](#) 객체 어레이

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 8개입니다.

필수 여부: 예

Tags

워크플로 그룹화 및 검색에 사용될 수 있는 키-값 쌍입니다. 태그는 어떠한 목적으로 워크플로에 연결되는 메타데이터입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

응답 구문

```
{
  "WorkflowId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[WorkflowId](#)

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: w-([a-z0-9]{17})

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예와 같이 워크플로 단계 정보를 텍스트 파일에 저장한 다음 해당 파일을 사용하여 워크플로를 생성할 수 있습니다. 다음 예에서는 워크플로 단계를 *example-file.json* (명령을 실행한 동일한 폴더)에 저장했으며 버지니아 북부(us-east-1) 리전에 워크플로를 생성하려고 한다고 가정합니다.

```
aws transfer create-workflow --description "example workflow from a file" --steps
file://example-file.json --region us-east-1
```

```
// Example file containing workflow steps
[
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "testTag"
        }
      ]
    }
  },
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "DOC-EXAMPLE-BUCKET",
          "Key": "DOC-EXAMPLE-KEY/"
        }
      },
      "OverwriteExisting": "TRUE",
      "SourceFileLocation": "${original.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails":{
```

```
    "Name": "DeleteStep",  
    "SourceFileLocation": "${original.file}"  
  }  
}  
]
```

예

이 `CreateWorkflow` 호출은 새 워크플로의 워크플로 ID를 반환합니다.

샘플 응답

```
{  
  "WorkflowId": "w-1234abcd5678efghi"  
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteAccess

ServerID 및 ExternalID 파라미터에 지정된 액세스를 삭제할 수 있습니다.

구문 요청

```
{  
  "ExternalId": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ExternalId

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName, ObjectSid
```

이 명령에서 YourGroupName 를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =, @, /- 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 예

ServerId

이 사용자가 할당한 서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteAgreement

제공된 AgreementId에 지정된 계약을 삭제합니다.

구문 요청

```
{  
  "AgreementId": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

AgreementId

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: a-([0-9a-f]{17})

필수 여부: 예

ServerId

삭제하려는 계약과 관련된 서버 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteCertificate

CertificateId파라미터에서 지정된 인증서를 삭제합니다.

구문 요청

```
{  
  "CertificateId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

CertificateId

삭제하려는 인증서 개체의 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

Pattern: cert-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteConnector

제공된 ConnectorId에 지정된 커넥터를 삭제합니다.

구문 요청

```
{  
  "ConnectorId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: c-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteHostKey

HostKeyId 파라미터에 지정된 호스트 키를 삭제합니다.

구문 요청

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

HostKeyId

삭제 중인 호스트 키의 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

Pattern: hostkey-[0-9a-f]{17}

필수 여부: 예

ServerId

삭제 중인 호스트 키를 포함한 서버의 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteProfile

ProfileId 파라미터에 지정된 프로필을 삭제합니다.

구문 요청

```
{  
  "ProfileId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ProfileId

삭제하려는 프로필의 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: p-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteServer

지정한 파일 전송 프로토콜 지원 서버를 삭제합니다.

이 작업에서 응답이 반환되지 않습니다.

구문 요청

```
{  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 서버를 삭제합니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef"
}
```

예

성공하면 아무 것도 반환되지 않습니다.

샘플 응답

```
{
```

```
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteSshPublicKey

사용자의 Secure Shell(SSH) 퍼블릭 키를 삭제합니다.

구문 요청

```
{
  "ServerId": "string",
  "SshPublicKeyId": "string",
  "UserName": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

사용자가 할당된 File Transfer 프로토콜 지원 서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

SshPublicKeyId

사용자의 특정 SSH 키를 참조하는 데 사용되는 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 21입니다.

Pattern: key-[0-9a-f]{17}

필수 여부: 예

UserName

퍼블릭 키를 삭제할 사용자를 식별하는 고유한 문자열입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: `[\w][\w@.-]{2,99}`

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예제에서는 사용자의 SSH 퍼블릭 키를 삭제합니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef",
  "SshPublicKeyId": "MyPublicKey",
  "UserName": "my_user"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteUser

지정한 파일 전송 프로토콜 지원 서버에 속한 사용자를 삭제합니다.

이 작업에서 응답이 반환되지 않습니다.

Note

서버에서 사용자를 삭제하면 사용자 정보가 손실됩니다.

구문 요청

```
{  
  "ServerId": "string",  
  "UserName": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

사용자가 할당된 서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

UserName

서버에서 삭제되는 사용자를 식별하는 고유한 문자열입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: `[\w][\w@.-]{2,99}`

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 Transfer Family 사용자를 삭제합니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef",
  "UserNames": "my_user"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DeleteWorkflow

지정된 워크플로를 삭제합니다.

구문 요청

```
{  
  "WorkflowId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: w-([a-z0-9]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeAccess

특정 File Transfer 프로토콜 지원 서버에 할당된 액세스 권한을 해당 ServerId 속성과 해당 ExternalId 속성으로 식별하여 설명합니다.

이 직접 호출의 응답은 지정된 ServerId 값과 연결된 액세스 속성을 반환합니다.

구문 요청

```
{
  "ExternalId": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ExternalId

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자는 를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName, ObjectSid
```

이 명령에서 YourGroupName를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =, @, /- 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 예

ServerId

이 액세스 권한이 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "Access": {
    "ExternalId": "string",
    "HomeDirectory": "string",
    "HomeDirectoryMappings": [
      {
        "Entry": "string",
        "Target": "string",
        "Type": "string"
      }
    ],
    "HomeDirectoryType": "string",
    "Policy": "string",
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Role": "string"
  },
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Access

액세스 권한이 연결된 서버의 외부 식별자.

타입: [DescribedAccess](#) 객체

ServerId

이 액세스 권한이 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeAgreement

AgreementId로 식별되는 계약을 설명합니다.

구문 요청

```
{  
  "AgreementId": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

AgreementId

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: a-([0-9a-f]{17})

필수 여부: 예

ServerId

계약과 연결된 서버 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
```

```

"Agreement": {
  "AccessRole": "string",
  "AgreementId": "string",
  "Arn": "string",
  "BaseDirectory": "string",
  "Description": "string",
  "LocalProfileId": "string",
  "PartnerProfileId": "string",
  "ServerId": "string",
  "Status": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Agreement

지정된 계약의 세부 정보로, DescribedAgreement 객체로 반환됩니다.

타입: [DescribedAgreement](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeCertificate

CertificateId로 식별되는 인증서를 설명합니다.

구문 요청

```
{  
  "CertificateId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

CertificateId

가져온 인증서의 식별자 배열입니다. 프로필 및 파트너 프로필 작업에 이 식별자를 사용합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

Pattern: cert-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{  
  "Certificate": {  
    "ActiveDate": number,  
    "Arn": "string",  
    "Certificate": "string",  
    "CertificateChain": "string",  
    "CertificateId": "string",  
    "Description": "string",  
    "InactiveDate": number,  
    "NotAfterDate": number,  
    "NotBeforeDate": number,  
  }
```

```
  "Serial": "string",
  "Status": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Type": "string",
  "Usage": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Certificate](#)

지정된 인증서의 세부 정보로, 객체로 반환됩니다.

타입: [DescribedCertificate](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeConnector

ConnectorId.로 식별되는 커넥터를 설명합니다.

구문 요청

```
{  
  "ConnectorId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: c-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{  
  "Connector": {  
    "AccessRole": "string",  
    "Arn": "string",  
    "As2Config": {  
      "BasicAuthSecretId": "string",  
      "Compression": "string",  
      "EncryptionAlgorithm": "string",  
      "LocalProfileId": "string",  
      "MdnResponse": "string",  
      "MdnSigningAlgorithm": "string",
```

```

    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "ConnectorId": "string",
  "LoggingRole": "string",
  "ServiceManagedEgressIpAddresses": [ "string" ],
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Url": "string"
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Connector](#)

커넥터의 세부 정보를 포함하는 구조입니다.

타입: [DescribedConnector](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeExecution

DescribeExecution를 사용하여 지정된 워크플로의 실행 세부 정보를 확인할 수 있습니다.

Note

이 API 호출은 진행 중인 워크플로에 대한 세부 정보만 반환합니다.
진행 중이 아닌 실행의 ID를 제공하거나 실행이 지정된 워크플로 ID와 일치하지 않는 경우 ResourceNotFound 예외가 발생합니다.

구문 요청

```
{  
  "ExecutionId": "string",  
  "WorkflowId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ExecutionId

워크플로 실행의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 36입니다.

Pattern: [0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}

필수 여부: 예

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: w-([a-z0-9]{17})

필수 여부: 예

응답 구문

```
{
  "Execution": {
    "ExecutionId": "string",
    "ExecutionRole": "string",
    "InitialFileLocation": {
      "EfsFileLocation": {
        "FileSystemId": "string",
        "Path": "string"
      },
      "S3FileLocation": {
        "Bucket": "string",
        "Etag": "string",
        "Key": "string",
        "VersionId": "string"
      }
    },
    "LoggingConfiguration": {
      "LoggingRole": "string",
      "LogGroupName": "string"
    },
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Results": {
      "OnExceptionSteps": [
        {
          "Error": {
            "Message": "string",
            "Type": "string"
          },
          "Outputs": "string",
          "StepType": "string"
        }
      ]
    }
  }
}
```

```

    ],
    "Steps": [
      {
        "Error": {
          "Message": "string",
          "Type": "string"
        },
        "Outputs": "string",
        "StepType": "string"
      }
    ],
  },
  "ServiceMetadata": {
    "UserDetails": {
      "ServerId": "string",
      "SessionId": "string",
      "UserName": "string"
    }
  },
  "Status": "string"
},
"WorkflowId": "string"
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Execution

워크플로 예외의 세부 정보를 포함하는 구조입니다.

타입: [DescribedExecution](#) 객체

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: w-([a-z0-9]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeHostKey

HostKeyId 및 ServerId에 의해 지정된 호스트 키의 세부 정보를 반환합니다.

구문 요청

```
{  
  "HostKeyId": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

HostKeyId

설명하려는 호스트 키의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

Pattern: hostkey-[0-9a-f]{17}

필수 여부: 예

ServerId

설명하려는 호스트 키가 들어 있는 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
```

```
"HostKey": {
  "Arn": "string",
  "DateImported": number,
  "Description": "string",
  "HostKeyFingerprint": "string",
  "HostKeyId": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Type": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[HostKey](#)

지정된 호스트 키의 세부 정보를 반환합니다.

타입: [DescribedHostKey](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeProfile

ProfileId에 의해 지정된 프로필의 세부 정보를 반환합니다.

구문 요청

```
{
  "ProfileId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ProfileId

설명하려는 프로필의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: p-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "Profile": {
    "Arn": "string",
    "As2Id": "string",
    "CertificateIds": [ "string" ],
    "ProfileId": "string",
    "ProfileType": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  }
}
```

```

    }
  ]
}
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Profile](#)

지정된 프로파일의 세부 정보로, 객체로 반환됩니다.

타입: [DescribedProfile](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeSecurityPolicy

File Transfer 프로토콜 지원 서버에 연결된 보안 정책을 나열합니다. 응답에는 보안 정책 속성에 대한 설명이 포함됩니다. 보안 정책에 대한 자세한 내용은 [보안 정책을 사용하는 작업](#)을 참조하세요.

구문 요청

```
{
  "SecurityPolicyName": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[SecurityPolicyName](#)

서버에 연결된 보안 정책의 명칭을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

Pattern: TransferSecurityPolicy-.+

필수 여부: 예

응답 구문

```
{
  "SecurityPolicy": {
    "Fips": boolean,
    "SecurityPolicyName": "string",
    "SshCiphers": [ "string" ],
    "SshKexs": [ "string" ],
    "SshMacs": [ "string" ],
    "TlsCiphers": [ "string" ]
  }
}
```


Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[SecurityPolicy](#)

보안 정책의 속성을 포함하는 배열.

타입: [DescribedSecurityPolicy](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예 명령은 보안 정책 이름을 인수로 사용하고 지정된 보안 정책에 대한 알고리즘을 반환합니다.

샘플 요청

```
aws transfer describe-security-policy --security-policy-name "TransferSecurityPolicy-FIPS-2023-05"
```

샘플 응답

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

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeServer

ServerId 파라미터를 전달하여 지정하는 파일 전송 프로토콜 지원 서버를 설명합니다.

응답에는 서버 속성에 대한 설명이 포함됩니다. 를 EndpointType로 설정하면 응답VPC에 이 포함됩니다EndpointDetails.

구문 요청

```
{
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "Server": {
    "Arn": "string",
    "As2ServiceManagedEgressIpAddresses": [ "string" ],
    "Certificate": "string",
    "Domain": "string",
    "EndpointDetails": {
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],

```

```

    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKeyFingerprint": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "IdentityProviderType": "string",
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
  "ServerId": "string",
  "State": "string",
  "StructuredLogDestinations": [ "string" ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "UserCount": number,
  "WorkflowDetails": {
    "OnPartialUpload": [
      {
        "ExecutionRole": "string",
        "WorkflowId": "string"
      }
    ]
  },
],

```

```

    "OnUpload": [
      {
        "ExecutionRole": "string",
        "WorkflowId": "string"
      }
    ]
  }
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Server

지정한 ServerID(이)가 있는 서버의 속성을 포함하는 배열입니다.

타입: [DescribedServer](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음은 서버에 할당된 속성을 반환하는 예입니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef"
}
```

예

이 예제에서는 의 한 가지 사용량을 보여줍니다 DescribeServer.

샘플 응답

```
{
  "Server": {
    "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
    "EndpointDetails": {
      "AddressAllocationIds": [
        "eipalloc-01a2eabe3c04d5678",
        "eipalloc-102345be"
      ],
      "SubnetIds": [
        "subnet-047eaa7f0187a7cde",
        "subnet-0a2d0f474daffde18"
      ],
      "VpcEndpointId": "vpce-03fe0080e7cb008b8",
      "VpcId": "vpc-09047a51f1c8e1634"
    },
    "EndpointType": "VPC",
  }
}
```

```
    "HostKeyFingerprint": "your host key",
    "IdentityProviderType": "SERVICE_MANAGED",
    "ServerId": "s-01234567890abcdef",
    "State": "ONLINE",
    "Tags": [],
    "UserCount": 0
  }
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeUser

ServerId 속성으로 식별되는 특정 File Transfer 프로토콜 지원 서버에 할당된 사용자를 설명합니다.

이 직접적인 호출의 응답은 지정된 ServerId 값과 관련된 사용자의 속성을 반환합니다.

구문 요청

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

이 사용자가 할당한 서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

UserName

하나 이상의 서버에 할당된 사용자 이름. 사용자 이름은 AWS Transfer Family 서비스를 사용하고 파일 전송 작업을 수행하기 위한 로그인 보안 인증의 일부입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\w][\w@.-]{2,99}

필수 여부: 예

응답 구문

```
{
  "ServerId": "string",
  "User": {
    "Arn": "string",
    "HomeDirectory": "string",
    "HomeDirectoryMappings": [
      {
        "Entry": "string",
        "Target": "string",
        "Type": "string"
      }
    ],
    "HomeDirectoryType": "string",
    "Policy": "string",
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Role": "string",
    "SshPublicKeys": [
      {
        "DateImported": number,
        "SshPublicKeyBody": "string",
        "SshPublicKeyId": "string"
      }
    ],
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "UserName": "string"
  }
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ServerId

이 사용자가 할당한 서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

User

지정한 ServerID 값에 대한 Transfer Family 사용자의 속성이 들어 있는 배열입니다.

타입: [DescribedUser](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 기존 사용자의 세부 정보를 보여줍니다.

샘플 요청

```
aws transfer describe-user --server-id s-1111aaaa2222bbbb3 --user-name bob-test
```

샘플 응답

```
{
  "ServerId": "s-1111aaaa2222bbbb3",
  "User": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:user/s-1111aaaa2222bbbb3/bob-test",
    "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
    "HomeDirectoryType": "PATH",
    "Role": "arn:aws:iam::111122223333:role/bob-role",
    "SshPublicKeys": [
      {
        "DateImported": "2022-03-31T12:27:52.614000-04:00",
        "SshPublicKeyBody": "ssh-rsa AAAAB3NzaC1yc..... bobusa@mycomputer.us-east-1.amazonaws.com",
        "SshPublicKeyId": "key-abcde12345fghik67"
      }
    ],
    "Tags": [],
    "UserName": "bob-test"
  }
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)

- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

DescribeWorkflow

지정된 워크플로를 설명합니다.

구문 요청

```
{
  "WorkflowId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: w-([a-z0-9]{17})

필수 여부: 예

응답 구문

```
{
  "Workflow": {
    "Arn": "string",
    "Description": "string",
    "OnExceptionSteps": [
      {
        "CopyStepDetails": {
          "DestinationFileLocation": {
            "EfsFileLocation": {
              "FileSystemId": "string",
              "Path": "string"
            },
            "S3FileLocation": {
```

```

        "Bucket": "string",
        "Key": "string"
      }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string"
  },
  "CustomStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Target": "string",
    "TimeoutSeconds": number
  },
  "DecryptStepDetails": {
    "DestinationFileLocation": {
      "EfsFileLocation": {
        "FileSystemId": "string",
        "Path": "string"
      },
      "S3FileLocation": {
        "Bucket": "string",
        "Key": "string"
      }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string",
    "Type": "string"
  },
  "DeleteStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string"
  },
  "TagStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  }
},

```

```

    "Type": "string"
  }
],
"Steps": [
  {
    "CopyStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string"
    },
    "CustomStepDetails": {
      "Name": "string",
      "SourceFileLocation": "string",
      "Target": "string",
      "TimeoutSeconds": number
    },
    "DecryptStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string",
      "Type": "string"
    },
    "DeleteStepDetails": {
      "Name": "string",

```



```

        "SourceFileLocation": "string"
    },
    "TagStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Tags": [
            {
                "Key": "string",
                "Value": "string"
            }
        ]
    },
    "Type": "string"
}
],
"Tags": [
    {
        "Key": "string",
        "Value": "string"
    }
],
"WorkflowId": "string"
}
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Workflow](#)

워크플로의 세부 정보를 포함하는 구조입니다.

타입: [DescribedWorkflow](#) 객체

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ImportCertificate

로컬 (AS2) 프로파일 및 파트너 프로파일을 생성하는 데 필요한 서명 및 암호화 인증서를 가져옵니다.

구문 요청

```
{
  "ActiveDate": number,
  "Certificate": "string",
  "CertificateChain": "string",
  "Description": "string",
  "InactiveDate": number,
  "PrivateKey": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Usage": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ActiveDate

인증서가 활성화되는 시기를 지정하는 선택적 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Certificate

- 예 URI 형식의 인증서에 대한 파일 경로를 CLI제공합니다. 예: --certificate file:// encryption-cert.pem. 또는 원시 콘텐츠를 제공할 수 있습니다.
- 예 인증서 파일의 원시 콘텐츠를 SDK지정합니다. 예: --certificate "`cat encryption-cert.pem`".

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 16384입니다.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

필수 여부: 예

[CertificateChain](#)

가져오는 인증서의 체인을 구성하는 선택적 인증서 목록.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 2097152입니다.

패턴: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

[Description](#)

인증서를 식별하는 데 도움이 되는 간단한 설명.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: `[\p{Graph}]+`

필수 여부: 아니요

[InactiveDate](#)

인증서가 비활성화되는 시기를 지정하는 선택적 날짜.

타입: Timestamp

필수 여부: 아니요

[PrivateKey](#)

- 의 경우 프라이빗 키의 파일 경로를 URI 형식으로 CLI제공합니다.예: `--private-key file://encryption-key.pem`. 또는 프라이빗 키 파일의 원시 콘텐츠를 제공할 수도 있습니다.
- 예 프라이빗 키 파일의 원시 콘텐츠를 SDK지정합니다. 예제: `--private-key "`cat encryption-key.pem`"`

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 16384입니다.

패턴: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

Tags

인증서를 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Usage

이 인증서가 서명 또는 암호화에 사용되는지를 지정합니다.

타입: 문자열

유효 값: SIGNING | ENCRYPTION

필수 여부: 예

응답 구문

```
{  
  "CertificateId": "string"  
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

CertificateId

가져온 인증서의 식별자 배열입니다. 프로필 및 파트너 프로필 작업에 이 식별자를 사용합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 암호화에 사용할 인증서를 가져옵니다. 첫 번째 명령에서는 인증서 및 인증서 체인 파일의 내용을 제공합니다. SDK 명령에 이 형식을 사용합니다.

```
aws transfer import-certificate --usage ENCRYPTION --certificate "`cat encryption-  
cert.pem`" \
```

```
--private-key "`cat encryption-key.pem`" --certificate-chain "`cat root-ca.pem`"
```

예

다음 예는 프라이빗 키, 인증서 및 인증서 체인 파일의 파일 위치를 제공한다는 점을 제외하면 이전 명령과 동일합니다. 를 사용하는 경우 이 버전의 명령은 작동하지 않습니다 SDK.

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

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ImportHostKey

ServerId 파라미터로 지정된 서버에 호스트 키를 추가합니다.

구문 요청

```
{
  "Description": "string",
  "HostKeyBody": "string",
  "ServerId": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Description

이 호스트 키를 식별하는 텍스트 설명.

타입: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: [\p{Print}]*

Required: No

HostKeyBody

키 페어의 프라이빗 SSH 키 부분입니다.

AWS Transfer Family 는 RSA, ECDSA 및 ED25519 키를 허용합니다.

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096입니다.

필수 여부: 예

ServerId

가져오려는 호스트 키가 들어 있는 서버의 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Tags

그룹화 및 호스트 키 검색에 사용될 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

응답 구문

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

HostKeyId

가져온 키의 호스트 키 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

패턴: hostkey-[0-9a-f]{17}

ServerId

가져온 키가 포함된 서버 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ImportSshPublicKey

특정 파일 전송 프로토콜 지원 서버에 할당된 UserName 값으로 식별되고 로 식별되는 Transfer Family 사용자에게 Secure Shell(SSH) 퍼블릭 키를 추가합니다 ServerId.

응답은 UserName 값, ServerId 값 및 SshPublicKeyId의 명칭을 반환합니다.

구문 요청

```
{
  "ServerId": "string",
  "SshPublicKeyBody": "string",
  "UserName": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

SshPublicKeyBody

키 페어의 퍼블릭 SSH 키 부분입니다.

AWS Transfer Family 는 RSA, ECDSA 및 ED25519 키를 허용합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 예

UserName

하나 이상의 서버에 할당된 Transfer Family 사용자의 명칭.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: `[\w][\w@.-]{2,99}`

필수 여부: 예

응답 구문

```
{
  "ServerId": "string",
  "SshPublicKeyId": "string",
  "UserName": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ServerId

서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: `s-([0-9a-f]{17})`

SshPublicKeyId

가져온 시스템에서 퍼블릭 키에 부여한 명칭.

타입: 문자열

길이 제약 조건: 고정 길이는 21입니다.

패턴: key-[0-9a-f]{17}

UserName

지정한 ServerID 값에 할당된 사용자 이름입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\w][\w@.-]{2,99}

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

이 명령은 id_ecdsa.pub 파일에 저장된 ECDSA 키를 가져옵니다.

```
aws transfer import-ssh-public-key --server-id s-021345abcdef6789 --ssh-public-key-body
file://id_ecdsa.pub --user-name jane-doe
```

예

명령이 제대로 실행되지 않으면, 시스템에서 다음과 비슷한 정보를 반환합니다.

```
{
  "ServerId": "s-021345abcdef6789",
  "SshPublicKeyId": "key-1234567890abcdef0",
  "UserName": "jane-doe"
}
```

참고

언어별 종 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)

- [AWS SDK Ruby V3용](#)

ListAccesses

서버에 있는 모든 액세스 권한의 세부 정보를 나열합니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환할 최대 액세스 수IDs를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListAccesses 호출에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 NextToken 파라미터에 후속 명령을 전달하여 추가 액세스를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

ServerId

사용자가 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "Accesses": [
    {
      "ExternalId": "string",
      "HomeDirectory": "string",
      "HomeDirectoryType": "string",
      "Role": "string"
    }
  ],
  "NextToken": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Accesses](#)

지정한 ServerId 값에 대한 액세스 및 해당 속성을 반환합니다.

타입: [ListedAccess](#) 객체 배열

[NextToken](#)

ListAccesses 호출에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 NextToken 파라미터에 후속 명령을 전달하여 추가 액세스를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

ServerId

사용자가 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListAgreements

ServerId이(가) 제공한 계약으로 식별되는 서버의 계약 목록을 반환합니다. 결과를 특정 수로 제한하려면 MaxResults 파라미터 값을 제공하세요. 이전에 명령을 실행하여 NextToken에 대한 값을 받은 경우 해당 값을 제공하여 중단한 부분부터 계약을 계속 나열할 수 있습니다.

구문 요청

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환할 최대 계약 수입니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListAgreements 호출에서 추가 결과를 얻을 수 있는 경우, 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 NextToken 파라미터에 후속 명령을 전달하여 추가 계약을 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

ServerId

계약 목록을 작성하려는 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "Agreements": [
    {
      "AgreementId": "string",
      "Arn": "string",
      "Description": "string",
      "LocalProfileId": "string",
      "PartnerProfileId": "string",
      "ServerId": "string",
      "Status": "string"
    }
  ],
  "NextToken": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Agreements

각 항목에 계약 세부 정보가 포함된 배열을 반환합니다.

타입: [ListedAgreement](#) 객체 배열

NextToken

ListAgreements를 다시 호출하여 추가 결과(있는 경우)를 수신하는 데 사용할 수 있는 토큰을 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)

- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListCertificates

로 가져온 현재 인증서 목록을 반환합니다 AWS Transfer Family. 결과를 특정 수로 제한하려면 `MaxResults` 파라미터 값을 제공하세요. 이전에 명령을 실행하여 `NextToken` 파라미터 값을 받은 경우 해당 값을 제공하여 중단한 부분부터 인증서를 계속 나열할 수 있습니다.

구문 요청

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[MaxResults](#)

반환될 최대 인증서 수입니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

[NextToken](#)

`ListCertificates` 호출에서 추가 결과를 얻을 수 있는 경우 출력에 `NextToken` 파라미터가 반환됩니다. 그런 다음 `NextToken` 파라미터에 후속 명령을 전달하여 추가 인증서를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{
  "Certificates": [
    {
      "ActiveDate": number,
      "Arn": "string",
      "CertificateId": "string",
      "Description": "string",
      "InactiveDate": number,
      "Status": "string",
      "Type": "string",
      "Usage": "string"
    }
  ],
  "NextToken": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Certificates

ListCertificates 호출에 지정된 인증서 배열을 반환합니다.

타입: [ListedCertificate](#) 객체 배열

NextToken

다음 인증서를 나열하는 데 사용할 수 있는 다음 토큰을 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)

- [AWS SDK Ruby V3용](#)

ListConnectors

지정된 지역의 커넥터를 나열합니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환될 최대 커넥터 수입니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListConnectors 호출에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 NextToken 파라미터에 후속 명령을 전달하여 추가 커넥터를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{
```

```
"Connectors": [  
  {  
    "Arn": "string",  
    "ConnectorId": "string",  
    "Url": "string"  
  }  
],  
"NextToken": "string"  
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Connectors](#)

각 항목에 커넥터의 세부 정보가 포함된 배열을 반환합니다.

타입: [ListedConnector](#) 객체 배열

[NextToken](#)

ListConnectors를 다시 호출하여 추가 결과(있는 경우)를 수신하는 데 사용할 수 있는 토큰을 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListExecutions

지정된 워크플로에 대해 진행 중인 모든 실행을 나열합니다.

Note

지정된 워크플로 ID를 찾을 수 없는 경우 ListExecutions은(는) ResourceNotFound 예외를 반환합니다.

구문 요청

```
{
  "MaxResults": number,
  "NextToken": "string",
  "WorkflowId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환할 최대 집행 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListExecutions은(는) 출력에 NextToken 파라미터를 반환합니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 실행을 계속 나열할 수 있습니다.

예를 들어, 이는 페이지 매김에 유용합니다. 워크플로 실행 횟수가 100개인 경우 처음 10개만 나열하는 것이 좋습니다. 그렇다면 `max-results`를 지정하여 결과를 호출합니다.


```
aws transfer list-executions --max-results 10
```

그러면 처음 10개 집행에 대한 세부 정보와 11번째 실행에 대한 포인터(NextToken)가 반환됩니다. 이제 를 API 다시 호출하여 받은 NextToken 값을 제공할 수 있습니다.

```
aws transfer list-executions --max-results 10 --next-token
$somePointerReturnedFromPreviousListResult
```

이 호출은 다음 10번의 집행(11번째부터 20번째)을 반환합니다. 그런 다음 100개 실행에 대한 세부 정보가 모두 반환될 때까지 호출을 반복할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

[WorkflowId](#)

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: w-([a-z0-9]{17})

필수 여부: 예

응답 구문

```
{
  "Executions": [
    {
      "ExecutionId": "string",
      "InitialFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Etag": "string",

```

```

        "Key": "string",
        "VersionId": "string"
    },
    "ServiceMetadata": {
        "UserDetails": {
            "ServerId": "string",
            "SessionId": "string",
            "UserName": "string"
        }
    },
    "Status": "string"
},
"NextToken": "string",
"WorkflowId": "string"
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[Executions](#)

각 실행의 세부 정보를 ListedExecution 배열로 반환합니다.

타입: [ListedExecution](#) 객체 배열

[NextToken](#)

ListExecutions은(는) 출력에 NextToken 파라미터를 반환합니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 실행을 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

[WorkflowId](#)

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: w-([a-z0-9]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListHostKeys

파라미터로 지정된 서버의 호스트 키 목록을 반환합니다. ServerId

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환할 최대 호스트 키 수입니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

반환되지 않은 추가 결과가 있는 경우 NextToken 파라미터가 반환됩니다. 이 값을 ListHostKeys에 대한 후속 호출에 사용하여 결과를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

ServerId

확인할 호스트 키가 포함된 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "HostKeys": [
    {
      "Arn": "string",
      "DateImported": number,
      "Description": "string",
      "Fingerprint": "string",
      "HostKeyId": "string",
      "Type": "string"
    }
  ],
  "NextToken": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[HostKeys](#)

각 항목에 호스트 키의 세부 정보가 포함된 배열을 반환합니다.

타입: [ListedHostKey](#) 객체 배열

[NextToken](#)

ListHostKeys를 다시 호출하여 추가 결과(있는 경우)를 수신하는 데 사용할 수 있는 토큰을 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

ServerId

나열된 호스트 키가 포함된 서버 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListProfiles

시스템의 프로필 목록을 반환합니다. 결과를 특정 수로 제한하려면 MaxResults 파라미터 값을 제공하세요. 이전에 명령을 실행하여 NextToken에 대한 값을 받은 경우, 해당 값을 제공하여 중단한 부분부터 프로필을 계속 나열할 수 있습니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ProfileType": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

반환할 최대 프로필 수입니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

반환되지 않은 추가 결과가 있는 경우 NextToken 파라미터가 반환됩니다. 이 값을 ListProfiles에 대한 후속 호출에 사용하여 결과를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

ProfileType

LOCAL 타입 프로필만 나열할지 아니면 PARTNER 타입 프로필만 나열할지를 나타냅니다. 요청에 입력되지 않은 경우 명령은 모든 타입의 프로필을 나열합니다.

타입: 문자열

유효 값: LOCAL | PARTNER

필수 항목 여부: 아니요

응답 구문

```
{
  "NextToken": "string",
  "Profiles": [
    {
      "Arn": "string",
      "As2Id": "string",
      "ProfileId": "string",
      "ProfileType": "string"
    }
  ]
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[NextToken](#)

다시 ListProfiles를 호출하여 추가 결과(있는 경우)를 수신하는 데 사용할 수 있는 토큰을 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

[Profiles](#)

각 항목에 프로필의 세부 정보가 포함된 배열을 반환합니다.

타입: [ListedProfile](#) 객체 배열

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListSecurityPolicies

파일 전송 프로토콜 지원 서버에 연결된 보안 정책을 나열합니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

ListSecurityPolicies 쿼리에 대한 응답으로 반환할 보안 정책 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListSecurityPolicies 명령에서 추가 결과를 얻으면 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 보안 정책을 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{
```

```
"NextToken": "string",  
"SecurityPolicyNames": [ "string" ]  
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[NextToken](#)

ListSecurityPolicies 작업에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 다음 명령에서 NextToken 파라미터를 전달하여 보안 정책을 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

[SecurityPolicyNames](#)

나열된 보안 정책의 배열.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

Pattern: TransferSecurityPolicy-.+

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에는 사용 가능한 모든 보안 정책의 이름이 전부 나열되어 있습니다.

샘플 요청

```
aws transfer list-security-policies
```

샘플 응답

```
{
  "SecurityPolicyNames": [
    "TransferSecurityPolicy-2022-03",
    "TransferSecurityPolicy-FIPS-2020-06",
    "TransferSecurityPolicy-2018-11",
    "TransferSecurityPolicy-2023-05",
    "TransferSecurityPolicy-FIPS-2023-05",
    "TransferSecurityPolicy-2020-06"
  ]
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)

- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListServers

AWS 계정과 연결된 파일 전송 프로토콜 지원 서버를 나열합니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

ListServers 쿼리에 대한 응답으로 반환할 서버 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListServers 명령에서 추가 결과를 얻으면 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 서버를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{
```

```

"NextToken": "string",
"Servers": [
  {
    "Arn": "string",
    "Domain": "string",
    "EndpointType": "string",
    "IdentityProviderType": "string",
    "LoggingRole": "string",
    "ServerId": "string",
    "State": "string",
    "UserCount": number
  }
]
}

```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

NextToken

ListServers 작업에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 다음 명령에서 NextToken 파라미터를 전달하여 추가 서버를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

Servers

나열된 서버 배열입니다.

타입: [ListedServer](#) 객체 배열

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예제에서는 예에 있는 서버를 나열합니다 AWS 계정.

참고로, 예의 NextToken 값은 실제 값이 아닙니다. 이 값은 파라미터 사용 방법을 나타내기 위한 것입니다.

샘플 요청

```
{
  "MaxResults": 1,
  "NextToken": "token-from-previous-API-call"
}
```

샘플 응답

```
{
  "NextToken": "another-token-to-continue-listing",
  "Servers": [
    {
      "Arn": "arn:aws:transfer:us-east-1:111112222222:server/s-01234567890abcdef",
      "Domain": "S3",

```

```
    "IdentityProviderType": "SERVICE_MANAGED",
    "EndpointType": "PUBLIC",
    "LoggingRole": "arn:aws:iam::111112222222:role/my-role",
    "ServerId": "s-01234567890abcdef",
    "State": "ONLINE",
    "UserCount": 3
  }
]
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListTagsForResource

지정한 Amazon 리소스 이름(ARN)과 연결된 모든 태그를 나열합니다. 리소스는 사용자, 서버 또는 역할입니다.

구문 요청

```
{
  "Arn": "string",
  "MaxResults": number,
  "NextToken": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Arn

특정 Amazon 리소스 이름()과 연결된 태그를 요청합니다ARN. ARN 는 서버, 사용자 또는 역할과 같은 특정 AWS 리소스의 식별자입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

MaxResults

ListTagsForResource 요청에 대한 응답으로 반환할 태그 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListTagsForResource 작업의 추가 결과를 요청하면 입력에 NextToken 파라미터가 반환됩니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 태그를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{
  "Arn": "string",
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Arn

태그를 나열하도록 ARN 지정한입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

[NextToken](#)

ListTagsForResource 호출에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 태그를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

[Tags](#)

일반적으로 항목을 그룹화하고 검색하기 위해 리소스에 할당되는 키-값 쌍입니다. 태그는 사용자가 정의하는 메타데이터입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예제에서는 지정한 리소스를 사용하여 리소스의 태그를 나열ARN합니다.

샘플 요청

```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef"
}
```

예

이 예제에서는 의 한 가지 사용량을 보여줍니다 ListTagsForResource.

샘플 응답

```
{
  "Tags": [
    {
      "Key": "Name",
      "Value": "MyServer"
    }
  ]
}
```

참고

언어별 중 하나API에서 이 리소스를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListUsers

ServerId 파라미터를 전달하여 지정한 파일 전송 프로토콜 지원 서버의 사용자를 나열합니다.

구문 요청

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

MaxResults

ListUsers 요청에 대한 응답으로 반환할 사용자 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

NextToken

ListUsers 호출의 추가 결과가 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 NextToken을 후속 ListUsers 명령에 전달하여 추가 사용자를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

ServerId

사용자가 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "NextToken": "string",
  "ServerId": "string",
  "Users": [
    {
      "Arn": "string",
      "HomeDirectory": "string",
      "HomeDirectoryType": "string",
      "Role": "string",
      "SshPublicKeyCount": number,
      "UserName": "string"
    }
  ]
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

NextToken

ListUsers 호출에서 추가 결과를 얻을 수 있는 경우 출력에 NextToken 파라미터가 반환됩니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 사용자를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

ServerId

사용자가 할당된 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Users

지정한 ServerId 값에 대한 Transfer Family 사용자 및 해당 속성을 반환합니다.

타입: [ListedUser](#) 객체 배열

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

ListUsers API 호출은 지정된 서버와 연결된 사용자 목록을 반환합니다.

샘플 요청

```
{
  "MaxResults": 100,
  "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
  "ServerId": "s-01234567890abcdef"
}
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
  "ServerId": "s-01234567890abcdef",
  "Users": [
    {
      "Arn": "arn:aws:transfer:us-east-1:176354371281:user/s-01234567890abcdef/charlie",
      "HomeDirectory": "/tests/home/charlie",
      "SshPublicKeyCount": 1,
      "Role": "arn:aws:iam::176354371281:role/transfer-role1",
      "Tags": [
        {
          "Key": "Name",
          "Value": "user1"
        }
      ],
      "UserName": "my_user"
    }
  ]
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

ListWorkflows

현재 리전에 AWS 계정 대해 와 연결된 모든 워크플로를 나열합니다.

구문 요청

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[MaxResults](#)

반환할 최대 워크플로 수를 지정합니다.

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1000입니다.

필수 여부: 아니요

[NextToken](#)

ListWorkflows은(는) 출력에 NextToken 파라미터를 반환합니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 워크플로를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

필수 여부: 아니요

응답 구문

```
{  
  "NextToken": "string",  
}
```

```
"Workflows": [  
  {  
    "Arn": "string",  
    "Description": "string",  
    "WorkflowId": "string"  
  }  
]
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[NextToken](#)

ListWorkflows은(는) 출력에 NextToken 파라미터를 반환합니다. 그런 다음 후속 명령에 NextToken 파라미터를 전달하여 추가 워크플로를 계속 나열할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 6144입니다.

[Workflows](#)

각 워크플로에 대해 Arn, WorkflowId 및 Description를 반환합니다.

타입: [ListedWorkflow](#) 객체 배열

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidNextTokenException

전달된 NextToken 파라미터가 유효하지 않습니다.

HTTP 상태 코드: 400

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

SendWorkflowStepState

비동기 사용자 지정 단계에 대한 콜백을 전송할 수 있습니다.

ExecutionIdWorkflowId, 및 Token 는 워크플로의 사용자 지정 단계를 실행하는 동안 대상 리소스에 전달됩니다. 상태를 제공할 뿐만 아니라 콜백에도 이러한 항목을 포함해야 합니다.

구문 요청

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ExecutionId

워크플로 실행의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 36입니다.

Pattern: [0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}

필수 여부: 예

Status

지정된 단계의 성공 또는 실패 여부를 나타냅니다.

타입: 문자열

유효 값: SUCCESS | FAILURE

필수 사항 여부: 예

Token

동일한 실행 내에서 여러 Lambda 단계에 대한 여러 콜백을 구분하는 데 사용됩니다.

타입: 문자열

길이 제한: 최소 길이는 1. 최대 길이는 64.

Pattern: \w+

필수 여부: 예

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: w-([a-z0-9]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

StartFileTransfer

로컬 AWS 스토리지와 원격 AS2 또는 SFTP 서버 간에 파일 전송을 시작합니다.

- AS2 커넥터의 경우 ConnectorId 및 하나 이상을 지정SendFilePaths하여 전송하려는 파일을 식별합니다.
- SFTP 커넥터의 경우 파일 전송은 아웃바운드 또는 인바운드일 수 있습니다. 두 경우 모두 ConnectorId를 지정합니다. 전송 방향에 따라 다음 항목도 지정합니다.
 - 파트너의 서버에서 SFTP Amazon Web Services 스토리지로 파일을 전송하는 경우 전송할 파일을 식별RetreiveFilePaths하도록 하나 이상을 지정하고 대상 폴더를 지정LocalDirectoryPath하도록 를 지정합니다.
 - 스토리지에서 AWS 파트너의 SFTP 서버로 파일을 전송하는 경우 전송할 파일을 식별SendFilePaths하도록 하나 이상을 지정하고 대상 폴더를 지정RemoteDirectoryPath하도록 를 지정합니다.

구문 요청

```
{
  "ConnectorId": "string",
  "LocalDirectoryPath": "string",
  "RemoteDirectoryPath": "string",
  "RetrieveFilePaths": [ "string" ],
  "SendFilePaths": [ "string" ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: c-([0-9a-f]{17})

필수 여부: 예

LocalDirectoryPath

인바운드 전송의 경우 는 파트너의 SFTP 서버에서 전송되는 하나 이상의 파일의 대상을 LocalDirectoryPath 지정합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 1024입니다.

패턴: (.)+

Required: No

RemoteDirectoryPath

아웃바운드 전송의 경우 는 파트너의 SFTP 서버로 전송되는 하나 이상의 파일의 대상을 RemoteDirectoryPath 지정합니다. 를 지정하지 않으면 전송RemoteDirectoryPath된 파일의 대상은 SFTP 사용자의 홈 디렉터리입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 1024입니다.

패턴: (.)+

Required: No

RetrieveFilePaths

파트너 SFTP 서버의 소스 경로가 하나 이상 있습니다. 각 문자열은 한 번의 인바운드 File Transfer 에 대한 소스 파일 경로를 나타냅니다.

타입: 문자열 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 10개입니다.

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 1024입니다.

패턴: (.)+

Required: No

SendFilePaths

Amazon S3 스토리지를 위한 하나 이상의 소스 경로. 각 문자열은 한 번의 아웃바운드 파일 전송에 대한 소스 파일 경로를 나타냅니다. 예: `DOC-EXAMPLE-BUCKET/myfile.txt` .

Note

`DOC-EXAMPLE-BUCKET` 를 실제 버킷 중 하나와 바꾸세요.

타입: 문자열 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 10개입니다.

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 1024입니다.

패턴: `(.)+`

필수 여부: 아니요

응답 구문

```
{
  "TransferId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

TransferId

파일 전송에 대해 고유 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 512입니다.

패턴: `[0-9a-zA-Z./-]+`

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예제에서는 Transfer Family 서버에서 원격 거래 파트너의 엔드포인트로 AS2 파일 전송을 시작합니다. `DOC-EXAMPLE-BUCKET` 를 실제 버킷 중 하나로 바꾸세요.

샘플 요청

```
{
  "ConnectorId": "c-AAAA1111BBBB2222C",
```



```
"SendFilePaths": [  
    "/DOC-EXAMPLE-BUCKET/myfile-1.txt",  
    "/DOC-EXAMPLE-BUCKET/myfile-2.txt",  
    "/DOC-EXAMPLE-BUCKET/myfile-3.txt"  
]  
}
```

샘플 응답

```
{  
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"  
}
```

예

다음 예제에서는 로컬 AWS 스토리지에서 원격 SFTP 서버로 파일 전송을 시작합니다.

샘플 요청

```
{  
  "ConnectorId": "c-01234567890abcdef",  
  "SendFilePaths": [  
    "/DOC-EXAMPLE-BUCKET/myfile-1.txt",  
    "/DOC-EXAMPLE-BUCKET/myfile-2.txt",  
    "/DOC-EXAMPLE-BUCKET/myfile-3.txt"  
  ],  
  "RemoteDirectoryPath": "/MySFTPRootFolder/fromTransferFamilyServer"  
}
```

샘플 응답

```
{  
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"  
}
```

예

다음 예제에서는 원격 SFTP 서버에서 로컬 AWS 스토리지로 파일 전송을 시작합니다.

샘플 요청

```
{
```

```
"ConnectorId": "c-111122223333AAAAA",
"RetrieveFilePaths": [
  "/MySFTPFolder/toTransferFamily/myfile-1.txt",
  "/MySFTPFolder/toTransferFamily/myfile-2.txt",
  "/MySFTPFolder/toTransferFamily/myfile-3.txt"
],
"LocalDirectoryPath": "/DOC-EXAMPLE-BUCKET/mySourceFiles"
}
```

샘플 응답

```
{
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

StartServer

File Transfer 프로토콜이 활성화된 서버의 상태를 OFFLINE에서 ONLINE로 변경합니다. 이미 ONLINE 설치된 서버에는 영향을 주지 않습니다. ONLINE서버는 File Transfer 작업을 수락하고 처리할 수 있습니다.

STARTING 상태는 서버가 완전히 응답할 수 없거나 완전히 온라인 상태가 아닌 중간 상태임을 나타냅니다. START_FAILED의 값은 오류 상태를 나타낼 수 있습니다.

이 직접 호출에서 응답이 반환되지 않습니다.

구문 요청

```
{
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

시작하려는 서버에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 서버를 시작합니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef"
}
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "ServerId": "s-01234567890abcdef"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

StopServer

File Transfer 프로토콜이 활성화된 서버의 상태를 OFFLINE에서 ONLINE로 변경합니다. OFFLINE 서버는 File Transfer 작업을 수락하고 처리할 수 없습니다. 서버 및 사용자 속성과 같이 서버에 연결된 정보는 서버를 중지해도 영향을 받지 않습니다.

Note

서버를 중지해도 File Transfer 프로토콜 엔드포인트 청구가 줄어들거나 영향을 미치지 않습니다. 요금 청구를 중지하려면 서버를 삭제해야 합니다.

STOPPING 상태는 서버가 완전히 응답할 수 없거나 완전히 오프라인 상태가 아닌 중간 상태임을 나타냅니다. STOP_FAILED의 값은 오류 상태를 나타낼 수 있습니다.

이 직접 호출에서 응답이 반환되지 않습니다.

구문 요청

```
{  
  "ServerId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ServerId

중지한 서버에 대해 시스템에서 할당한 고유 식별자.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 서버를 중지합니다.

샘플 요청

```
{
  "ServerId": "s-01234567890abcdef"
}
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "ServerId": "s-01234567890abcdef"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

TagResource

Amazon 리소스 이름()으로 식별되는 리소스에 키-값 페어를 연결합니다ARN. 리소스는 사용자, 서버, 역할 및 기타 개체입니다.

이 직접적인 호출에서 응답이 반환되지 않았습니다.

구문 요청

```
{
  "Arn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Arn

서버, 사용자 또는 역할과 같은 특정 리소스의 Amazon AWS 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

Tags

유형별로 리소스를 그룹화하고 검색하는 데 사용할 수 ARNs 있는 에 할당된 키-값 페어입니다. 어떤 목적으로든 이 메타데이터를 리소스(서버, 사용자, 워크폴로 등)에 연결할 수 있습니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 File Transfer 프로토콜이 활성화된 서버에 태그를 추가합니다.

샘플 요청

```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
  "Tags": [
    {
      "Key": "Group",
      "Value": "Europe"
    }
  ]
}
```

예

이 예제에서는 의 한 가지 사용량을 보여줍니다 TagResource.

샘플 응답

HTTP 200 response with an empty HTTP body.

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

TestConnection

SFTP 커넥터가 성공적으로 설정되었는지 테스트합니다. 로컬 AWS 스토리지와 거래 파트너의 SFTP 서버 간에 파일을 전송하는 기능을 테스트하려면 이 작업을 호출하는 것이 좋습니다.

구문 요청

```
{
  "ConnectorId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: c-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "ConnectorId": "string",
  "Status": "string",
  "StatusMessage": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ConnectorId

테스트 중인 커넥터 객체의 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: c-([0-9a-f]{17})

Status

테스트 성공 시 OK 또는 테스트 실패 시 ERROR를 반환됩니다.

타입: 문자열

StatusMessage

테스트가 성공한 경우 Connection succeeded를 반환합니다. 또는 테스트 실패 시 설명이 포함된 오류 메시지를 반환합니다. 다음 목록은 표시되는 오류 메시지에 따른 문제 해결 세부 정보를 제공합니다.

- 암호 이름이 역할 전송 권한의 이름과 일치하는지 확인하세요.
- 커넥터 구성의 서버를 확인하고 로그인 보안 인증 정보가 커넥터 외부URL에서 성공적으로 작동하는지 확인합니다.
- 암호가 존재하고 형식이 올바른지 확인하세요.
- 커넥터 구성의 신뢰 호스트 키가 ssh-keyscan 출력과 일치하는지 확인하세요.

타입: 문자열

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 원격 서버와의 연결을 테스트합니다.

```
aws transfer test-connection --connector-id c-abcd1234567890fff
```

샘플 응답

API 통화가 성공하면 다음 세부 정보가 반환됩니다.

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

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)

- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

TestIdentityProvider

파일 전송 프로토콜 지원 서버의 IdentityProviderType가 AWS_DIRECTORY_SERVICE 또는 API_Gateway인 경우 ID 제공자가 성공적으로 설정되었는지 테스트합니다. 서버를 생성하는 즉시 이 작업을 호출하여 인증 방법을 테스트하는 것이 좋습니다. 이렇게 하면 ID 제공자 통합 문제를 해결하여 사용자가 서비스를 성공적으로 사용할 수 있도록 할 수 있습니다.

ServerId 및 UserName 파라미터가 필요합니다. ServerProtocol, SourceIp, 및 UserPassword은 모두 옵션입니다.

유념할 사항:

- 서버의 IdentityProviderType가 SERVICE_MANAGED인 경우에는 TestIdentityProvider를 사용할 수 없습니다.
- TestIdentityProvider는 키와 함께 사용할 수 없습니다. 암호만 받아들입니다.
- TestIdentityProvider는 키와 암호를 처리하는 맞춤 ID 공급자의 암호 작업을 테스트할 수 있습니다.
- 파라미터에 잘못된 값을 입력하면 Response 필드가 비어 있습니다.
- 서비스 관리 사용자를 사용하는 서버의 서버 ID를 제공하면 오류가 발생합니다.

An error occurred (InvalidRequestException) when calling the TestIdentityProvider operation: s-server-ID not configured for external auth

- 실제 전송 서버를 식별하지 않는 --server-id 파라미터에 서버 ID를 입력하면 다음과 같은 오류 메시지가 나타납니다.

An error occurred (ResourceNotFoundException) when calling the TestIdentityProvider operation: Unknown server.

서버가 다른 지역에 있을 수 있습니다. 미국 동부(오하이오)에 있는 서버를 지정하는 것과 같이 --region region-code(예: --region us-east-2)를 추가하여 지역을 지정할 수 있습니다.

구문 요청

```
{
  "ServerId": "string",
  "ServerProtocol": "string",
  "SourceIp": "string",
```



```
"UserName": "string",  
"UserPassword": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[ServerId](#)

서버에 대해 시스템에서 할당한 식별자입니다. 사용자 이름과 암호를 사용해 서버의 사용자 인증 방법을 테스트합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

[ServerProtocol](#)

테스트할 파일 전송 프로토콜의 타입입니다.

사용 가능한 프로토콜은 다음과 같습니다:

- 보안 셸(SSH) 파일 전송 프로토콜(SFTP)
- 파일 전송 프로토콜 보안(FTPS)
- 파일 전송 프로토콜(FTP)
- 적용 가능성 설명 2(AS2)

타입: 문자열

유효 값: SFTP | FTP | FTPS | AS2

필수 여부: 아니요

[SourceIp](#)

테스트할 계정의 소스 IP 주소입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이 32.

패턴: \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

필수 여부: 아니요

UserName

테스트할 계정의 명칭입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\w][\w@.-]{2,99}

필수 여부: 예

UserPassword

테스트할 계정의 암호입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이 1,024.

필수 여부: 아니요

응답 구문

```
{
  "Message": "string",
  "Response": "string",
  "StatusCode": number,
  "Url": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

Message

테스트 성공 여부를 나타내는 메시지입니다.

Note

빈 문자열이 반환되는 경우 가장 가능성이 높은 원인은 잘못된 사용자 이름 또는 암호로 인해 인증에 실패했기 때문입니다.

유형: 문자열

Response

API Gateway 또는 Lambda 함수에서 반환되는 응답입니다.

유형: 문자열

StatusCode

API Gateway 또는 Lambda 함수의 응답인 HTTP 상태 코드입니다.

유형: 정수

Url

사용자를 인증하는 데 사용되는 서비스의 엔드포인트입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 요청은 사용자 이름과 암호 조합이 에 사용할 수 있는 유효한 자격 증명이라는 메시지를 자격 증명 공급자로부터 반환합니다 AWS Transfer Family.

샘플 요청

```
{
  "ServerID": "s-01234567890abcdef",
  "UserName": "my_user",
  "UserPassword": "MyPassword-1"
}
```

예

다음 응답은 성공적인 테스트에 대한 샘플 응답을 보여줍니다.

샘플 응답

```
"Response": "
  {\"homeDirectory\": \"~/mybucket001\", \"homeDirectoryDetails\": null,
  \"homeDirectoryType\": \"PATH\", \"posixProfile\": null,
  \"publicKeys\": \"[ssh-rsa-key]\", \"role\": \"arn:aws:iam::123456789012:role/my_role\", \"policy\": null, \"username\": \"transferuser002\",
  \"identityProviderType\": null, \"userConfigMessage\": null})"
```

```
"StatusCode": "200",
"Message": ""
```

예

다음 응답은 지정된 사용자가 액세스 권한이 있는 둘 이상의 그룹에 속해 있음을 나타냅니다.

```
"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."
```

예

API Gateway를 사용하여 사용자 지정 자격 증명 공급자를 생성하고 구성한 경우 다음 명령을 입력하여 사용자를 테스트할 수 있습니다.

```
aws transfer test-identity-provider --server-id s-0123456789abcdefg --user-name myuser
```

여기서 s-0123456789abcdefg는 전송 서버이고 myuser는 맞춤 사용자의 사용자 이름입니다.

명령이 성공하면 다음과 유사한 응답이 표시됩니다, 여기서:

- AWS 계정 ID는 012345678901입니다.
- 사용자 역할: user-role-api-gateway
- 홈 디렉터리는 myuser-bucket임
- 퍼블릭 키는 public-key임
- 호출URL은 호출입니다.URL

```
{
  "Response": "{\"Role\": \"arn:aws:iam::012345678901:role/user-role-api-gateway\", \"HomeDirectory\": \"~/myuser-bucket\", \"PublicKeys\": \"[public-key]\"}\",
  \"StatusCode\": 200,
  \"Message\": \"\",
  \"Url\": \"https://invocation-URL/servers/s-0123456789abcdefg/users/myuser/config\"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UntagResource

Amazon 리소스 이름()으로 식별되는 리소스에서 키-값 페어를 분리합니다ARN. 리소스는 사용자, 서버, 역할 및 기타 개체입니다.

이 직접 호출에서 응답이 반환되지 않습니다.

구문 요청

```
{
  "Arn": "string",
  "TagKeys": [ "string" ]
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Arn

태그가 제거될 리소스의 값입니다. Amazon 리소스 이름(ARN)은 서버, 사용자 또는 역할과 같은 특정 AWS 리소스의 식별자입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

TagKeys

TagKeys 는 유형별로 리소스를 그룹화하고 검색하는 데 사용할 수 ARNs 있는 에 할당된 키-값 페어입니다. 이 메타데이터는 어떤 목적으로든 리소스에 첨부할 수 있습니다.

타입: 문자열 배열

배열 멤버: 최소수는 1개입니다. 최대 항목 수는 50개입니다.

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 128입니다.

필수 여부: 예

Response Elements

작업이 성공하면 서비스는 빈 HTTP 본문과 함께 HTTP 200개의 응답을 다시 보냅니다.

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

예시

예

다음 예에서는 File Transfer 프로토콜이 활성화된 서버의 태그를 제거합니다.

샘플 요청


```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
  "TagKeys": "Europe" ]
}
```

예

이 예제에서는 의 한 가지 사용량을 보여줍니다 UntagResource.

샘플 응답

HTTP 200 response with an empty HTTP body.

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateAccess

ServerID 및 ExternalID 파라미터에 지정된 액세스의 파라미터를 업데이트할 수 있습니다.

구문 요청

```
{
  "ExternalId": "string",
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[ExternalId](#)

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자는 를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

이 명령에서 YourGroupName 를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =, @: /- 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 예

[HomeDirectory](#)

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

[HomeDirectoryMappings](#)

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 는 경로가 Entry 어떻게 표시되는지, Target 는 실제 Amazon S3 또는 Amazon EFS 경로입니다. 대상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할 이 의 경로에 대한 액세스를 제공하는지 확인해야 합니다 Target. 이 값은 이 로 설정된 경우에만 HomeDirectoryType 설정할 수 있습니다 LOGICAL.

다음은 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

대부분의 경우 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리("chroot")로 제한할 수 있습니다. 이렇게 하려면 Entry을 /로 설정하고, Target을 HomeDirectory 파라미터 값으로 설정하면 됩니다.

다음은 chroot에 대한 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

타입: [HomeDirectoryMapEntry](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

[HomeDirectoryType](#)

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

[Policy](#)

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 사용자를 위한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액

세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

Note

이 정책은 `ServerId`의 도메인이 Amazon S3인 경우에만 적용됩니다. AmazonEFS은 세션 정책을 사용하지 않습니다.

세션 정책의 경우 는 정책의 Amazon 리소스 이름(ARN) 대신 정책을 JSON 블록으로 AWS Transfer Family 저장합니다. 정책을 JSON blob으로 저장하고 Policy 인수에 전달합니다. 세션 정책의 예는 [세션 정책 예](#)를 참조하세요.

자세한 내용은 Security Token Service 참조 [AssumeRole](#)의 섹션을 참조하세요. AWS API

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

[PosixProfile](#)

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

[Role](#)

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

필수 여부: 아니요

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이 항목은 사용자를 추가한 특정 서버입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `s-([0-9a-f]{17})`

필수 여부: 예

응답 구문

```
{
  "ExternalId": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ExternalId

AWS Transfer Family를 사용하여 활성화된 프로토콜을 통해 사용자가 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있는 그룹의 외부 식별자입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: `S-1-[\d-]+`

ServerId

사용자가 연결된 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateAgreement

기존 계약의 일부 파라미터를 업데이트합니다. 업데이트할 파라미터의 새 값과 함께 업데이트하려는 계약의 AgreementId와 ServerId를 입력합니다.

구문 요청

```
{
  "AccessRole": "string",
  "AgreementId": "string",
  "BaseDirectory": "string",
  "Description": "string",
  "LocalProfileId": "string",
  "PartnerProfileId": "string",
  "ServerId": "string",
  "Status": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

AccessRole

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출StartFileTransfer하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2수 있습니다SendFilePaths. 파일의 상위 디렉터리(예: 의 경우 --send-file-paths /bucket/dir/file.txt상위 디렉터리는 /bucket/dir/)를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 AccessRole은(는) StartFileTransfer 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 StartFileTransfer와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 secretsmanager:GetSecretValue 권한이 필요합니다. Secrets Manager의 AWS 관리형 키

대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 `kms:Decrypt` 권한도 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 `StartFileTransfer` 요청에서 사용된 파일 위치의 상위 디렉터리
에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 `secretsmanager:GetSecretValue` 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

필수 여부: 아니요

AgreementId

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `a-([0-9a-f]{17})`

필수 여부: 예

BaseDirectory

전송되는 파일의 랜딩 디렉터리(폴더)를 변경하려면 사용할 버킷 폴더(예: `/DOC-EXAMPLE-BUCKET/home/mydirectory`)를 입력합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `(|/.*)`

필수 여부: 아니요

Description

기존 설명을 대체하려면 계약에 대한 간단한 설명을 제공하세요.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: $[\backslash p\{Graph\}]^+$

Required: No

LocalProfileId

AS2 로컬 프로필의 고유 식별자입니다.

로컬 프로필 식별자를 변경하려면 여기에 새 값을 입력합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: $p-([0-9a-f]\{17\})$

필수 여부: 아니요

PartnerProfileId

파트너 프로필의 고유 식별자입니다. 파트너 프로필 식별자를 변경하려면 여기에 새 값을 입력하세요.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: $p-([0-9a-f]\{17\})$

필수 여부: 아니요

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이는 계약에서 사용하는 특정 서버를 나타냅니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: $s-([0-9a-f]\{17\})$

필수 여부: 예

Status

계약 상태를 업데이트하여 비활성 계약을 활성화하거나 그 반대로 업데이트할 수 있습니다.

타입: 문자열

유효 값: ACTIVE | INACTIVE

필수 항목 여부: 아니요

응답 구문

```
{
  "AgreementId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[AgreementId](#)

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: a-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)

- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateCertificate

인증서의 활성 및 비활성 날짜를 업데이트합니다.

구문 요청

```
{  
  "ActiveDate": number,  
  "CertificateId": "string",  
  "Description": "string",  
  "InactiveDate": number  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

ActiveDate

인증서가 활성화되는 시기를 지정하는 선택적 날짜입니다.

타입: Timestamp

필수 여부: 아니요

CertificateId

업데이트하려는 인증서 객체의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

Pattern: cert-([0-9a-f]{17})

필수 여부: 예

Description

인증서를 식별하는 데 도움이 되는 간단한 설명입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: [\p{Graph}]+

필수 여부: 아니요

InactiveDate

인증서가 비활성화되는 시기를 지정하는 선택적 날짜.

타입: Timestamp

필수 여부: 아니요

응답 구문

```
{  
  "CertificateId": "string"  
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

CertificateId

업데이트 중인 인증서 객체의 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예제에서는 인증서의 활성 날짜를 업데이트하여 활성 날짜를 2022년 1월 16일 16:12:07 UTC -5 시간으로 설정합니다.

샘플 요청

```
aws transfer update-certificate --certificate-id c-abcdefgh123456hijk --active-date
2022-01-16T16:12:07-05:00
```

예

다음은 이 API 호출에 대한 샘플 응답입니다.

샘플 응답

```
"CertificateId": "c-abcdefgh123456hijk"
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateConnector

기존 커넥터의 일부 파라미터를 업데이트합니다. 업데이트할 파라미터의 새 값과 함께 업데이트하려는 프로파일의 ConnectorId를 입력합니다.

구문 요청

```
{
  "AccessRole": "string",
  "As2Config": {
    "BasicAuthSecretId": "string",
    "Compression": "string",
    "EncryptionAlgorithm": "string",
    "LocalProfileId": "string",
    "MdnResponse": "string",
    "MdnSigningAlgorithm": "string",
    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "ConnectorId": "string",
  "LoggingRole": "string",
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Url": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

AccessRole

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출 `StartFileTransfer` 하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2 수 있습니다 `SendFilePaths`. 파일의 상위 디렉터리(예: 의 경우 `--send-file-paths /bucket/dir/file.txt`) 상위 디렉터리는 `/bucket/dir/`를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 `AccessRole`은(는) `StartFileTransfer` 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 `StartFileTransfer`와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 `secretsmanager:GetSecretValue` 권한이 필요합니다. Secrets Manager의 AWS 관리형 키 대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 `kms:Decrypt` 권한도 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 `StartFileTransfer` 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 에 대한 `secretsmanager:GetSecretValue` 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

Required: No

[As2Config](#)

AS2 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [As2ConnectorConfig](#) 객체

필수 여부: 아니요

[ConnectorId](#)

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: c-([0-9a-f]{17})

필수 여부: 예

[LoggingRole](#)

커넥터가 Amazon S3 이벤트에 대한 CloudWatch 로깅을 켤 수 있도록 허용하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. Amazon S3 설정하면 CloudWatch 로그에서 커넥터 활동을 볼 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

[SftpConfig](#)

SFTP 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [SftpConnectorConfig](#) 객체

필수 여부: 아니요

[Url](#)

파트너 AS2 또는 SFTP 엔드포인트URL의 .

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

필수 여부: 아니요

응답 구문

```
{
  "ConnectorId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ConnectorId

업데이트 중인 커넥터 객체의 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: c-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateHostKey

ServerId 및 HostKeyId 파라미터로 지정된 호스트 키의 설명을 업데이트합니다.

구문 요청

```
{
  "Description": "string",
  "HostKeyId": "string",
  "ServerId": "string"
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

Description

호스트 키에 대한 업데이트된 설명입니다.

타입: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: [\p{Print}]*

필수 여부: 예

HostKeyId

업데이트 중인 호스트 키의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

Pattern: hostkey-[0-9a-f]{17}

필수 여부: 예

[ServerId](#)

업데이트 중인 호스트 키가 들어 있는 서버의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[HostKeyId](#)

업데이트된 호스트 키의 호스트 키 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

패턴: hostkey-[0-9a-f]{17}

[ServerId](#)

업데이트된 호스트 키가 들어 있는 서버에 대한 서버 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)
- [AWS SDK C++용](#)

- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateProfile

기존 프로필의 일부 파라미터를 업데이트합니다. 업데이트할 파라미터의 새 값과 함께 업데이트하려는 프로필의 ProfileId를 입력합니다.

구문 요청

```
{  
  "CertificateIds": [ "string" ],  
  "ProfileId": "string"  
}
```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

CertificateIds

가져온 인증서의 식별자 배열입니다. 프로필 및 파트너 프로필 작업에 이 식별자를 사용합니다.

타입: 문자열 배열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

Required: No

ProfileId

업데이트하려는 프로필 객체의 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: p-([0-9a-f]{17})

필수 여부: 예

응답 구문

```
{  
  "ProfileId": "string"  
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[ProfileId](#)

업데이트 중인 프로필의 식별자를 반환합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateServer

서버가 생성된 후 파일 전송 프로토콜이 활성화된 서버의 속성을 업데이트합니다.

이 UpdateServer 호출은 업데이트한 서버의 ServerId를 반환합니다.

구문 요청

```
{
  "Certificate": "string",
  "EndpointDetails": {
    "AddressAllocationIds": [ "string" ],
    "SecurityGroupIds": [ "string" ],
    "SubnetIds": [ "string" ],
    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKey": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
  "ServerId": "string",
  "StructuredLogDestinations": [ "string" ],
  "WorkflowDetails": {
```

```

    "OnPartialUpload": [
      {
        "ExecutionRole": "string",
        "WorkflowId": "string"
      }
    ],
    "OnUpload": [
      {
        "ExecutionRole": "string",
        "WorkflowId": "string"
      }
    ]
  }
}

```

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[Certificate](#)

AWS Certificate Manager(ARN) 인증서의 Amazon 리소스 이름(ACM)입니다. Protocols이(가) FTPS(으)로 설정된 경우에 필요합니다.

새 퍼블릭 인증서를 요청하려면 AWS Certificate Manager 사용 설명서의 [퍼블릭 인증서 요청](#)을 참조하세요.

기존 인증서를 로 가져오려면 AWS Certificate Manager 사용 설명서의 [로 인증서 가져오기ACM](#)를 ACM참조하세요.

프라이빗 IP 주소를 FTPS 통해 프라이빗 인증서를 사용하도록 요청하려면 AWS Certificate Manager 사용 설명서의 [프라이빗 인증서 요청을 참조하세요](#).

다음 암호화 알고리즘 및 키 크기를 사용하는 인증서가 지원됩니다:

- 2048비트RSA(RSA_2048)
- 4096비트RSA(RSA_4096)
- 타원 프라임 곡선 256비트(EC_prime256v1)
- 타원 프라임 곡선 384 비트(EC_secp384r1)

- 타원 프라임 곡선 521비트(EC_secp521r1)

Note

인증서는 FQDN 또는 IP 주소가 지정된 유효한 SSL/TLS X.509 버전 3 인증서와 발급자에 대한 정보여야 합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1600입니다.

필수 여부: 아니요

EndpointDetails

서버에 대해 구성된 가상 프라이빗 클라우드(VPC) 엔드포인트 설정입니다. 내에서 엔드포인트를 호스팅할 때 엔드포인트를 내 리소스에만 액세스하도록 하거나 VPC탄력적 IP 주소를 연결하고 인터넷을 통해 클라이언트가 엔드포인트에 액세스할 VPC수 있도록 할 수 있습니다. VPC의 기본 보안 그룹은 엔드포인트에 자동으로 할당됩니다.

유형: [EndpointDetails](#) 객체

필수 여부: 아니요

EndpointType

서버에서 사용할 엔드포인트 타입입니다. 서버의 엔드포인트에 공개적으로 액세스(PUBLIC)하거나에서 호스팅하도록 선택할 수 있습니다VPC. 에서 호스팅되는 엔드포인트를 사용하면 내에서만 서버 및 리소스에 대한 액세스를 제한VPC하거나 Elastic IP 주소를 직접 연결하여 인터넷에 연결하도록 선택할 VPC수 있습니다.

Note

2021년 5월 19일 이후에는 2021년 5월 19일 이전에 AWS계정이 아직 생성되지 않은 경우 계정EndpointType=VPC_ENDPOINT에서 를 사용하여 서버를 생성할 수 없습니다. 2021년 5월 19일 또는 그 이전에 EndpointType=VPC_ENDPOINT AWS계정에 가 있는 서버를 이미 생성한 경우 영향을 받지 않습니다. 이 날짜 이후에는 EndpointType=VPC를 사용하세요.

자세한 내용은 [VPC 사용 중단ENDPOINT](#)를 참조하세요.

VPC를 EndpointType(으)로 사용하는 것이 좋습니다. 이 엔드포인트 유형을 사용하면 최대 3개의 탄력적 IPv4 주소(BYOIP 포함)를 서버의 엔드포인트와 직접 연결하고 VPC

보안 그룹을 사용하여 클라이언트의 퍼블릭 IP 주소로 트래픽을 제한할 수 있습니다. EndpointType를 VPC_ENDPOINT(으)로 설정하면 이 작업을 할 수 없습니다.

타입: 문자열

유효 값: PUBLIC | VPC | VPC_ENDPOINT

필수 여부: 아니요

HostKey

SFTP사용 가능한 서버에 사용할 RSAECDSA, 또는 ED25519 프라이빗 키입니다. 키를 교체하거나 다른 알고리즘을 사용하는 활성 키 집합이 있는 경우, 여러 호스트 키를 추가할 수 있습니다.

다음 명령을 사용하여 암호 없이 RSA 2048비트 키를 생성합니다.

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

-b 옵션에는 최소값인 2048을 사용합니다. 3072 또는 4096을 사용하여 더 강력한 키를 만들 수 있습니다.

다음 명령을 사용하여 암호 없이 ECDSA 256비트 키를 생성합니다.

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

에 대한 -b 옵션의 유효한 값은 256, 384 및 521ECDSA입니다.

다음 명령을 사용하여 암호가 없는 ED25519 키를 생성합니다.

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

이러한 모든 명령의 경우 를 원하는 문자열my-new-server-key로 바꿀 수 있습니다.

Important

기존 사용자를 기존 SFTP지원 서버에서 새 서버로 마이그레이션할 계획이 없는 경우 호스트 키를 업데이트하지 마세요. 실수로 서버의 호스트 키를 변경하면 작업에 영향을 줄 수 있습니다.

자세한 내용은 AWS Transfer Family 사용 설명서의 [SFTP사용 가능한 서버의 호스트 키 업데이트를 참조하세요.](#)

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096입니다.

필수 여부: 아니요

[IdentityProviderDetails](#)

고객의 인증 API 방법을 호출하는 데 필요한 모든 정보가 포함된 배열입니다.

유형: [IdentityProviderDetails](#) 객체

필수 여부: 아니요

[LoggingRole](#)

서버가 Amazon S3 또는 Amazon 에 대한 Amazon CloudWatch 로깅을 켤 수 있도록 허용하는 () 역할ARN의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다EFSevents. 설정하면 CloudWatch 로그에서 사용자 활동을 볼 수 있습니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2,048.

패턴: (|arn:.*role/\S+)

필수 여부: 아니요

[PostAuthenticationLoginBanner](#)

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증한 후에 표시됩니다.

Note

SFTP 프로토콜은 인증 후 표시 배너를 지원하지 않습니다.

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: [\x09-\x0D\x20-\x7E]*

필수 여부: 아니요

[PreAuthenticationLoginBanner](#)

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증하기 전에 표시됩니다. 예를 들어 다음 배너는 시스템 사용에 대한 세부 정보를 표시합니다.

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

타입: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: `[\x09-\x0D\x20-\x7E]*`

필수 여부: 아니요

[ProtocolDetails](#)

서버에 대해 구성된 프로토콜 설정입니다.

- 패시브 모드(FTP 및 FTPS 프로토콜용)를 표시하려면 `PassiveIp` 파라미터를 사용합니다. 방화벽, 라우터 또는 로드 밸런서의 외부 IP IPv4 주소와 같은 단일 점 쿼드 주소를 입력합니다.
- Amazon S3 버킷에 업로드하는 파일에 대해 클라이언트가 `SETSTAT` 명령을 사용하려 할 때 생성되는 오류를 무시하려면 `SetStatOption` 파라미터를 사용합니다. AWS Transfer Family 서버가 SFTP 클라이언트를 변경할 필요 없이 `SETSTAT` 명령을 무시하고 파일을 업로드하도록 하려면 값을 `ENABLE_NO_OP`로 설정합니다. `SetStatOption` 파라미터를 `ENABLE_NO_OP`로 설정하면 Transfer Family가 Amazon CloudWatch Logs에 로그 항목을 생성하여 클라이언트가 `SETSTAT` 전화를 거는 시기를 확인할 수 있습니다.
- AWS Transfer Family 서버가 고유한 세션 ID를 통해 최근 협상된 세션을 재개하는지 확인하려면 `TlsSessionResumptionMode` 파라미터를 사용합니다.
- `As2Transports`는 AS2 메시지의 전송 방법을 나타냅니다. 현재 HTTP만 지원됩니다.

유형: [ProtocolDetails](#) 객체

필수 여부: 아니요

[Protocols](#)

파일 전송 프로토콜 클라이언트가 서버의 엔드포인트에 연결할 수 있는 파일 전송 프로토콜을 지정합니다. 사용 가능한 프로토콜은 다음과 같습니다:

- SFTP (Secure Shell (SSH) 파일 전송 프로토콜): 파일 전송 SSH
- FTPS (파일 전송 프로토콜 보안): TLS 암호화를 사용한 파일 전송
- FTP (File Transfer Protocol): 암호화되지 않은 파일 전송
- AS2 (적용 설명 2): 구조화된 business-to-business 데이터 전송에 사용

Note

- 를 선택하는 경우 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용되는 AWS Certificate Manager (ACM)에 저장된 인증서를 선택해야 FTPS합니다FTPS.
- Protocol에 FTP 또는 FTPS이(가) 포함된 경우 EndpointType은(는) VPC이고 IdentityProviderType은(는) AWS_DIRECTORY_SERVICE, AWS_LAMBDA 또는 API_GATEWAY여야 합니다.
- Protocol에 FTP이(가) 포함된 경우 AddressAllocationIds를 연결할 수 없습니다.
- Protocol이 SFTP로만 설정된 경우 EndpointType을 PUBLIC으로 설정하고 IdentityProviderType을 지원되는 ID 타입(SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA, API_GATEWAY) 중 하나로 설정할 수 있습니다.
- Protocol에 AS2이(가) 포함된 경우 EndpointType은(는) VPC여야 하고, 도메인은 Amazon S3여야 합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 4개입니다.

유효 값: SFTP | FTP | FTPS | AS2

필수 여부: 아니요

S3StorageOptions

Amazon S3 디렉터리의 성능 최적화 여부를 지정합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

기본적으로 홈 디렉터리 매핑의 는 TYPE입니다DIRECTORY. 이 옵션을 활성화하면 매핑에 파일 대상이 포함되도록 HomeDirectoryMapEntry Type FILE 하려면 를 로 명시적으로 설정해야 합니다.

유형: S3StorageOptions 객체

필수 여부: 아니요

SecurityPolicyName

서버에 연결된 보안 정책의 명칭을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

패턴: TransferSecurityPolicy-.+

Required: No

ServerId

Transfer Family 사용자가 할당된 서버 인스턴스에 대한 시스템 할당 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

StructuredLogDestinations

사용자의 서버 로그가 전송될 로그 그룹을 지정합니다.

로그 그룹을 지정하려면 기존 로그 그룹에 ARN 대해 를 제공해야 합니다. 이 경우, 로그 그룹의 형식은 다음과 같습니다:

arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*

예제: arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*

이전에 서버의 로그 그룹을 지정한 경우, update-server 호출 시 이 파라미터에 빈 값을 제공하여 로그 그룹을 지우고 사실상 구조화된 로깅을 끌 수 있습니다. 예:

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

타입: 문자열 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 1개입니다.

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

Required: No

[WorkflowDetails](#)

할당할 워크플로의 워크플로 ID와 워크플로 실행에 사용되는 실행 역할을 지정합니다.

파일이 완전히 업로드될 때 실행되는 워크플로 외에도 WorkflowDetails에는 부분 업로드 시 실행할 워크플로의 워크플로 ID와 실행 역할이 포함될 수 있습니다. 파일이 업로드되는 동안 서버 세션 연결이 끊기면 부분 업로드가 수행됩니다.

서버에서 연결된 워크플로를 제거하려면 다음 예와 같이 빈 OnUpload 객체를 제공하면 됩니다.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-
details '{"OnUpload":[]}'
```

타입: [WorkflowDetails](#) 객체

필수 항목 여부: 아니요

응답 구문

```
{
  "ServerId": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

[ServerId](#)

Transfer Family 사용자가 할당된 서버에 대한 시스템 할당 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 [일반적인 오류](#) 섹션을 참조하세요.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

ConflictException

이 예외는 UpdateServer가 엔드포인트 유형VPC으로 가 있고 서버VpcEndpointID가 사용 가능한 상태가 아닌 파일 전송 프로토콜 지원 서버에 대해 호출될 때 발생합니다.

HTTP 상태 코드: 400

InternalServiceError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceExistsException

요청된 리소스가 존재하지 않거나 명령에 지정된 리전이 아닌 다른 리전에 있습니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 서버의 역할을 업데이트합니다.

샘플 요청

```
{
  "EndpointDetails": {
    "VpcEndpointId": "vpce-01234f056f3g13",
    "LoggingRole": "CloudWatchS3Events",
    "ServerId": "s-01234567890abcdef"
  }
}
```

예

다음 예에서는 모든 관련 워크플로를 서버에서 제거합니다.

샘플 요청

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
'{"OnUpload":[]}'
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "ServerId": "s-01234567890abcdef"
}
```

```
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용 .NET](#)
- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

UpdateUser

사용자에게 새 속성을 할당합니다. 전달한 파라미터는 지정한 UserName 및 ServerId의 홈 디렉터리, 역할, 정책 중 일부 또는 전부를 수정합니다.

응답은 업데이트된 사용자에게 ServerId 및 UserName를 반환합니다.

콘솔에서 사용자를 생성하거나 업데이트할 때 제한됨을 선택할 수 있습니다. 이렇게 하면 사용자가 홈 디렉터리 외부의 어떤 것에도 액세스할 수 없습니다. 이 동작을 프로그래밍 방식으로 구성하는 방법은 사용자를 업데이트하는 것입니다. 를 HomeDirectoryType로 설정하고 HomeDirectoryMappings를 루트(/)Entry로 LOGICAL지정하고 를 홈 디렉터리Target로 지정합니다.

예를 들어 사용자의 홈 디렉터리가 인 경우 콘솔의 구성에 제한된 플래그가 선택됨으로 표시되도록 /test/admin-user다음 명령은 사용자를 업데이트합니다.

```
aws transfer update-user --server-id <server-id> --user-name admin-user --home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/\", \"Target\":\"/test/admin-user\"}]"
```

구문 요청

```
{
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string",
  "UserName": "string"
```

}

요청 파라미터

모든 작업에 공통되는 파라미터에 대한 내용은 [공통 파라미터](#)를 참조하십시오.

요청은 JSON 형식의 다음 데이터를 수락합니다.

[HomeDirectory](#)

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

[HomeDirectoryMappings](#)

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 Entry는 경로가 어떻게 표시되는지, Target는 실제 Amazon S3 또는 Amazon EFS 경로입니다. 대상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할이 의 경로에 대한 액세스를 제공하는지 확인해야 합니다 Target. 이 값은 이 로 설정된 경우에만 HomeDirectoryType 설정할 수 있습니다 LOGICAL.

다음은 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

대부분의 경우 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리("chroot")로 제한할 수 있습니다. 이렇게 하려면 `"/Entry"`로 설정하고 파라미터 값으로 설정할 수 `Target` 있습니다 `HomeDirectory`.

다음은 `chroot`에 대한 `Entry` 및 `Target` 쌍의 예입니다.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

타입: [HomeDirectoryMapEntry](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

[HomeDirectoryType](#)

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 `PATH`파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 `HomeDirectoryMappings` 대한 매핑을 에 `LOGICAL`제공해야 합니다.

Note

`HomeDirectoryType`이 `LOGICAL`인 경우, `HomeDirectoryMappings` 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 `HomeDirectoryType`이 `PATH`인 경우, `HomeDirectory` 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 `HomeDirectory` 및 `HomeDirectoryMappings`를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: `PATH` | `LOGICAL`

필수 여부: 아니요

[Policy](#)

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 사용자를 위한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

Note

이 정책은 ServerId의 도메인이 Amazon S3인 경우에만 적용됩니다. AmazonEFS은 세션 정책을 사용하지 않습니다.

세션 정책의 경우 는 정책의 Amazon 리소스 이름(ARN) 대신 정책을 JSON 블록으로 AWS Transfer Family 저장합니다. 정책을 JSON blob으로 저장하고 Policy 인수에 전달합니다. 세션 정책의 예는 [세션 정책 예](#)를 참조하세요.

자세한 내용은 Security Token Service 참조 [AssumeRole](#)의 섹션을 참조하세요. AWS API

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

PosixProfile

Amazon Elastic File Systems(AmazonEfs)에 대한 사용자의 액세스를 제어하는 사용자 ID(IDs(Uid), 그룹 ID(SecondaryGids) 및 보조 그룹())을 포함한 전체 POSIX 자격 증명을 지정합니다. EFS. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

ServerId

사용자가 할당된 Transfer Family 서버 인스턴스에 대한 시스템 할당 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

UserName

ServerId에서 지정된 바와 같이 사용자를 식별하고 서버와 연결되는 고유한 문자열입니다. 이 사용자 이름은 3~100자여야 합니다. a-z, A-Z, 0-9, _(밑줄), -(하이픈), .(마침표) 및 @ 기호를 유효한 문자로 사용할 수 있습니다. 사용자 이름은 하이픈, 마침표 및 @ 기호로 시작할 수 없습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\\w][\\w@.-]{2,99}

필수 여부: 예

응답 구문

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Response Elements

작업이 성공하면 서비스가 HTTP 200개의 응답을 다시 보냅니다.

다음 데이터는 서비스에서 JSON 형식으로 반환됩니다.

ServerId

계정이 할당된 Transfer Family 서버 인스턴스에 대한 시스템 할당 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

UserName

요청에 지정된 서버 인스턴스에 할당된 사용자의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\w][\w@.-]{2,99}

Errors

모든 작업에 공통되는 오류에 대한 내용은 [일반적인 오류](#) 섹션을 참조하십시오.

InternalServerError

이 예외는 AWS Transfer Family 서비스에서 오류가 발생할 때 발생합니다.

HTTP 상태 코드: 500

InvalidRequestException

이 예외는 클라이언트가 잘못된 형식의 요청을 제출할 때 던져집니다.

HTTP 상태 코드: 400

ResourceNotFoundException

AWS Transfer Family 서비스에서 리소스를 찾을 수 없는 경우 이 예외가 발생합니다.

HTTP 상태 코드: 400

ServiceUnavailableException

AWS Transfer Family 서비스를 사용할 수 없으므로 요청이 실패했습니다.

HTTP 상태 코드: 500

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

예시

예

다음 예에서는 Transfer Family 사용자를 업데이트합니다.

샘플 요청

```
{
  "HomeDirectory": "/bucket2/documentation",
  "HomeDirectoryMappings": [
    {
      "Entry": "/directory1",
      "Target": "/bucket_name/home/mydirectory"
    }
  ],
  "HomeDirectoryType": "PATH",
  "Role": "AssumeRole",
  "ServerId": "s-01234567890abcdef",
  "UserName": "my_user"
}
```

예

이 API 통화의 샘플 응답입니다.

샘플 응답

```
{
  "ServerId": "s-01234567890abcdef",
  "UserName": "my_user"
}
```

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS Command Line Interface](#)
- [AWS SDK 용.NET](#)

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK PHP V3용](#)
- [AWS SDK Python용](#)
- [AWS SDK Ruby V3용](#)

데이터 유형

다음 데이터 유형이 지원됩니다.

- [As2ConnectorConfig](#)
- [CopyStepDetails](#)
- [CustomStepDetails](#)
- [DecryptStepDetails](#)
- [DeleteStepDetails](#)
- [DescribedAccess](#)
- [DescribedAgreement](#)
- [DescribedCertificate](#)
- [DescribedConnector](#)
- [DescribedExecution](#)
- [DescribedHostKey](#)
- [DescribedProfile](#)
- [DescribedSecurityPolicy](#)
- [DescribedServer](#)
- [DescribedUser](#)
- [DescribedWorkflow](#)
- [EfsFileLocation](#)
- [EndpointDetails](#)
- [ExecutionError](#)

- [ExecutionResults](#)
- [ExecutionStepResult](#)
- [FileLocation](#)
- [HomeDirectoryMapEntry](#)
- [IdentityProviderDetails](#)
- [InputFileLocation](#)
- [ListedAccess](#)
- [ListedAgreement](#)
- [ListedCertificate](#)
- [ListedConnector](#)
- [ListedExecution](#)
- [ListedHostKey](#)
- [ListedProfile](#)
- [ListedServer](#)
- [ListedUser](#)
- [ListedWorkflow](#)
- [LoggingConfiguration](#)
- [PosixProfile](#)
- [ProtocolDetails](#)
- [S3FileLocation](#)
- [S3InputFileLocation](#)
- [S3StorageOptions](#)
- [S3Tag](#)
- [ServiceMetadata](#)
- [SftpConnectorConfig](#)
- [SshPublicKey](#)
- [Tag](#)
- [TagStepDetails](#)
- [UserDetails](#)
- [WorkflowDetail](#)

- [WorkflowDetails](#)
- [WorkflowStep](#)

As2ConnectorConfig

AS2 커넥터 객체에 대한 세부 정보를 포함합니다. 커넥터 객체는 AS2 아웃바운드 프로세스에 사용되며 고객을 AWS Transfer Family 거래 파트너와 연결하는 데 사용됩니다.

내용

BasicAuthSecretId

AS2 커넥터에 기본 인증 지원을 제공합니다. 기본 인증을 사용하려면 보안 암호의 이름 또는 Amazon 리소스 이름(ARN)을 제공해야 합니다 AWS Secrets Manager.

이 파라미터의 기본값은 null이며, 커넥터에 대해 기본 인증을 사용할 수 없음을 나타냅니다.

커넥터에서 기본 인증을 사용해야 하는 경우 암호는 다음 형식이어야 합니다.

```
{ "Username": "user-name", "Password": "user-password" }
```

user-name 및 user-password를 인증 중인 실제 사용자의 보안 인증 정보로 바꾸세요.

유의할 사항:

- 이러한 보안 인증 정보를 이 에 직접 전달하지 않고 Secrets Manager에 저장합니다.
- API, SDKs 또는 CloudFormation을 사용하여 커넥터를 구성하는 경우 기본 인증을 활성화하려면 먼저 보안 암호를 생성해야 합니다. 그러나 AWS 관리 콘솔을 사용하는 경우 시스템에서 보안 암호를 생성하도록 할 수 있습니다.

이전에 커넥터에 대한 기본 인증을 활성화한 경우 UpdateConnector API 호출을 사용하여 비활성화할 수 있습니다. 예를 들어 를 사용하는 경우 다음 명령을 실행하여 기본 인증을 제거할 수 있습니다.

```
update-connector --connector-id my-connector-id --as2-config
'BasicAuthSecretId=""'
```

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

Compression

AS2 파일이 압축되는지 여부를 지정합니다.

타입: 문자열

유효 값: ZLIB | DISABLED

필수 여부: 아니요

EncryptionAlgorithm

알고리즘은 파일을 암호화하는 데 사용됩니다.

유의할 사항:

- DES_EDE3_CBC 알고리즘이 필요한 레거시 클라이언트를 지원해야 하는 경우가 아니면 알고리즘을 사용하지 마세요. 암호화 알고리즘이 약하기 때문입니다.
- 커넥터URL의 NONE가 를 사용하는 경우에만 지정할 수 있습니다HTTPS. HTTPS 를 사용하면 트래픽이 일반 텍스트로 전송되지 않습니다.

타입: 문자열

유효 값: AES128_CBC | AES192_CBC | AES256_CBC | DES_EDE3_CBC | NONE

필수 여부: 아니요

LocalProfileId

AS2 로컬 프로필의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Required: No

MdnResponse

전송에 대한 파트너 응답이 동기식인지 비동기식인지 여부를 결정하기 위한 아웃바운드 요청 (AWS Transfer Family 서버에서 파트너 AS2 서버로)에 사용됩니다. 다음 값 중 하나를 지정합니다.

- SYNC: 시스템은 동기 MDN 응답을 예상하여 파일이 성공적으로 전송되었는지(또는 전송되지 않았는지) 확인합니다.
- NONE: MDN 응답이 필요하지 않음을 지정합니다.

타입: 문자열

유효 값: SYNC | NONE

필수 여부: 아니요

MdnSigningAlgorithm

MDN 응답의 서명 알고리즘입니다.

Note

를 로 설정하면DEFAULT(또는 전혀 설정하지 않으면) 의 값이 SigningAlgorithm 사용 됩니다.

타입: 문자열

유효 값: SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

필수 여부: 아니요

MessageSubject

커넥터와 함께 전송되는 AS2 메시지에서 Subject HTTP 헤더 속성으로 사용됩니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 1024입니다.

패턴: [\p{Print}\p{Blank}]+

Required: No

PartnerProfileId

커넥터의 파트너 프로필의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Required: No

SigningAlgorithm

커넥터로 전송된 AS2 메시지에 서명하는 데 사용되는 알고리즘입니다.

타입: 문자열

유효 값: SHA256 | SHA384 | SHA512 | SHA1 | NONE

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

CopyStepDetails

각 단계 타입에는 자체의 StepDetails 구조가 있습니다.

내용

DestinationFileLocation

복사할 파일의 위치를 지정합니다. 이 필드에서 `${Transfer:UserName}` 또는 `${Transfer:UploadDate}`를 사용하여 사용자 이름 또는 업로드 날짜를 기준으로 대상 접두사를 파라미터화할 수 있습니다.

- 파일을 업로드한 Transfer Family 사용자의 명칭이 접두사로 붙은 Amazon S3 버킷에 업로드된 파일을 복사하려면 DestinationFileLocation의 값을 `${Transfer:UserName}`(으)로 설정합니다.
- 업로드 날짜 접두사가 붙은 Amazon S3 버킷에 업로드된 파일을 복사하려면 DestinationFileLocation의 값을 `${Transfer:UploadDate}`(으)로 설정합니다.



Note

파일은 UploadDate에 업로드된 날짜를 기준으로 YYYY-MM-DD의 날짜 형식으로 확인됩니다. UTC.

유형: [InputFileLocation](#) 객체

필수 여부: 아니요

Name

단계의 명칭, 식별자로 사용됨.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 30입니다.

패턴: `[\w-]*`

필수 여부: 아니요

OverwriteExisting

같은 명칭의 기존 파일을 덮어쓸지 여부를 나타내는 플래그입니다. 기본값은 FALSE입니다.

워크플로에서 기존 파일과 명칭이 같은 파일을 처리하는 경우, 동작은 다음과 같습니다.

- `OverwriteExisting`(가) `TRUE`인 경우, 기존 파일이 처리 중인 파일로 대체됩니다.
- `OverwriteExisting`(가) `FALSE`인 경우, 아무 일도 일어나지 않고 워크플로 처리가 중지됩니다.

타입: 문자열

유효 값: `TRUE` | `FALSE`

필수 여부: 아니요

SourceFileLocation

워크플로 단계의 입력으로 사용할 파일(이전 단계의 출력 또는 워크플로에 처음 업로드한 파일)을 지정합니다.

- 이전 파일을 입력으로 사용하려면 `${previous.file}`를 입력합니다. 이 경우 이 워크플로 단계에서는 이전 워크플로 단계의 출력 파일을 입력으로 사용합니다. 이것이 기본값입니다.
- 시초로 업로드된 파일 위치를 이 단계의 입력으로 사용하려면 `${original.file}`를 입력합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `^\$\\{(\w+.)+\w+\\}`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

CustomStepDetails

각 단계 타입에는 자체의 StepDetails 구조가 있습니다.

내용

Name

단계의 명칭, 식별자로 사용됨.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 30입니다.

패턴: `[\w-]*`

필수 여부: 아니요

SourceFileLocation

워크플로 단계의 입력으로 사용할 파일(이전 단계의 출력 또는 워크플로에 처음 업로드한 파일)을 지정합니다.

- 이전 파일을 입력으로 사용하려면 `${previous.file}`를 입력합니다. 이 경우 이 워크플로 단계에서는 이전 워크플로 단계의 출력 파일을 입력으로 사용합니다. 이것이 기본값입니다.
- 시초로 업로드된 파일 위치를 이 단계의 입력으로 사용하려면 `${original.file}`를 입력합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `\$\{(\w+.\w+)\}`

Required: No

Target

호출 중인 Lambda 함수ARN의 입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 170입니다.

패턴: `arn:[a-z-]+:lambda:.*`

필수 여부: 아니요

TimeoutSeconds

단계에 대한 시간 제한 (단위: 초).

타입: 정수

유효한 범위: 최소값은 1입니다. 최대값은 1800입니다.

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DecryptStepDetails

각 단계 타입에는 자체의 StepDetails 구조가 있습니다.

내용

DestinationFileLocation

해독되는 파일의 위치를 지정합니다. 이 필드에서 `${Transfer:UserName}` 또는 `${Transfer:UploadDate}`를 사용하여 사용자 이름 또는 업로드 날짜를 기준으로 대상 접두사를 파라미터화할 수 있습니다.

- 파일을 업로드한 Transfer Family 사용자의 명칭이 접두사로 붙은 Amazon S3 버킷에 업로드된 파일을 복호화하려면 DestinationFileLocation의 값을 `${Transfer:UserName}`으(로) 설정합니다.
- 업로드 날짜가 접두사가 붙은 Amazon S3 버킷에 업로드된 파일을 복호화하려면 DestinationFileLocation의 값을 `${Transfer:UploadDate}`으(로) 설정합니다.



Note

파일은 UploadDate에 업로드된 날짜를 기준으로 YYYY-MM-DD의 날짜 형식으로 확인됩니다. UTC.

유형: [InputFileLocation](#) 객체

필수 여부: 예

Type

사용된 암호화 타입. 현재, 이 값은 PGP이어야 합니다.

타입: 문자열

유효 값: PGP

필수 여부: 예

Name

단계의 명칭, 식별자로 사용됨.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 30입니다.

패턴: `[\w-]*`

필수 여부: 아니요

OverwriteExisting

같은 명칭의 기존 파일을 덮어쓸지 여부를 나타내는 플래그입니다. 기본값은 FALSE입니다.

워크플로에서 기존 파일과 명칭이 같은 파일을 처리하는 경우, 동작은 다음과 같습니다.

- OverwriteExisting이(가) TRUE인 경우, 기존 파일이 처리 중인 파일로 대체됩니다.
- OverwriteExisting이(가) FALSE인 경우, 아무 일도 일어나지 않고 워크플로 처리가 중지됩니다.

타입: 문자열

유효 값: TRUE | FALSE

필수 여부: 아니요

SourceFileLocation

워크플로 단계의 입력으로 사용할 파일(이전 단계의 출력 또는 워크플로에 처음 업로드한 파일)을 지정합니다.

- 이전 파일을 입력으로 사용하려면 `${previous.file}`를 입력합니다. 이 경우 이 워크플로 단계에서는 이전 워크플로 단계의 출력 파일을 입력으로 사용합니다. 이것이 기본값입니다.
- 시초로 업로드된 파일 위치를 이 단계의 입력으로 사용하려면 `${original.file}`를 입력합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `\$\{(\w+.\w+)\}`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DeleteStepDetails

단계의 명칭, 삭제 단계를 나타내는 데 사용됨.

내용

Name

단계의 명칭, 식별자로 사용됨.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 30입니다.

패턴: `[\w-]*`

필수 여부: 아니요

SourceFileLocation

워크플로 단계의 입력으로 사용할 파일(이전 단계의 출력 또는 워크플로에 처음 업로드한 파일)을 지정합니다.

- 이전 파일을 입력으로 사용하려면 `${previous.file}`를 입력합니다. 이 경우 이 워크플로 단계에서는 이전 워크플로 단계의 출력 파일을 입력으로 사용합니다. 이것이 기본값입니다.
- 시초로 업로드된 파일 위치를 이 단계의 입력으로 사용하려면 `${original.file}`를 입력합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `\$\{(\w+.\w+)\}`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)

- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedAccess

지정된 액세스 속성을 설명합니다.

내용

ExternalId

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자를 를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName, ObjectSid
```

이 명령에서 YourGroupName 를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =, ., @, /- 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 아니요

HomeDirectory

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

HomeDirectoryMappings

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 는 경로가 어떻게 표시되는 Entry지, 는 실제 Amazon S3 또는 Amazon EFS 경로 Target입니다. 대상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할 이 의 경로에 대한 액세스를 제공하는지 확인해야 합니다 Target. 이 값은 이 로 설정된 경우에만 HomeDirectoryType 설정할 수 있습니다 LOGICAL.

대부분의 경우 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리("chroot")의 연계된 액세스로 제약할 수 있습니다. 이렇게 하려면 Entry를 '/'로 설정하고, Target를 HomeDirectory 파라미터 값으로 설정하면 됩니다.

타입: [HomeDirectoryMapEntry](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

HomeDirectoryType

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로 가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시하는 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

Policy

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 하는 사용자에 대한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

PosixProfile

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedAgreement

계약의 속성을 설명합니다.

내용

Arn

계약의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: `arn:\S+`

필수 여부: 예

AccessRole

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출 `StartFileTransfer` 하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2 수 있습니다 `SendFilePaths`. 파일의 상위 디렉터리(예: 의 경우 `--send-file-paths /bucket/dir/file.txt` 상위 디렉터리는 `/bucket/dir/`)를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 `AccessRole` 은(는) `StartFileTransfer` 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 `StartFileTransfer` 와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 `secretsmanager:GetSecretValue` 권한이 필요합니다. Secrets Manager의 AWS 관리형 키 대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 `kms:Decrypt` 권한이 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 secretsmanager:GetSecretValue 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

필수 여부: 아니요

AgreementId

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: a-([0-9a-f]{17})

Required: No

BaseDirectory

AS2 프로토콜을 사용하여 전송되는 파일의 랜딩 디렉터리(폴더)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

필수 여부: 아니요

Description

계약을 식별하는 데 사용되는 명칭 또는 간단한 설명입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: [\p{Graph}]+

Required: No

LocalProfileId

AS2 로컬 프로필의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

필수 여부: 아니요

PartnerProfileId

계약에 사용되는 파트너 프로필의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

필수 여부: 아니요

ServerId

서버 인스턴스에 대해 시스템에서 할당한 고유 식별자입니다. 이 식별자는 계약에서 사용하는 특정 서버를 나타냅니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

필수 여부: 아니요

Status

계약의 현재 상태는 ACTIVE 또는 INACTIVE입니다.

타입: 문자열

유효 값: ACTIVE | INACTIVE

필수 여부: 아니요

Tags

계약을 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedCertificate

인증서의 속성을 설명합니다.

내용

Arn

인증서의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: `arn:\S+`

필수 여부: 예

ActiveDate

인증서가 활성화되는 시기를 지정하는 선택적 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Certificate

인증서의 파일 명칭입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 16384입니다.

패턴: `[\u0009\u000A\u000D\u0020-\u00FF]*`

필수 여부: 아니요

CertificateChain

인증서의 체인을 구성하는 인증서의 목록입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 2097152입니다.

패턴: [\u0009\u000A\u000D\u0020-\u00FF]*

필수 여부: 아니요

CertificateId

가져온 인증서의 식별자 배열입니다. 프로필 및 파트너 프로필 작업에 이 식별자를 사용합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

필수 여부: 아니요

Description

인증서를 식별하는 데 사용되는 명칭 또는 설명입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: [\p{Graph}]+

필수 여부: 아니요

InactiveDate

인증서가 비활성화되는 시기를 지정하는 선택적 날짜.

타입: Timestamp

필수 여부: 아니요

NotAfterDate

인증서가 유효한 최종 날짜입니다.

타입: Timestamp

필수 여부: 아니요

NotBeforeDate

인증서가 유효한 가장 이른 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Serial

인증서의 일련 번호입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 48입니다.

패턴: `[\p{XDigit}{2}:?]*`

필수 여부: 아니요

Status

인증서는 ACTIVE, PENDING_ROTATION 또는 INACTIVE일 수 있습니다. PENDING_ROTATION은 (는) 이 인증서가 만료되면 현재 인증서를 대체함을 의미합니다.

타입: 문자열

유효 값: ACTIVE | PENDING_ROTATION | INACTIVE

필수 여부: 아니요

Tags

인증서를 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Type

인증서에 대해 프라이빗 키가 지정된 경우 해당 타입은 CERTIFICATE_WITH_PRIVATE_KEY입니다. 프라이빗 키가 없는 경우 타입은 CERTIFICATE입니다.

타입: 문자열

유효 값: CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

필수 여부: 아니요

Usage

이 인증서가 서명 또는 암호화에 사용되는지를 지정합니다.

타입: 문자열

유효 값: SIGNING | ENCRYPTION

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedConnector

ConnectorId(으)로 식별되는 커넥터의 파라미터를 설명합니다.

내용

Arn

커넥터의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

AccessRole

커넥터는 AS2 또는 SFTP 프로토콜을 사용하여 파일을 전송하는 데 사용됩니다. 액세스 역할에 사용할 AWS Identity and Access Management 역할의 Amazon 리소스 이름(ARN)을 입력합니다.

AS2 커넥터의 경우

를 사용하면 를 호출StartFileTransfer하고 요청 파라미터 에서 파일 경로를 지정하여 파일을 보낼 AS2수 있습니다SendFilePaths. 파일의 상위 디렉터리(예: 의 경우 --send-file-paths /bucket/dir/file.txt상위 디렉터리는 /bucket/dir/)를 사용하여 처리된 AS2 메시지 파일을 임시로 저장하고, 파트너로부터 받을 MDN 때 를 저장하고, 전송의 관련 메타데이터가 포함된 최종 JSON 파일을 작성합니다. 따라서 AccessRole은(는) StartFileTransfer 요청에 사용된 파일 위치의 상위 디렉터리에 대한 읽기 및 쓰기 액세스를 제공해야 합니다. 또한 StartFileTransfer와(과) 함께 전송하려는 파일의 상위 디렉터리에 대한 읽기 및 쓰기 액세스 권한을 제공해야 합니다.

AS2 커넥터에 기본 인증을 사용하는 경우 액세스 역할에 보안 암호에 대한 secretsmanager:GetSecretValue 권한이 필요합니다. Secrets Manager의 AWS 관리형 키 대신 고객 관리형 키를 사용하여 보안 암호를 암호화하면 역할에도 해당 키에 대한 kms:Decrypt 권한도 필요합니다.

SFTP 커넥터의 경우

액세스 역할이 StartFileTransfer 요청에서 사용된 파일 위치의 상위 디렉터리
에 대한 읽기 및 쓰기 액세스 권한을 제공하는지 확인하세요. 또한 역할이 에 대한
secretsmanager:GetSecretValue 권한을 제공하는지 확인합니다 AWS Secrets Manager.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

As2Config

AS2 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [As2ConnectorConfig](#) 객체

필수 여부: 아니요

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: c-([0-9a-f]{17})

Required: No

LoggingRole

커넥터가 Amazon S3 이벤트에 대한 CloudWatch 로깅을 켤 수 있도록 허용하는 (ARN) 역할의
Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. Amazon S3 설정하면
CloudWatch 로그에서 커넥터 활동을 볼 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

ServiceManagedEgressIpAddresses

이 커넥터의 발신 IP 주소 목록입니다. 이러한 IP 주소는 커넥터를 생성할 때 자동으로 할당됩니다.

타입: 문자열 배열

패턴: \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

Required: No

SftpConfig

SFTP 커넥터 객체의 파라미터를 포함하는 구조입니다.

유형: [SftpConnectorConfig](#) 객체

필수 여부: 아니요

Tags

커넥터를 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Url

파트너 AS2 또는 SFTP 엔드포인트URL의 .

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)

- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedExecution

실행 객체에 대한 세부 정보입니다.

내용

ExecutionId

워크플로 실행의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 36입니다.

패턴: `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Required: No

ExecutionRole

실행과 연결된 IAM 역할입니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

Required: No

InitialFileLocation

Amazon S3 또는 EFS 파일 위치를 설명하는 구조입니다. 실행이 시작될 때의 파일 위치입니다. 파일이 복사되는 경우 이 위치는 대상이 아닌 초기 파일 위치입니다.

타입: [FileLocation](#) 객체

필수 여부: 아니요

LoggingConfiguration

실행과 연결된 IAM 로깅 역할입니다.

유형: [LoggingConfiguration](#) 객체

필수 여부: 아니요

PosixProfile

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹 IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

Results

실행 결과를 설명하는 구조입니다. 여기에는 각 단계의 세부 정보, 오류 타입 및 메시지(있는 경우), OnExceptionSteps 구조와 함께 단계 목록이 포함됩니다.

타입: [ExecutionResults](#) 객체

필수 여부: 아니요

ServiceMetadata

워크플로와 관련된 세션 세부 정보를 위한 컨테이너 객체입니다.

타입: [ServiceMetadata](#) 객체

필수 여부: 아니요

Status

상태는 실행 중 하나입니다. 진행 중이거나, 완료되었거나, 예외가 발생했거나, 예외를 처리 중일 수 있습니다.

타입: 문자열

유효 값: IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedHostKey

서버 호스트 키에 대한 세부 정보입니다.

내용

Arn

호스트 키의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

DateImported

호스트 키가 서버에 추가된 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Description

이 호스트 키에 대한 텍스트 설명입니다.

타입: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: [\p{Print}]*

Required: No

HostKeyFingerprint

퍼블릭 키 핑거프린트는 더 긴 퍼블릭 키를 식별하는 데 사용되는 짧은 시퀀스의 바이트입니다.

타입: 문자열

필수 항목 여부: 아니요

HostKeyId

호스트 키의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

패턴: hostkey-[0-9a-f]{17}

Required: No

Tags

그룹화 및 호스트 키 검색에 사용될 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Type

호스트 키에 사용되는 암호화 알고리즘입니다. Type 파라미터는 다음 값 중 하나를 사용하여 지정합니다.

- ssh-rsa
- ssh-ed25519
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)

- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedProfile

로컬 또는 파트너 AS2 프로파일의 세부 정보입니다.

내용

Arn

프로파일의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: `arn:\S+`

필수 여부: 예

As2Id

As2Id 는 4130에 정의된 AS2-name입니다. [RFC](#) 인바운드 전송의 경우 파트너에서 보낸 AS2 메시지의 AS2-From 헤더입니다. 아웃바운드 커넥터의 경우 작업을 사용하여 파트너에게 전송되는 AS2 메시지의 AS2-To 헤더입니다. 이 ID는 공백을 포함할 수 없습니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

패턴: `[\p{Print}\s]*`

필수 여부: 아니요

CertificateIds

가져온 인증서의 식별자 배열입니다. 프로파일 및 파트너 프로파일 작업에 이 식별자를 사용합니다.

타입: 문자열 배열

길이 제약 조건: 고정 길이는 22입니다.

패턴: `cert-([0-9a-f]{17})`

Required: No

ProfileId

로컬 또는 파트너 AS2 프로파일의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Required: No

ProfileType

LOCAL 타입 프로파일만 나열할지 아니면 PARTNER 타입 프로파일만 나열할지를 나타냅니다. 요청에 입력되지 않은 경우 명령은 모든 타입의 프로 파일을 나열합니다.

타입: 문자열

유효 값: LOCAL | PARTNER

필수 여부: 아니요

Tags

프로 파일을 그룹화하고 검색하는 데 사용할 수 있는 키-값 쌍입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedSecurityPolicy

지정된 보안 정책의 속성을 설명합니다. 보안 정책에 대한 자세한 내용은 [보안 정책을 사용하는 작업을 참조](#)하세요.

내용

SecurityPolicyName

서버에 연결된 보안 정책의 명칭을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

Pattern: TransferSecurityPolicy-.+

필수 여부: 예

Fips

이 정책이 연방 정보 처리 표준(FIPS)을 활성화할지 여부를 지정합니다.

타입: 부울

필수 항목 여부: 아니요

SshCiphers

서버에 연결된 보안 정책에서 활성화된 Secure Shell(SSH) 암호 암호화 알고리즘을 지정합니다.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 50입니다.

필수 여부: 아니요

SshKexs

서버에 연결된 보안 정책에서 활성화된 SSH 키 교환(KEX) 암호화 알고리즘을 지정합니다.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 50입니다.

필수 여부: 아니요

SshMacs

서버에 연결된 보안 정책에서 활성화된 SSH 메시지 인증 코드(MAC) 암호화 알고리즘을 지정합니다.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 50입니다.

필수 여부: 아니요

TlsCiphers

서버에 연결된 보안 정책에서 활성화된 전송 계층 보안(TLS) 암호 암호화 알고리즘을 지정합니다.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 50입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedServer

지정된 File Transfer 프로토콜 지원 서버의 속성을 설명합니다.

내용

Arn

서버의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

As2ServiceManagedEgressIpAddresses

이 서버의 발신 IP 주소 목록입니다. 이러한 IP 주소는 AS2 프로토콜을 사용하는 서버와만 관련이 있습니다. 비동기 를 보내는 데 사용됩니다MDNs.

이러한 IP 주소는 AS2 서버를 생성할 때 자동으로 할당됩니다. 또한 기존 서버를 업데이트하고 AS2 프로토콜을 추가하면 정적 IP 주소도 할당됩니다.

타입: 문자열 배열

패턴: \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

Required: No

Certificate

AWS Certificate Manager(ACM) 인증서ARN의 를 지정합니다. Protocols이(가) FTPS(으)로 설정된 경우에 필요합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1600입니다.

필수 여부: 아니요

Domain

File Transfer에 사용되는 스토리지 시스템의 도메인을 지정합니다.

타입: 문자열

유효 값: S3 | EFS

필수 여부: 아니요

EndpointDetails

서버에 대해 구성된 가상 프라이빗 클라우드(VPC) 엔드포인트 설정입니다. 내에서 엔드포인트를 호스팅할 때 엔드포인트를 내 리소스에만 액세스하도록 하거나 VPC탄력적 IP 주소를 연결하고 인터넷을 통해 클라이언트가 엔드포인트에 액세스할 VPC수 있도록 할 수 있습니다. VPC의 기본 보안 그룹은 엔드포인트에 자동으로 할당됩니다.

유형: [EndpointDetails](#) 객체

필수 여부: 아니요

EndpointType

서버가 연결된 엔드포인트의 타입을 정의합니다. 서버가 VPC 엔드포인트에 연결된 경우 퍼블릭 인터넷을 통해 서버에 액세스할 수 없습니다.

타입: 문자열

유효 값: PUBLIC | VPC | VPC_ENDPOINT

필수 여부: 아니요

HostKeyFingerprint

서버 호스트 키의 Base64-encoded SHA256 지문을 지정합니다. 이 값은 `ssh-keygen -l -f my-new-server-key` 명령의 출력과 동등합니다.

타입: 문자열

필수 항목 여부: 아니요

IdentityProviderDetails

고객 제공 인증을 호출하는 정보를 지정합니다API. 서버의 `IdentityProviderType`이 `AWS_DIRECTORY_SERVICE`이거나 또는 `SERVICE_MANAGED`인 경우, 이 필드는 채워지지 않습니다.

타입: [IdentityProviderDetails](#) 객체

필수 여부: 아니요

IdentityProviderType

서버 인증 모드. 기본값은 `SERVICE_MANAGED`, 이를 통해 AWS Transfer Family 서비스 내에서 사용자 자격 증명을 저장하고 액세스할 수 있습니다.

`AWS_DIRECTORY_SERVICE` 를 사용하여 온프레미스 환경에서 AWS Directory Service for Microsoft Active Directory 또는 Microsoft Active Directory의 Active Directory 그룹에 대한 액세스를 제공하거나 AD Connector를 AWS 사용합니다. 또한 이 옵션을 사용하려면 `IdentityProviderDetails` 파라미터를 사용하여 디렉터리 ID를 제공해야 합니다.

`API_GATEWAY` 값을 사용하여 선택하는 자격 증명 제공자와 통합합니다. 이 `API_GATEWAY` 설정을 수행하려면 `IdentityProviderDetails` 파라미터를 사용하여 인증을 호출URL할 Amazon API Gateway 엔드포인트를 제공해야 합니다.

`AWS_LAMBDA` 값을 사용하여 AWS Lambda 함수를 자격 증명 공급자로 직접 사용합니다. 이 값을 선택하는 경우 `IdentityProviderDetails` 데이터 유형의 `Function` 파라미터에 ARN Lambda 함수에 대해 를 지정해야 합니다.

타입: 문자열

유효 값: `SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

필수 여부: 아니요

LoggingRole

서버가 Amazon S3 또는 Amazon 에 대한 Amazon CloudWatch 로깅을 켤 수 있도록 허용하는 () 역할ARN의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다EFSevents. 설정하면 CloudWatch 로그에서 사용자 활동을 볼 수 있습니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2,048.

패턴: `(|arn:.*role/\S+)`

필수 여부: 아니요

PostAuthenticationLoginBanner

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증한 후에 표시됩니다.

Note

SFTP 프로토콜은 인증 후 표시 배너를 지원하지 않습니다.

유형: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: `[\x09-\x0D\x20-\x7E]*`

필수 여부: 아니요

PreAuthenticationLoginBanner

사용자가 서버에 연결할 때 표시할 문자열을 지정합니다. 이 문자열은 사용자가 인증하기 전에 표시됩니다. 예를 들어 다음 배너는 시스템 사용에 대한 세부 정보를 표시합니다.

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

타입: 문자열

길이 제약: 최소 길이는 0입니다. 최대 길이는 4096자입니다.

패턴: `[\x09-\x0D\x20-\x7E]*`

필수 여부: 아니요

ProtocolDetails

서버에 대해 구성된 프로토콜 설정입니다.

- 패시브 모드(FTP 및 FTPS 프로토콜용)를 표시하려면 `PassiveIp` 파라미터를 사용합니다. 방화벽, 라우터 또는 로드 밸런서의 외부 IP IPv4 주소와 같은 단일 점 쿼드 주소를 입력합니다.
- Amazon S3 버킷에 업로드하는 파일에 대해 클라이언트가 `SETSTAT` 명령을 사용하려 할 때 생성되는 오류를 무시하려면 `SetStatOption` 파라미터를 사용합니다. AWS Transfer Family 서버가 SFTP 클라이언트를 변경할 필요 없이 `SETSTAT` 명령을 무시하고 파일을 업로드하도록 하려면 값을 `ENABLE_NO_OP`로 설정합니다. `SetStatOption` 파라미터를 `ENABLE_NO_OP`로 설정하면 Transfer Family가 Amazon CloudWatch Logs에 로그 항목을 생성하여 클라이언트가 `SETSTAT` 전화를 거는 시기를 확인할 수 있습니다.

- AWS Transfer Family 서버가 고유한 세션 ID를 통해 최근 협상된 세션을 재개하는지 확인하려면 `TlsSessionResumptionMode` 파라미터를 사용합니다.
- `As2Transports` 는 AS2 메시지의 전송 방법을 나타냅니다. 현재 HTTP만 지원됩니다.

유형: [ProtocolDetails](#) 객체

필수 여부: 아니요

Protocols

파일 전송 프로토콜 클라이언트가 서버의 엔드포인트에 연결할 수 있는 파일 전송 프로토콜을 지정합니다. 사용 가능한 프로토콜은 다음과 같습니다:

- SFTP (Secure Shell (SSH) 파일 전송 프로토콜): 파일 전송 SSH
- FTPS (파일 전송 프로토콜 보안): TLS 암호화를 사용한 파일 전송
- FTP (File Transfer Protocol): 암호화되지 않은 파일 전송
- AS2 (적용 설명 2): 구조화된 business-to-business 데이터 전송에 사용

Note

- 를 선택하는 경우 클라이언트가 를 통해 서버를 연결할 때 서버를 식별하는 데 사용되는 AWS Certificate Manager (ACM)에 저장된 인증서를 선택해야 FTPS합니다FTPS.
- Protocol에 FTP 또는 FTPS이(가) 포함된 경우 EndpointType은(는) VPC이고 IdentityProviderType은(는) AWS_DIRECTORY_SERVICE, AWS_LAMBDA 또는 API_GATEWAY여야 합니다.
- Protocol에 FTP이(가) 포함된 경우 AddressAllocationIds를 연결할 수 없습니다.
- Protocol이 SFTP로만 설정된 경우 EndpointType을 PUBLIC으로 설정하고 IdentityProviderType을 지원되는 ID 타입(SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA, API_GATEWAY) 중 하나로 설정할 수 있습니다.
- Protocol에 AS2이(가) 포함된 경우 EndpointType은(는) VPC여야 하고, 도메인은 Amazon S3여야 합니다.

타입: 문자열 배열

배열 구성원: 최소수는 1개입니다. 최대 항목 수는 4개입니다.

유효 값: SFTP | FTP | FTPS | AS2

필수 여부: 아니요

S3StorageOptions

Amazon S3 디렉터리의 성능 최적화 여부를 지정합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

기본적으로 홈 디렉터리 매핑의 는 TYPE입니다DIRECTOR. 이 옵션을 활성화하면 매핑에 파일 대상이 포함되도록 HomeDirectoryMapEntry Type FILE 하려면 를 로 명시적으로 설정해야 합니다.

유형: [S3StorageOptions](#) 객체

필수 여부: 아니요

SecurityPolicyName

서버에 연결된 보안 정책의 명칭을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 100입니다.

패턴: TransferSecurityPolicy-.*

Required: No

ServerId

인스턴스화하는 서버의 고유한 시스템 할당 식별자를 지정합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Required: No

State

설명된 서버의 상태입니다. 값이 ONLINE 이면 서버가 작업을 수락하고 파일을 전송할 수 있음을 나타냅니다. State값이 OFFLINE(이)면 서버에서 File Transfer 작업을 수행할 수 없습니다.

STARTING 및 STOPPING 상태는 서버가 완전히 응답할 수 없거나 완전히 오프라인 상태가 아닌 중간 상태임을 나타냅니다. START_FAILED 또는 STOP_FAILED의 값은 오류 상태를 나타낼 수 있습니다.

타입: 문자열

유효 값: OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

필수 여부: 아니요

StructuredLogDestinations

사용자의 서버 로그가 전송될 로그 그룹을 지정합니다.

로그 그룹을 지정하려면 기존 로그 그룹에 ARN 대해 를 제공해야 합니다. 이 경우, 로그 그룹의 형식은 다음과 같습니다:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

예제: `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

이전에 서버의 로그 그룹을 지정한 경우, `update-server` 호출 시 이 파라미터에 빈 값을 제공하여 로그 그룹을 지우고 사실상 구조화된 로깅을 끌 수 있습니다. 예:

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

타입: 문자열 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 1개입니다.

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: `arn:\S+`

Required: No

Tags

설명된 서버에 할당된 서버를 검색하고 그룹화하는 데 사용할 수 있는 키-값 쌍을 지정합니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

UserCount

ServerId를 사용하여 지정한 서버에 할당되는 사용자 수를 지정합니다.

타입: 정수

필수 항목 여부: 아니요

WorkflowDetails

할당할 워크플로의 워크플로 ID와 워크플로 실행에 사용되는 실행 역할을 지정합니다.

파일이 완전히 업로드될 때 실행되는 워크플로 외에도 WorkflowDetails에는 부분 업로드 시 실행할 워크플로의 워크플로 ID와 실행 역할이 포함될 수 있습니다. 파일이 업로드되는 동안 서버 세션 연결이 끊기면 부분 업로드가 수행됩니다.

타입: [WorkflowDetails](#) 객체

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedUser

지정된 사용자의 속성을 설명합니다.

내용

Arn

설명하도록 요청된 사용자의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

HomeDirectory

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

HomeDirectoryMappings

사용자에게 표시해야 하는 Amazon S3 또는 Amazon EFS 경로와 키를 지정하는 논리적 디렉터리 매핑과 이를 표시할 방법을 지정합니다. Entry 및 Target 페어를 지정해야 합니다. 여기서 는 경로가 Entry 어떻게 표시되는지, Target 는 실제 Amazon S3 또는 Amazon EFS 경로입니다. 대 상만 지정하는 경우, 그대로 표시됩니다. 또한 AWS Identity and Access Management (IAM) 역할

이 경로에 대한 액세스를 제공해야 합니다. 이 값은 이 로 설정된 경우에만 `HomeDirectoryType` 설정할 수 있습니다. `LOGICAL`.

대부분의 경우, 세션 정책 대신 이 값을 사용하여 사용자를 지정된 홈 디렉터리("chroot")로 제한할 수 있습니다. 이렇게 하려면 `"/Entry`로 설정하고 파라미터 값으로 설정할 수 `Target` 있습니다 `HomeDirectory`.

유형: [HomeDirectoryMapEntry](#) 객체 어레이

어레이 멤버: 최소 항목 수 1개. 최대 항목 수는 50,000개입니다.

필수 여부: 아니요

HomeDirectoryType

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 `PATH` 파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 `HomeDirectoryMappings` 대한 매핑을 에 `LOGICAL` 제공해야 합니다.

Note

`HomeDirectoryType`이 `LOGICAL`인 경우, `HomeDirectoryMappings` 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 `HomeDirectoryType`이 `PATH`인 경우, `HomeDirectory` 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 `HomeDirectory` 및 `HomeDirectoryMappings`를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: `PATH` | `LOGICAL`

필수 여부: 아니요

Policy

여러 사용자 간에 동일한 AWS Identity and Access Management (IAM) 역할을 사용할 수 있도록 사용자를 위한 세션 정책입니다. 이 정책은 Amazon S3 버킷의 부분에 대한 사용자의 액세스 범위를 축소합니다. 이 정책 내에서 사용할 수 있는 변수는 `${Transfer:UserName}`, `${Transfer:HomeDirectory}` 및 `${Transfer:HomeBucket}`입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 아니요

PosixProfile

Amazon Elastic File System(AmazonEFS) 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(IDs(Uid), 그룹 ID(SecondaryGids) 및 보조 그룹(EFS)을 비롯한 전체 POSIX 자격 증명을 지정합니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

유형: [PosixProfile](#) 객체

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

Required: No

SshPublicKeys

설명된 사용자에게 대해 저장된 Secure Shell(SSH) 키의 퍼블릭 키 부분을 지정합니다.

유형: [SshPublicKey](#) 객체 어레이

배열 멤버: 최소 항목 수 0개. 최대 항목 수 5개.

필수 여부: 아니요

Tags

요청된 사용자의 카-값 쌍을 지정합니다. 태그를 사용하여 다양한 목적으로 사용자를 검색하고 그룹화할 수 있습니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

UserName

설명이 요청된 사용자의 명칭을 지정합니다. 사용자 이름은 인증 목적으로 사용됩니다. 사용자가 서버에 로그인할 때 사용하는 문자열입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

패턴: `[\w][\w@.-]{2,99}`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

DescribedWorkflow

지정된 워크플로에 저장된 속성을 설명합니다.

내용

Arn

워크플로의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: `arn:\S+`

필수 여부: 예

Description

워크플로에 대한 텍스트 설명을 지정합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `[\w- ]*`

Required: No

OnExceptionSteps

워크플로를 실행하는 동안 오류가 발생할 경우 수행할 단계(작업)를 지정합니다.

타입: [WorkflowStep](#) 객체 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 8개입니다.

필수 여부: 아니요

Steps

지정된 워크플로에 있는 단계에 대한 세부 정보를 지정합니다.

타입: [WorkflowStep](#) 객체 배열

배열 멤버: 최소 항목 수는 0개입니다. 최대 항목 수는 8개입니다.

필수 여부: 아니요

Tags

워크플로 그룹화 및 검색에 사용될 수 있는 키-값 쌍입니다. 태그는 어떠한 목적으로 워크플로에 연결되는 메타데이터입니다.

타입: [Tag](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: w-([a-z0-9]{17})

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

EfsFileLocation

워크플로에서 사용 중인 파일의 파일 위치에 대한 세부 정보를 지정합니다. Amazon Elastic File Systems(Amazon EFS)를 스토리지로 사용하는 경우에만 적용됩니다.

내용

FileSystemId

Amazon 에서 할당한 파일 시스템의 식별자입니다EFS.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 128입니다.

패턴: (arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})

Required: No

Path

워크플로에서 사용 중인 폴더의 경로 이름.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 65536입니다.

패턴: [^\x00]+

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

EndpointDetails

파일 전송 프로토콜 지원 서버에 대해 구성된 가상 프라이빗 클라우드(VPC) 엔드포인트 설정입니다. VPC 엔드포인트를 사용하면 내에서만 서버 및 리소스에 대한 액세스를 제한할 수 있습니다. 들어오는 인터넷 트래픽을 제어하려면 `UpdateServerAPI` 호출로 탄력적 IP 주소를 서버의 엔드포인트에 연결합니다.

Note

2021년 5월 19일 이후에는 2021년 5월 19일 이전에 AWS계정이 아직 생성되지 않은 경우 계정 `EndpointType=VPC_ENDPOINT`에서 `를 사용하여 서버를 생성할 수 없습니다. 2021년 5월 19일 또는 그 이전에 EndpointType=VPC_ENDPOINT AWS계정에 가 있는 서버를 이미 생성한 경우 영향을 받지 않습니다. 이 날짜 이후에는 EndpointType=VPC를 사용하세요. 자세한 내용은 VPC\_ 사용 중단ENDPOINT를 참조하세요.`

내용

AddressAllocationIds

탄력적 IP 주소를 서버의 엔드포인트에 연결하는 데 IDs 필요한 주소 할당 목록입니다.

주소 할당 ID는 탄력적 IP 주소의 할당 ID에 해당합니다. 이 값은 Amazon EC2 [주소](#) 데이터 유형의 `allocationId` 필드에서 검색할 수 있습니다. 이 값을 검색하는 한 가지 방법은 EC2 [DescribeAddresses](#)를 호출하는 것입니다.

이 파라미터는 선택 사항입니다. VPC 엔드포인트를 퍼블릭 대면으로 만들려면 이 파라미터를 설정합니다. 자세한 내용은 [서버의 인터넷 연결 엔드포인트 생성을 참조하세요](#).

Note

이 속성은 다음과 같이만 설정할 수 있습니다.

- `EndpointType`를 `로 설정해야 합니다. VPC`
- Transfer Family 서버는 오프라인 상태여야 합니다.
- FTP 프로토콜을 사용하는 Transfer Family 서버에는 이 파라미터를 설정할 수 없습니다.
- 서버가 이미 채워져 있어야 합니다(`SubnetIds` 및 `SubnetIds`는 동시에 업데이트할 수 없음).

- AddressAllocationIds에는 중복이 포함될 수 없으며 길이는 와 같아야 합니다SubnetIds. 예를 들어 서브넷이 3개인 경우 주소 할당 3개도 지정IDs해야 합니다IDs.
- 를 호출UpdateServerAPI하여 이 파라미터를 설정하거나 변경합니다.

유형: String 배열

필수 여부: 아니요

SecurityGroupIds

서버의 엔드포인트에 연결할 수 IDs 있는 보안 그룹 목록입니다.

Note

이 속성은 EndpointType이(가) VPC(으)로 설정된 경우에만 사용할 수 있습니다. EndpointType PUBLIC 또는 에서 로 변경하는 [UpdateServer](#) API 경우에만 에서 SecurityGroupIds 속성을 편집할 수 VPC_ENDPOINT 있습니다VPC. 생성 후 서버의 VPC 엔드포인트와 연결된 보안 그룹을 변경하려면 Amazon EC2 [ModifyVpcEndpoint](#) 를 사용합니다API.

타입: 문자열 배열

길이 제약 조건: 최소 길이는 11입니다. 최대 길이는 20입니다.

패턴: sg-[0-9a-f]{8,17}

Required: No

SubnetIds

에서 서버 엔드포인트를 호스팅IDs하는 데 필요한 서브넷 목록입니다VPC.

Note

이 속성은 EndpointType이(가) VPC(으)로 설정된 경우에만 사용할 수 있습니다.

타입: 문자열 배열

필수 여부: 아니요

VpcEndpointId

VPC 엔드포인트의 식별자입니다.

Note

이 속성은 EndpointType이(가) VPC_ENDPOINT(으)로 설정된 경우에만 사용할 수 있습니다.

자세한 내용은 [VPC_사용 중단ENDPOINT](#)를 참조하세요.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

패턴: vpce-[0-9a-f]{17}

Required: No

VpcId

서버의 엔드포인트가 호스팅될 VPC 의 VPC 식별자입니다.

Note

이 속성은 EndpointType이(가) VPC(으)로 설정된 경우에만 사용할 수 있습니다.

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK Ruby V3용](#)

ExecutionError

워크플로 실행 중에 발생하는 오류에 대한 오류 메시지와 타입을 지정합니다.

내용

Message

ErrorType에 해당하는 설명 메시지를 지정합니다.

타입: 문자열

필수 항목 여부: 예

Type

오류 타입을 지정합니다.

- **ALREADY_EXISTS**: 덮어쓰기 옵션을 선택하지 않고 대상 위치에 같은 이름의 파일이 이미 있는 경우 복사 단계에서 발생합니다.
- **BAD_REQUEST**: 일반적인 잘못된 요청: 예를 들어 S3 EFS 파일만 태그 지정될 수 **BAD_REQUEST**있으므로 파일에 태그를 지정하려고 시도하는 단계는 를 반환합니다.
- **CUSTOM_STEP_FAILED**: 사용자 지정 단계에서 실패를 나타내는 콜백을 제공한 경우 발생합니다.
- **INTERNAL_SERVER_ERROR**: 다양한 이유로 발생할 수 있는 포괄적인 오류입니다.
- **NOT_FOUND**: 요청된 개체(예: 복사 단계의 소스 파일)가 존재하지 않을 때 발생합니다.
- **PERMISSION_DENIED**: 워크플로에서 하나 이상의 단계를 완료할 수 있는 올바른 권한이 정책에 포함되어 있지 않은 경우 발생합니다.
- **TIMEOUT**: 실행 시간이 초과되면 발생합니다.

Note

사용자 지정 단계에 대해 TimeoutSeconds을 1초에서 1800(30분) 사이로 설정할 수 있습니다.

- **THROTTLED**: 초당 한 워크플로의 새 실행 리필 비율을 초과할 경우 발생합니다.

타입: 문자열

유효 값: PERMISSION_DENIED | CUSTOM_STEP_FAILED | THROTTLED
| ALREADY_EXISTS | NOT_FOUND | BAD_REQUEST | TIMEOUT |
INTERNAL_SERVER_ERROR

필수 여부: 예

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ExecutionResults

워크플로의 단계와 워크플로 실행 중 오류가 발생할 경우 실행할 단계를 지정합니다.

내용

OnExceptionSteps

워크플로를 실행하는 동안 오류가 발생할 경우 수행할 단계(작업)를 지정합니다.

타입: [ExecutionStepResult](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

Steps

지정된 워크플로에 있는 단계에 대한 세부 정보를 지정합니다.

타입: [ExecutionStepResult](#) 객체 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 50개입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ExecutionStepResult

단계에 대해 오류(있는 경우), 출력(있는 경우), 단계 타입 등의 세부 정보를 지정합니다.

내용

Error

지정된 워크플로 단계를 실행하는 동안 오류가 발생한 경우 해당 오류의 세부 정보를 지정합니다.

타입: [ExecutionError](#) 객체

필수 여부: 아니요

Outputs

키/값 쌍의 값이 파일에 태그로 적용되었습니다. 단계 타입이 TAG인 경우에만 적용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 65536입니다.

필수 여부: 아니요

StepType

사용 가능한 단계 타입 중 하나입니다.

- **COPY** - 다른 위치에 파일을 복사합니다.
- **CUSTOM** - AWS Lambda 함수 대상으로 사용자 지정 단계를 수행합니다.
- **DECRYPT** - 업로드되기 전에 암호화된 파일을 복호화합니다.
- **DELETE** - 파일을 삭제합니다.
- **TAG** - 파일에 태그를 추가합니다.

타입: 문자열

유효 값: COPY | CUSTOM | TAG | DELETE | DECRYPT

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

FileLocation

단계에서 사용할 Amazon S3 또는 EFS 파일 세부 정보를 지정합니다.

내용

EfsFileLocation

Amazon EFS 식별자와 사용 중인 파일의 경로를 지정합니다.

유형: [EfsFileLocation](#) 객체

필수 여부: 아니요

S3FileLocation

버킷, ETag 등 사용 중인 파일의 S3 세부 정보를 지정합니다.

유형: [S3FileLocation](#) 객체

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

HomeDirectoryMapEntry

HomeDirectoryMappings을 위한 항목과 대상을 포함하는 객체를 나타냅니다.

다음은 chroot에 대한 Entry 및 Target 쌍의 예입니다.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

내용

Entry

HomeDirectoryMappings에 대한 항목을 나타냅니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

Pattern: /. *

필수 여부: 예

Target

HomeDirectoryMapEntry에서 사용되는 맵 대상을 나타냅니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

Pattern: /. *

필수 여부: 예

Type

매핑 유형을 지정합니다. 매핑이 파일을 가리키도록 FILE하려면 유형을 로 설정하고 디렉터리 DIRECTORY가 디렉터리를 가리키도록 하려면 유형을 로 설정합니다.

Note

기본적으로 Transfer Family 서버를 생성할 Type DIRECTORY 때 홈 디렉터리 매핑의 는 입니다. 매핑에 파일 대상이 포함되도록 FILE 하려면 명시적으로 를 Type 로 설정해야 합니다.

타입: 문자열

유효 값: FILE | DIRECTORY

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

IdentityProviderDetails

파일 전송 프로토콜을 사용하는 서버의 사용자에게 사용되는 사용자 인증 타입과 관련된 정보를 반환합니다. 서버는 인증 메서드로 하나만 사용할 수 있습니다.

내용

DirectoryId

자격 증명 공급자로 사용할 AWS Directory Service 디렉터리의 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 12입니다.

패턴: d-[0-9a-f]{10}

Required: No

Function

Lambda 함수ARN가 자격 증명 공급자에 사용할 용 .

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 170입니다.

패턴: arn:[a-z-]+:lambda:.*

필수 여부: 아니요

InvocationRole

이 파라미터는 IdentityProviderType가 API_GATEWAY인 경우에만 적용됩니다. 사용자 계정을 인증하는 데 사용되는 InvocationRole의 타입을 제공합니다.

타입: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

SftpAuthenticationMethods

SFTP활성화된 서버의 경우 , 사용자 지정 자격 증명 공급자의 경우 만 암호, SSH 키 페어 또는 둘 다를 사용하여 인증할지 여부를 지정할 수 있습니다.

- **PASSWORD** - 연결하려면 사용자가 암호를 입력해야 합니다.
- **PUBLIC_KEY** - 연결하려면 사용자가 프라이빗 키를 제공해야 합니다.
- **PUBLIC_KEY_OR_PASSWORD** - 사용자는 암호나 키로 인증할 수 있습니다. 이것이 기본값입니다.
- **PUBLIC_KEY_AND_PASSWORD** - 연결하려면 사용자가 프라이빗 키와 암호를 모두 제공해야 합니다. 서버가 먼저 키를 확인한 다음 키가 유효하면 암호를 입력하라는 메시지가 표시됩니다. 제공된 프라이빗 키가 저장된 퍼블릭 키와 일치하지 않는 경우 인증이 실패합니다.

타입: 문자열

유효 값: PASSWORD | PUBLIC_KEY | PUBLIC_KEY_OR_PASSWORD |
PUBLIC_KEY_AND_PASSWORD

필수 여부: 아니요

Url

사용자를 인증하는 데 사용되는 서비스 엔드포인트의 위치를 제공합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

InputFileLocation

처리 중인 파일의 위치를 지정합니다.

내용

EfsFileLocation

복호화되는 Amazon Elastic File System(AmazonEFS) 파일의 세부 정보를 지정합니다.

유형: [EfsFileLocation](#) 객체

필수 여부: 아니요

S3FileLocation

복사 또는 복호화 중인 Amazon S3 파일의 세부 정보를 지정합니다.

타입: [S3InputFileLocation](#) 객체

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedAccess

하나 이상의 지정된 관련 액세스의 속성을 나열합니다.

내용

ExternalId

디렉터리 내의 특정 그룹을 식별하는 데 필요한 고유 식별자입니다. 연결하는 그룹의 사용자를 사용하여 활성화된 프로토콜을 통해 Amazon S3 또는 Amazon EFS 리소스에 액세스할 수 있습니다 AWS Transfer Family. 그룹 이름을 알고 있는 경우 Windows 를 사용하여 다음 명령을 실행하여 SID 값을 볼 수 있습니다 PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

이 명령에서 YourGroupName를 Active Directory 그룹의 이름으로 바꿉니다.

이 파라미터를 확인하는 데 사용되는 정규 표현식은 공백 없이 대문자 및 소문자 영숫자로 구성된 문자의 문자열입니다. 밑줄이나 또한 =,./@:/- 문자도 포함할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256입니다.

Pattern: S-1-[\d-]+

필수 여부: 아니요

HomeDirectory

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

HomeDirectoryType

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedAgreement

계약의 속성을 설명합니다.

내용

AgreementId

계약의 고유 식별자입니다. 계약을 생성하면 이 식별자가 반환됩니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: a-([0-9a-f]{17})

Required: No

Arn

지정된 계약의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

Required: No

Description

계약에 대한 현재 설명입니다. UpdateAgreement 작업을 직접적으로 호출하고 새 설명을 제공하여 변경할 수 있습니다.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: [\p{Graph}]+

Required: No

LocalProfileId

AS2 로컬 프로필의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

필수 여부: 아니요

PartnerProfileId

파트너 프로필의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Required: No

ServerId

계약의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Required: No

Status

계약은 ACTIVE 또는 INACTIVE 둘 중 하나일 수 있습니다.

타입: 문자열

유효 값: ACTIVE | INACTIVE

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedCertificate

인증서의 속성을 설명합니다.

내용

ActiveDate

인증서가 활성화되는 시기를 지정하는 선택적 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Arn

지정된 인증서의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

필수 여부: 아니요

CertificateId

가져온 인증서의 식별자 배열입니다. 프로필 및 파트너 프로필 작업에 이 식별자를 사용합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 22입니다.

패턴: cert-([0-9a-f]{17})

Required: No

Description

인증서를 식별하는 데 사용되는 이름 또는 간단한 설명.

타입: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 200입니다.

패턴: `[\p{Graph}]+`

필수 여부: 아니요

InactiveDate

인증서가 비활성화되는 시기를 지정하는 선택적 날짜.

타입: Timestamp

필수 여부: 아니요

Status

인증서는 ACTIVE, PENDING_ROTATION 또는 INACTIVE일 수 있습니다. PENDING_ROTATION은 (는) 이 인증서가 만료되면 현재 인증서를 대체함을 의미합니다.

타입: 문자열

유효 값: ACTIVE | PENDING_ROTATION | INACTIVE

필수 여부: 아니요

Type

인증서의 타입입니다. 인증서에 프라이빗 키가 지정된 경우 해당 타입은 CERTIFICATE_WITH_PRIVATE_KEY입니다. 프라이빗 키가 없는 경우 타입은 CERTIFICATE입니다.

타입: 문자열

유효 값: CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

필수 여부: 아니요

Usage

이 인증서가 서명 또는 암호화에 사용되는지를 지정합니다.

타입: 문자열

유효 값: SIGNING | ENCRYPTION

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedConnector

지정된 커넥터의 세부 정보를 반환합니다.

내용

Arn

지정된 커넥터의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

Required: No

ConnectorId

커넥터의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: c-([0-9a-f]{17})

Required: No

Url

파트너 AS2 또는 SFTP 엔드포인트URL의 .

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 255입니다.

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedExecution

지정된 실행의 속성을 반환합니다.

내용

ExecutionId

워크플로 실행의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 36입니다.

패턴: [0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}

Required: No

InitialFileLocation

Amazon S3 또는 EFS 파일 위치를 설명하는 구조입니다. 실행이 시작될 때의 파일 위치입니다. 파일이 복사되는 경우 이 위치는 대상이 아닌 초기 파일 위치입니다.

타입: [FileLocation](#) 객체

필수 여부: 아니요

ServiceMetadata

워크플로와 관련된 세션 세부 정보를 위한 컨테이너 객체입니다.

타입: [ServiceMetadata](#) 객체

필수 여부: 아니요

Status

상태는 실행 중 하나입니다. 진행 중이거나, 완료되었거나, 예외가 발생했거나, 예외를 처리 중일 수 있습니다.

타입: 문자열

유효 값: IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedHostKey

지정된 호스트 키의 속성을 반환합니다.

내용

Arn

호스트 키의 고유한 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

DateImported

호스트 키가 서버에 추가된 날짜입니다.

타입: Timestamp

필수 여부: 아니요

Description

호스트 키에 대한 현재 설명. UpdateHostKey 작업을 직접적으로 호출하고 새 설명을 제공하여 변경할 수 있습니다.

타입: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 200입니다.

패턴: [\p{Print}]*

Required: No

Fingerprint

퍼블릭 키 핑거프린트는 더 긴 퍼블릭 키를 식별하는 데 사용되는 짧은 시퀀스의 바이트입니다.

타입: 문자열

필수 항목 여부: 아니요

HostKeyId

호스트 키의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 25입니다.

패턴: hostkey-[0-9a-f]{17}

Required: No

Type

호스트 키에 사용되는 암호화 알고리즘입니다. Type 파라미터는 다음 값 중 하나를 사용하여 지정합니다.

- ssh-rsa
- ssh-ed25519
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

타입: 문자열

필수 항목 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedProfile

지정된 프로파일의 속성을 반환합니다.

내용

Arn

지정된 프로파일의 Amazon 리소스 이름(ARN)입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: arn:\S+

Required: No

As2Id

As2Id 는 4130에 정의된 AS2-name입니다. [RFC](#) 인바운드 전송의 경우 파트너에서 보낸 AS2 메시지의 AS2-From 헤더입니다. 아웃바운드 커넥터의 경우 작업을 사용하여 파트너에게 전송되는 AS2 메시지의 AS2-To 헤더입니다. 이 ID는 공백을 포함할 수 없습니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

패턴: [\p{Print}\s]*

Required: No

ProfileId

로컬 또는 파트너 AS2 프로파일의 고유 식별자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: p-([0-9a-f]{17})

Required: No

ProfileType

LOCAL 타입 프로파일만 나열할지 아니면 PARTNER 타입 프로파일만 나열할지를 나타냅니다. 요청에 입력되지 않은 경우 명령은 모든 타입의 프로파일을 나열합니다.

타입: 문자열

유효 값: LOCAL | PARTNER

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedServer

지정된 File Transfer 프로토콜 지원 서버의 속성을 반환합니다.

내용

Arn

나열할 서버의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

Domain

File Transfer에 사용되는 스토리지 시스템의 도메인을 지정합니다.

타입: 문자열

유효 값: S3 | EFS

필수 여부: 아니요

EndpointType

서버가 연결된 VPC 엔드포인트 유형을 지정합니다. 서버가 VPC 엔드포인트에 연결된 경우 퍼블릭 인터넷을 통해 서버에 액세스할 수 없습니다.

타입: 문자열

유효 값: PUBLIC | VPC | VPC_ENDPOINT

필수 여부: 아니요

IdentityProviderType

서버 인증 모드. 기본값은 이며SERVICE_MANAGED, 이를 통해 AWS Transfer Family 서비스 내에서 사용자 자격 증명을 저장하고 액세스할 수 있습니다.

AWS_DIRECTORY_SERVICE 를 사용하여 온프레미스 환경에서 AWS Directory Service for Microsoft Active Directory 또는 Microsoft Active Directory에서 또는 AD Connector AWS 를 사용하여 Active Directory 그룹에 대한 액세스를 제공합니다. 또한 이 옵션을 사용하려면 IdentityProviderDetails 파라미터를 사용하여 디렉터리 ID를 제공해야 합니다.

API_GATEWAY 값을 사용하여 선택하는 자격 증명 제공자와 통합합니다. 이 API_GATEWAY 설정을 사용하려면 IdentityProviderDetails 파라미터를 사용하여 인증을 호출URL할 Amazon API Gateway 엔드포인트를 제공해야 합니다.

AWS_LAMBDA 값을 사용하여 AWS Lambda 함수를 자격 증명 공급자로 직접 사용합니다. 이 값을 선택하는 경우 IdentityProviderDetails 데이터 유형의 Function 파라미터에 ARN Lambda 함수에 대한 를 지정해야 합니다.

타입: 문자열

유효 값: SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

필수 여부: 아니요

LoggingRole

서버가 Amazon S3 또는 Amazon 에 대한 Amazon CloudWatch 로깅을 켤 수 있도록 허용하는 () 역할ARN의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다EFSevents. 설정하면 CloudWatch 로그에서 사용자 활동을 볼 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/\S+

Required: No

ServerId

나열된 서버의 고유한 시스템 할당 식별자를 지정합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: s-([0-9a-f]{17})

Required: No

State

설명된 서버의 상태입니다. 값이 ONLINE 이면 서버가 작업을 수락하고 파일을 전송할 수 있음을 나타냅니다. State값이 OFFLINE(이)면 서버에서 File Transfer 작업을 수행할 수 없습니다.

STARTING 및 STOPPING 상태는 서버가 완전히 응답할 수 없거나 완전히 오프라인 상태가 아닌 중간 상태임을 나타냅니다. START_FAILED 또는 STOP_FAILED의 값은 오류 상태를 나타낼 수 있습니다.

타입: 문자열

유효 값: OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

필수 여부: 아니요

UserCount

ServerId를 사용하여 지정한 서버에 할당되는 사용자 수를 지정합니다.

타입: 정수

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedUser

지정한 사용자의 속성을 반환합니다.

내용

Arn

학습하려는 사용자의 고유한 Amazon 리소스 이름(ARN)을 제공합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

Pattern: arn:\S+

필수 여부: 예

HomeDirectory

사용자가 클라이언트를 사용하여 서버에 로그인하는 경우 사용자를 위한 랜딩 디렉터리(폴더).

HomeDirectory의 예: /bucket_name/home/mydirectory

Note

HomeDirectory 파라미터는 HomeDirectoryType이(가) PATH(으)로 설정된 경우에만 사용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: (|/.*)

Required: No

HomeDirectoryType

사용자가 서버에 로그인하는 경우 홈 디렉터리가 될 랜딩 디렉터리(폴더) 타입입니다. 로 설정하면 PATH파일 전송 프로토콜 클라이언트에서와 같이 절대 Amazon S3 버킷 또는 Amazon EFS 경로

가 표시됩니다. 로 설정한 경우 Amazon S3 또는 Amazon EFS 경로를 사용자에게 표시할 방법에 HomeDirectoryMappings 대한 매핑을 에 LOGICAL 제공해야 합니다.

Note

HomeDirectoryType이 LOGICAL인 경우, HomeDirectoryMappings 파라미터를 사용하여 매핑을 제공해야 합니다. 반면에 HomeDirectoryType이 PATH인 경우, HomeDirectory 파라미터를 사용하여 절대 경로를 제공하세요. 템플릿에 HomeDirectory 및 HomeDirectoryMappings를 모두 포함할 수는 없습니다.

타입: 문자열

유효 값: PATH | LOGICAL

필수 여부: 아니요

Role

Amazon S3 버킷 또는 Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 (ARN) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 이 역할에 연결된 정책은 Amazon S3 버킷 또는 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다. IAM 또한 역할에는 사용자의 전송 요청을 처리할 때 서버가 리소스에 액세스할 수 있도록 허용하는 신뢰 관계가 포함되어야 합니다.

Note

가 있는 서버의 경우 Amazon S3 버킷에 대한 사용자의 액세스를 제어하고 Domain=S3가 있는 서버의 경우 EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 IAM 역할입니다. Domain=EFS.

이 역할에 연결된 정책은 S3 버킷 또는 파일 EFS 시스템으로 파일을 전송하거나 전송할 때 사용자에게 제공할 액세스 수준을 결정합니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: arn:.*role/S+

Required: No

SshPublicKeyCount

지정한 사용자에 대해 저장된 SSH 퍼블릭 키 수를 지정합니다.

유형: 정수

필수 항목 여부: 아니요

UserName

가 지정된 사용자의 이름을 ARN 지정합니다. 사용자 이름은 인증 목적으로 사용됩니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

패턴: `[\w][\w@.-]{2,99}`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ListedWorkflow

워크플로의 식별자, 텍스트 설명 및 Amazon 리소스 이름(ARN)을 포함합니다.

내용

Arn

워크플로의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 20입니다. 최대 길이는 1600입니다.

패턴: `arn:\S+`

Required: No

Description

워크플로에 대한 텍스트 설명을 지정합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `[\w- ]*`

Required: No

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

패턴: `w-([a-z0-9]{17})`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

LoggingConfiguration

로깅 역할과 로그 그룹 명칭으로 구성됩니다.

내용

LoggingRole

서버가 Amazon S3 또는 Amazon EFS에 대한 Amazon CloudWatch 로깅을 켤 수 있도록 허용하는 () 역할ARN의 Amazon 리소스 이름 AWS Identity and Access Management (IAM)입니다. 설정하면 CloudWatch 로그에서 사용자 활동을 볼 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

패턴: `arn:.*role/\S+`

Required: No

LogGroupName

이 워크플로가 속한 AWS Transfer Family 서버의 CloudWatch 로깅 그룹 이름입니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 512입니다.

패턴: `[\.\-_\#A-Za-z0-9]*`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

PosixProfile

Amazon EFS 파일 시스템에 대한 사용자의 액세스를 제어하는 사용자 ID(Uid), 그룹 ID(Gid) 및 보조 그룹IDs(SecondaryGids)을 포함한 전체 POSIX 자격 증명입니다. 파일 시스템의 파일 및 디렉터리에 설정된 POSIX 권한에 따라 Amazon EFS 파일 시스템으로 파일을 전송하거나 전송할 때 사용자가 받는 액세스 수준이 결정됩니다.

내용

Gid

이 사용자가 모든 EFS 작업에 사용하는 POSIX 그룹 ID입니다.

타입: Long

유효 범위: 최소값은 0입니다. 최댓값은 4294967295입니다.

필수 여부: 예

Uid

이 POSIX 사용자가 모든 EFS 작업에 사용하는 사용자 ID입니다.

타입: Long

유효 범위: 최소값은 0입니다. 최댓값은 4294967295입니다.

필수 여부: 예

SecondaryGids

이 사용자가 모든 EFS 작업에 IDs 사용하는 보조 POSIX 그룹입니다.

타입: 로그 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 16개입니다.

유효 범위: 최소값은 0입니다. 최댓값은 4294967295입니다.

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ProtocolDetails

서버에 대해 구성된 프로토콜 설정입니다.

내용

As2Transports

AS2 메시지의 전송 방법을 나타냅니다. 현재 HTTP만 지원됩니다.

타입: 문자열 배열

배열 멤버: 고정된 항목 수는 1개입니다.

유효 값: HTTP

필수 여부: 아니요

PassiveIp

FTP 및 FTPS 프로토콜의 수동 모드를 나타냅니다. 방화벽, 라우터 또는 로드 밸런서의 퍼블릭 IP IPv4 주소와 같은 단일 주소를 입력합니다. 예:

```
aws transfer update-server --protocol-details PassiveIp=0.0.0.0
```

위의 예에서 0.0.0.0을 사용하려는 실제 IP 주소로 바꿉니다.

Note

PassiveIp 값을 변경하는 경우 변경 사항을 적용하려면 Transfer Family 서버를 중지했다가 다시 시작해야 합니다. NAT 환경에서 수동 모드(PASV)를 사용하는 방법에 대한 자세한 내용은 [방화벽 뒤의 FTPS 서버 구성 또는 NAT 를 참조하세요 AWS Transfer Family](#).

특수 값

AUTO 및 0.0.0.0은 PassiveIp 파라미터에 대한 특수 값입니다. 값은 기본적으로 FTP 및 FTPS 유형 서버에 할당 PassiveIp=AUTO됩니다. 이 경우 서버는 응답 IPs 내의 엔드포인트 중 하나로 자동으로 PASV 응답합니다. PassiveIp=0.0.0.0은 사용에 대한 보다 고유한 애플리케이션을 갖추고 있습니다. 예를 들어 서브넷이 3개인고가용성(HA) Network Load Balancer(NLB) 환경이 있는 경우 PassiveIp 파라미터를 사용하여 단일 IP 주소만 지정할 수 있습니다. 이렇게 하면고가용성의 효과가 감소합니다. 이 경우 PassiveIp=0.0.0.0을 지정할 수 있습니다. 이렇게 하

면 클라이언트가 Control 연결과 동일한 IP 주소를 사용하고 모든 를 연결AZs에 사용하도록 지시합니다. 그러나 모든 FTP 클라이언트가 PassiveIp=0.0.0.0 응답을 지원하는 것은 아닙니다. FileZilla 및 WinSCP은 응답을 지원합니다. 다른 클라이언트를 사용하는 경우 해당 클라이언트가 PassiveIp=0.0.0.0 응답을 지원하는지 확인하세요.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 15입니다.

필수 여부: 아니요

SetStatOption

SetStatOption을 사용하여 S3 버킷에 업로드하는 파일에 대해 클라이언트가 SETSTAT를 사용하려고 할 때 생성되는 오류를 무시합니다.

일부 SFTP 파일 전송 클라이언트는 파일을 업로드할 SETSTAT 때와 같은 명령을 사용하여 타임스탬프 및 권한을 포함하여 원격 파일의 속성을 변경하려고 시도할 수 있습니다. 그러나 이러한 명령은 Amazon S3와 같은 객체 스토리지 시스템과 호환되지 않습니다. 이러한 비호환성으로 인해 이러한 클라이언트에서 파일을 업로드하면 파일이 성공적으로 업로드된 경우에도 오류가 발생할 수 있습니다.

Transfer Family 서버가 SETSTAT 명령을 무시ENABLE_NO_OP하도록 값을 로 설정하고 SFTP 클라이언트를 변경할 필요 없이 파일을 업로드합니다. SetStatOption ENABLE_NO_OP 설정은 오류를 무시하지만 Amazon CloudWatch Logs에서 로그 항목을 생성하므로 클라이언트가 언제 SETSTAT 전화를 걸고 있는지 확인할 수 있습니다.

Note

파일의 원래 타임스탬프를 보존하고 를 사용하여 다른 파일 속성을 수정하려면 Transfer Family에서 Amazon을 백엔드 스토리지EFS로 사용할 SETSTAT수 있습니다.

타입: 문자열

유효 값: DEFAULT | ENABLE_NO_OP

필수 여부: 아니요

TlsSessionResumptionMode

FTPS 프로토콜을 사용하는 Transfer Family 서버에 사용되는 속성입니다. TLS 세션 재개는 FTPS 세션에 대한 제어와 데이터 연결 간에 협상된 보안 암호를 재개하거나 공유하는 메커

니즘을 제공합니다. 는 서버가 고유한 세션 ID를 통해 최근에 협상된 세션을 재개할지 여부를 TlsSessionResumptionMode 결정합니다. 이 속성은 CreateServer 및 UpdateServer 호출 중 사용할 수 있습니다. CreateServer 중에 TlsSessionResumptionMode 값을 지정하지 않으면 기본적으로 ENFORCED로 설정됩니다.

- **DISABLED:** 서버는 TLS 세션 재개 클라이언트 요청을 처리하지 않으며 각 요청에 대해 새 TLS 세션을 생성합니다.
- **ENABLED:** 서버는 TLS 세션 재개를 수행하는 클라이언트를 처리하고 수락합니다. 서버는 TLS 세션 재개 클라이언트 처리를 수행하지 않는 클라이언트 데이터 연결을 거부하지 않습니다.
- **ENFORCED:** 서버는 TLS 세션 재개를 수행하는 클라이언트를 처리하고 수락합니다. 서버는 TLS 세션 재개 클라이언트 처리를 수행하지 않는 클라이언트 데이터 연결을 거부합니다. 값을 ENFORCED로 설정하기 전에 클라이언트를 테스트합니다.

Note

모든 FTPS 클라이언트가 TLS 세션 재개를 수행하는 것은 아닙니다. 따라서 TLS 세션 재개를 적용하도록 선택하면 프로토콜 협상을 수행하지 않는 FTPS 클라이언트와의 연결을 방지할 수 있습니다. ENFORCED 값을 사용할 수 있는지 여부를 결정하려면 클라이언트를 테스트해야 합니다.

타입: 문자열

유효 값: DISABLED | ENABLED | ENFORCED

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

S3FileLocation

워크플로에서 사용 중인 파일의 파일 위치에 대한 세부 정보를 지정합니다. S3 스토리지를 사용하는 경우에만 해당됩니다.

내용

Bucket

사용 중인 파일이 포함된 S3 버킷을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 63입니다.

패턴: `[a-z0-9][\.-a-z0-9]{1,61}[a-z0-9]`

필수 여부: 아니요

Etag

개체 태그는 객체의 해시입니다. 는 메타데이터가 아닌 객체의 콘텐츠에 대한 변경 사항만 ETag 반영합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 65536입니다.

패턴: `.+`

필수 여부: 아니요

Key

Amazon S3 생성 시 작업에 할당된 명칭 객체 키를 사용하여 객체를 검색합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `[\P{M}\p{M}]*`

필수 여부: 아니요

VersionId

파일 버전을 지정합니다.

타입: 문자열

길이 제약: 최소 길이 1. 최대 길이는 1024입니다.

패턴: .+

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

S3InputFileLocation

고객이 입력한 Amazon S3 파일 위치를 지정합니다.

`copyStepDetails.DestinationFileLocation` 내부에서 사용하는 경우 S3 복사 대상이어야 합니다.

버킷과 키를 제공해야 합니다. 키는 경로 또는 파일을 나타낼 수 있습니다. 키 값 끝낼 슬래시 (/) 문자로 끝낼지 여부에 따라 결정됩니다. 마지막 문자가 "/"인 경우, 파일은 폴더에 복사되며 명칭은 변경되지 않습니다. 최종 문자가 영숫자인 경우, 업로드한 파일은 경로 값으로 명칭이 바뀝니다. 이 경우 같은 명칭의 파일이 이미 있으면 덮어씁니다.

예를 들어 경로가 `shared-files/bob/`인 경우 업로드한 파일은 `shared-files/bob/`, 폴더에 복사됩니다. 경로가 `shared-files/today`인 경우, 업로드된 각 파일이 `shared-files` 폴더에 복사되고 명칭이 `today(으)`로 지정됩니다. 각 업로드는 이전 버전의 `bob` 파일을 덮어씁니다.

내용

Bucket

고객 입력 파일의 S3 버킷을 지정합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 63입니다.

패턴: `[a-z0-9][\.-a-z0-9]{1,61}[a-z0-9]`

필수 여부: 아니요

Key

Amazon S3 생성 시 작업에 할당된 명칭 객체 키를 사용하여 객체를 검색합니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 1024입니다.

패턴: `[\P{M}\p{M}]*`

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

S3StorageOptions

서버에 대해 구성된 Amazon S3 스토리지 옵션입니다.

내용

DirectoryListingOptimization

Amazon S3 디렉터리의 성능 최적화 여부를 지정합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

기본적으로 홈 디렉터리 매핑의 는 TYPE입니다DIRECTORRY. 이 옵션을 활성화하면 매핑에 파일 대상이 포함되도록 HomeDirectoryMapEntry Type FILE 하려면 를 로 명시적으로 설정해야 합니다.

타입: 문자열

유효 값: ENABLED | DISABLED

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

S3Tag

태깅 단계 실행 중에 파일에 할당되는 키-값 쌍을 지정합니다.

내용

Key

생성한 태그에 할당한 명칭입니다.

타입: 문자열

길이 제약: 최소 길이는 1. 최대 길이 128.

Pattern: (`[\\p{L}\\p{Z}\\p{N}_.: /+=\\-@]*`)

필수 여부: 예

Value

키에 해당하는 값입니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: (`[\\p{L}\\p{Z}\\p{N}_.: /+=\\-@]*`)

필수 여부: 예

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

ServiceMetadata

워크플로와 관련된 세션 세부 정보를 위한 컨테이너 객체입니다.

내용

UserDetails

서버 ID(ServerId), 세션 ID(SessionId) 및 사용자(Username)는 UserDetails를(을) 구성합니다.

타입: [UserDetails](#) 객체

필수 여부: 예

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

SftpConnectorConfig

SFTP 커넥터 객체에 대한 세부 정보를 포함합니다. 커넥터 객체는 파트너의 SFTP 서버와 파일을 주고 받는 데 사용됩니다.

Note

SftpConnectorConfig 데이터 유형은 SFTP 커넥터 생성 및 업데이트 모두에 사용되므로 파라미터 TrustedHostKeys와 UserSecretId는 필요하지 않은 것으로 표시됩니다. 이는 기존 SFTP 커넥터를 업데이트할 때는 필요하지 않지만 새 SFTP 커넥터를 생성할 때는 필요하기 때문에 다소 오해의 소지가 있습니다.

내용

TrustedHostKeys

연결 중인 외부 서버를 식별하는 데 사용되는 호스트 키 또는 키의 공개 부분입니다. SFTP 서버에 대해 ssh-keyscan 명령을 사용하여 필요한 키를 검색할 수 있습니다.

세 가지 표준 SSH 퍼블릭 키 형식 요소는 각 요소 사이에 공백이 <comment> 있는 <key type><body base64>, 및 선택적입니다. <key type>과 <body base64>만 지정하세요. 키의 <comment> 부분은 입력하지 마세요.

신뢰할 수 있는 호스트 키의 경우 AWS Transfer Family 및 RSA ECDSA 키를 수락합니다.

- RSA 키의 경우 <key type> 문자열은 ssh-rsa.
- ECDSA 키의 경우 <key type> 문자열은 생성한 키의 크기에 따라 ecdsa-sha2-nistp521, ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 또는입니다.

이 명령을 실행하여 SFTP 서버 이름이 인 SFTP 서버 호스트 키를 검색합니다 ftp.host.com.

```
ssh-keyscan ftp.host.com
```

이렇게 하면 퍼블릭 호스트 키가 표준 출력으로 인쇄됩니다.

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key
```

이 문자열을 create-connector 명령의 TrustedHostKeys 필드에 복사하여 붙여넣거나 콘솔의 신뢰할 수 있는 호스트 키 필드에 붙여넣습니다.

타입: 문자열 배열

배열 멤버: 최소 항목 수는 1개입니다. 최대 항목 수는 10개입니다.

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 2,048.

필수 여부: 아니요

UserSecretId

SFTP 사용자의 프라이빗 키, 암호 또는 둘 다를 포함하는 보안 암호(AWS S Secrets Manager)의 식별자입니다. 식별자는 보안 암호의 Amazon 리소스 이름(ARN)이어야 합니다.

유형: 문자열

길이 제약: 최소 길이는 1. 최대 길이는 2,048.

필수 여부: 아니요

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

SshPublicKey

특정 파일 전송 프로토콜 지원 서버(로 식별됨SSH)에 대해 Transfer Family 사용자와 연결된 퍼블릭 Secure Shell() 키에 대한 정보를 제공합니다ServerId. 반환된 정보에는 키를 가져온 날짜, 퍼블릭 키 내용 및 퍼블릭 키 ID가 포함됩니다. 사용자는 특정 서버에 사용자 이름과 연결된 SSH 퍼블릭 키를 두 개 이상 저장할 수 있습니다.

내용

DateImported

퍼블릭 키가 Transfer Family 사용자 계정에 추가된 날짜를 지정합니다.

타입: Timestamp

필수 여부: 예

SshPublicKeyBody

에서 지정한 대로 SSH 퍼블릭 키의 콘텐츠를 지정합니다PublicKeyId.

AWS Transfer Family 는 RSA, ECDSA 및 ED25519 키를 허용합니다.

유형: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 2048입니다.

필수 여부: 예

SshPublicKeyId

퍼블릭 키의 식별자를 포함하는 SshPublicKeyId 파라미터를 지정합니다.

타입: 문자열

길이 제약 조건: 고정 길이는 21입니다.

Pattern: key-[0-9a-f]{17}

필수 여부: 예

참고

언어별 중 하나API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

Tag

특정 리소스의 키-값 쌍을 생성합니다. 태그는 다양한 목적으로 리소스를 검색하고 그룹화하는 데 사용할 수 있는 메타데이터입니다. 서버, 사용자 및 역할에 태그를 적용할 수 있습니다. 태그는 복수의 값을 가질 수 있습니다. 예를 들어, 계정 관리를 위해 서버를 그룹화하려면 Group(이)라는 태그를 만들고 해당 그룹에 값 Research 및 Accounting를 할당할 수 있습니다.

내용

Key

생성한 태그에 할당한 명칭입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 128입니다.

필수 여부: 예

Value

생성한 키 이름에 할당한 하나 이상의 값을 포함합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256.

필수 여부: 예

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

TagStepDetails

각 단계 타입에는 자체의 StepDetails 구조가 있습니다.

워크플로 단계를 실행하는 동안 파일에 태그를 지정하는 데 사용되는 키/값 쌍입니다.

내용

Name

단계의 명칭, 식별자로 사용됨.

타입: 문자열

길이 제약 조건: 최소 길이는 0입니다. 최대 길이는 30입니다.

패턴: `[\w-]*`

필수 여부: 아니요

SourceFileLocation

워크플로 단계의 입력으로 사용할 파일(이전 단계의 출력 또는 워크플로에 처음 업로드한 파일)을 지정합니다.

- 이전 파일을 입력으로 사용하려면 `${previous.file}`를 입력합니다. 이 경우 이 워크플로 단계에서는 이전 워크플로 단계의 출력 파일을 입력으로 사용합니다. 이것이 기본값입니다.
- 시초로 업로드된 파일 위치를 이 단계의 입력으로 사용하려면 `${original.file}`를 입력합니다.

타입: 문자열

길이 제약: 최소 길이는 0. 최대 길이는 256입니다.

Pattern: `\$\{(\w+.\w+)\}`

Required: No

Tags

1~10개의 키/값 쌍을 포함하는 배열.

타입: [S3Tag](#) 객체 배열

어레이 멤버: 최소 항목 수 1개. 최대 항목 수 10개.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

UserDetails

워크플로에 대한 사용자 이름, 서버 ID 및 세션 ID를 지정합니다.

내용

ServerId

전송 서버 인스턴스에 대한 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: s-([0-9a-f]{17})

필수 여부: 예

UserName

서버와 연결된 Transfer Family 사용자를 식별하는 고유한 문자열입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이는 100입니다.

Pattern: [\w][\w@.-]{2,99}

필수 여부: 예

SessionId

워크플로에 해당하는 세션에 대해 시스템에서 할당한 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 최소 길이는 3입니다. 최대 길이 32.

패턴: [\w-]*

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

WorkflowDetail

할당할 워크플로의 워크플로 ID와 워크플로 실행에 사용되는 실행 역할을 지정합니다.

파일이 완전히 업로드될 때 실행되는 워크플로 외에도 WorkflowDetails에는 부분 업로드 시 실행할 워크플로의 워크플로 ID와 실행 역할이 포함될 수 있습니다. 파일이 업로드되는 동안 서버 세션 연결이 끊기면 부분 업로드가 수행됩니다.

내용

ExecutionRole

Transfer가 수입할 수 있는 S3, EFS 및 Lambda 작업에 필요한 권한을 포함하여 모든 워크플로 단계가 필요한 리소스에서 작동할 수 있습니다.

유형: 문자열

길이 제약: 최소 길이는 20. 최대 길이는 2,048.

Pattern: `arn:.*role/\S+`

필수 여부: 예

WorkflowId

워크플로의 고유 식별자입니다.

타입: 문자열

길이 제약 조건: 고정 길이는 19입니다.

Pattern: `w-([a-z0-9]{17})`

필수 여부: 예

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK Ruby V3용](#)

WorkflowDetails

WorkflowDetail 데이터 타입에 대한 컨테이너입니다. 실행을 시작하도록 워크플로를 트리거하는 작업에서 사용됩니다.

내용

OnPartialUpload

파일이 부분적으로만 업로드된 경우 워크플로를 시작하는 트리거입니다. 부분 업로드가 있을 때마다 실행되는 서버에 워크플로를 연결할 수 있습니다.

세션 연결이 끊길 때 파일이 열려 있으면 부분 업로드가 수행됩니다.

타입: [WorkflowDetail](#) 객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

OnUpload

워크플로를 시작하는 트리거: 파일이 업로드된 후 워크플로가 실행되기 시작합니다.

서버에서 연결된 워크플로를 제거하려면 다음 예제와 같이 빈 OnUpload 객체를 제공하면 됩니다.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-  
details '{"OnUpload":[]}'
```

타입: [WorkflowDetail](#) 객체 배열

배열 구성원: 최소수는 0개입니다. 최대 항목 수는 1개입니다.

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)

- [AWS SDK Ruby V3용](#)

WorkflowStep

워크플로의 기본 구성 요소입니다.

내용

CopyStepDetails

파일 복사를 수행하는 단계에 대한 세부 정보입니다.

다음 값으로 구성됩니다.

- 설명
- 파일 사본의 대상에 대한 Amazon S3 위치입니다.
- 같은 이름의 기존 파일을 덮어쓸지 여부를 나타내는 플래그입니다. 기본값은 FALSE입니다.

타입: [CopyStepDetails](#) 객체

필수 여부: 아니요

CustomStepDetails

AWS Lambda 함수를 호출하는 단계에 대한 세부 정보입니다.

Lambda 함수의 이름, 대상 및 제한 시간(초)으로 구성됩니다.

타입: [CustomStepDetails](#) 객체

필수 여부: 아니요

DecryptStepDetails

암호화된 파일의 암호를 복호화하는 단계에 대한 세부 정보입니다.

다음 값으로 구성됩니다.

- 설명이 포함된 이름을 지정합니다.
- 소스 파일이 복호화할 Amazon S3 또는 Amazon Elastic File System(Amazon EFS) 위치입니다.
- 파일 복호화 대상의 S3 또는 Amazon EFS 위치입니다.
- 같은 명칭의 기존 파일을 덮어쓸지 여부를 나타내는 플래그입니다. 기본값은 FALSE입니다.
- 사용되는 암호화 타입입니다. 현재는 PGP 암호화만 지원됩니다.

유형: [DecryptStepDetails](#) 객체

필수 여부: 아니요

DeleteStepDetails

파일을 삭제하는 단계에 대한 세부 정보입니다.

타입: [DeleteStepDetails](#) 객체

필수 여부: 아니요

TagStepDetails

하나 이상의 태그를 생성하는 단계에 대한 세부 정보입니다.

태그를 하나 이상 지정합니다. 각 태그에는 키-값 쌍이 포함되어 있습니다.

타입: [TagStepDetails](#) 객체

필수 여부: 아니요

Type

현재 다음과 같은 단계 타입이 지원됩니다.

- **COPY** - 다른 위치에 파일을 복사합니다.
- **CUSTOM** - AWS Lambda 함수 대상으로 사용자 지정 단계를 수행합니다.
- **DECRYPT** - 업로드되기 전에 암호화된 파일을 복호화합니다.
- **DELETE** - 파일을 삭제합니다.
- **TAG** - 파일에 태그를 추가합니다.

타입: 문자열

유효 값: COPY | CUSTOM | TAG | DELETE | DECRYPT

필수 여부: 아니요

참고

언어별 중 하나 API에서 이 를 사용하는 방법에 대한 자세한 내용은 다음을 AWS SDKs 참조하세요.

- [AWS SDK C++용](#)
- [AWS SDK Go용](#)
- [AWS SDK Java V2용](#)
- [AWS SDK Ruby V3용](#)

API 요청 만들기

콘솔의 사용 외에도, AWS Transfer Family API를 사용하여 서버를 프로그래밍 방식으로 구성 및 관리할 수 있습니다. 이 섹션은 AWS Transfer Family 작동, 인증 요청 확인 및 오류 처리를 설명합니다. Transfer Family에서 사용할 수 있는 지역 및 엔드포인트에 대한 자세한 설명은 AWS 일반 참조의 [AWS Transfer Family 엔드포인트 및 할당량](#)을 참조하세요.

Note

Transfer Family로 애플리케이션을 개발할 때 AWS SDK를 사용할 수도 있습니다. Java, .NET 및 PHP용 AWS SDK는 프로그래밍 작업을 간소화하며 기본 Transfer Family API를 포함합니다. SDK 라이브러리 다운로드에 대한 정보는 [샘플 코드 라이브러리](#) 섹션을 참조하세요.

주제

- [Transfer Family 필수 요청 헤더](#)
- [Transfer Family 요청 입력 및 서명](#)
- [오류 응답](#)
- [사용 가능한 라이브러리](#)

Transfer Family 필수 요청 헤더

이 섹션에서는 AWS Transfer Family에 대한 모든 POST 요청과 함께 전송해야 하는 필수 헤더에 대해 설명합니다. 호출하려는 작업을 포함하는 요청에 대한 핵심 정보, 요청 날짜 및 요청 전송자의 권한을 부여함을 나타내는 정보를 식별할 HTTP 헤더를 포함해야 합니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음은 [ListServers](#) 작업에서 사용하는 헤더의 예입니다.

```
POST / HTTP/1.1
Host: transfer.us-east-1.amazonaws.com
x-amz-target: TransferService.ListServers
x-amz-date: 20220507T012034Z
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20220507/us-east-1/transfer/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=13550350a8681c84c861aac2e5b440161c2b33a3e4f302ac680ca5b686de48de
Content-Type: application/x-amz-json-1.1
```



```
Content-Length: 17
```

```
{"MaxResults":10}
```

다음은 Transfer Family에 대한 POST 요청과 함께 포함해야 하는 헤더입니다. "x-amz"로 시작하는 아래의 헤더는 AWS에 고유한 헤더입니다. 나머지 헤더는 HTTP 트랜잭션에 사용되는 공통 헤더입니다.

헤더	설명
Authorization	승인 헤더가 필요합니다. 형식은 표준 Sigv4 요청 서명이며, 이는 서명 AWS API 요청 에 설명되어 있습니다.
Content-Type	Transfer Family에 대한 모든 요청의 콘텐츠 타입으로 application/x-amz-json-1.1 를 사용하세요. Content-Type: application/x-amz-json-1.1
Host	호스트 헤더를 사용하여 요청을 전송하는 Transfer Family 엔드포인트를 지정합니다. 예컨대, transfer.us-east-1.amazonaws.com 은 미국 동부(오하이오) 지역의 엔드포인트입니다. Transfer Family에 사용할 수 있는 엔드포인트에 대한 자세한 설명은 AWS 일반 참조의 AWS Transfer Family 엔드포인트 및 할당량 을 참조하세요. Host: transfer. <i>region</i> .amazonaws.com
x-amz-date	HTTP Date 헤더 또는 AWS x-amz-date 헤더에 타임스탬프를 제공해야 합니다. 일부 HTTP 클라이언트 라이브러리에서는 Date 헤더를 설정할 수 없습니다. x-amz-date 헤더가 있으면 Transfer Family는 요청 인증 중 모든 Date 헤더를 무시합니다. x-amz-date 형식은 YYYYMMDD'T'HHMMSS'Z' 형식의 ISO8601이어야 합니다. x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i>
x-amz-target	이 헤더는 API의 버전과 요청 중인 작업을 지정합니다. 대상 헤더 값은 API 버전을 API 이름과 연결하여 구성하며 형식은 다음과 같습니다.

헤더	설명
	x-amz-target: TransferService. <i>operationName</i> OperationName 값(예: ListServers)은 API 목록인 ListServers에서 찾을 수 있습니다.
x-amz-security-token	이 헤더는 요청에 서명하는 데 사용되는 자격 증명이 임시 또는 세션 자격 증명인 경우 필요합니다(자세한 설명은 IAM 사용자 가이드의 AWS 리소스로 임시 자격 증명 사용 참조). 자세한 설명은 Amazon Web Services 일반 참조의 HTTP 요청에 서명 추가를 참조하세요.

Transfer Family 요청 입력 및 서명

모든 요청 입력은 요청 본문의 JSON 페이로드의 일부로 전송되어야 합니다. 모든 요청 필드가 선택 사항(예: ListServers)인 작업의 경우 요청 본문에 {}와 같이 빈 JSON 객체를 제공해야 합니다. Transfer Family 페이로드 요청/응답의 구조는 기존 API 참조(예: [DescribeServer](#))에 문서화되어 있습니다.

Transfer Family는 AWS 서명 버전 4를 이용한 인증을 지원합니다. 자세한 설명은 [AWS API 요청 서명](#)을 참조하세요.

오류 응답

오류가 있는 경우, 응답 헤더 정보에는 다음 내용이 포함됩니다.

- 콘텐츠 타입: application/x-amz-json-1.1
- 적절한 4xx 또는 5xx HTTP 상태 코드

오류 응답의 본문에는 발생한 오류에 대한 정보가 포함됩니다. 다음 샘플 오류 응답은 모든 오류 응답에 공통된 응답 요소의 출력 구문을 나타냅니다.

```
{
  "__type": "String",
  "Message": "String", <!-- Message is lowercase in some instances -->
  "Resource": String,
  "ResourceType": String
}
```

```
"RetryAfterSeconds": String
}
```

다음 표는 이전 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__타입

Transfer Family API 호출의 예외 중 하나입니다.

타입: 문자열

메시지 또는 메시지

작업 오류 코드 메시지 중 하나입니다.

Note

일부 예외에서 message가 사용되고 다른 예외에서 Message가 사용됩니다. 인터페이스의 코드를 확인하여 적절한 대/소문자를 확인할 수 있습니다. 또는 각 옵션을 테스트하여 어떤 옵션이 효과가 있는지 확인할 수 있습니다.

타입: 문자열

리소스

오류가 호출된 리소스입니다. 예컨대, 이미 존재하는 사용자를 만들려고 하면 Resource가 기존 사용자의 사용자 이름이 됩니다.

타입: 문자열

ResourceType

오류가 호출되는 리소스 타입입니다. 예컨대, 이미 존재하는 사용자를 만들려고 하면 ResourceType이 User가 됩니다.

타입: 문자열

RetryAfterSeconds

명령을 재시도하기 전에 대기하는 시간(초).

타입: 문자열

오류 응답 예

DescribeServer API를 호출하고 존재하지 않는 서버를 지정하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

API 실행 시 병목 현상이 발생하는 경우 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

CreateServer API를 사용하고 Transfer Family 서버를 생성할 수 있는 충분한 권한이 없는 경우 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

CreateUser API를 사용하고 이미 존재하는 사용자를 지정하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

사용 가능한 라이브러리

AWS에서는 command-line 도구 및 Query API 대신 언어별로 고유한 API를 사용하여 애플리케이션을 빌드하는 것을 선호하는 소프트웨어 개발자를 위해 라이브러리, 샘플 코드, 자습서 및 기타 리소스를

제공합니다. 이러한 라이브러리는 보다 쉽게 시작하도록 요청 인증, 요청 재시도 및 오류 처리 같은 기본 기능(API에는 포함되지 않음)을 제공합니다. [AWS 기반 도구](#)를 참조하세요.

모든 언어의 라이브러리와 샘플 코드는 [샘플 코드 및 라이브러리](#)를 참조하세요.

공통 파라미터

다음 목록에는 모든 작업이 쿼리 문자열을 사용하여 Signature Version 4 요청에 서명하는 데 사용하는 파라미터가 포함되어 있습니다. 작업별 파라미터는 그 작업에 대한 항목에 나열되어 있습니다. Signature Version 4에 대한 자세한 내용은 IAM 사용 설명서의 [AWS API 요청에 서명](#)을 참조하세요.

Action

수행할 작업입니다.

유형: 문자열

필수 항목 여부: 예

Version

요청이 작성되는 API 버전으로 YYYY-MM-DD 형식으로 표시됩니다.

유형: 문자열

필수 항목 여부: 예

X-Amz-Algorithm

요청 서명을 생성하는 데 사용된 해시 알고리즘입니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

유효한 값: AWS4-HMAC-SHA256

필수 항목 여부: 조건부

X-Amz-Credential

자격 증명 범위 값이며 액세스 키, 날짜, 대상으로 하는 리전, 요청하는 서비스 및 종료 문자열("aws4_request")이 포함된 문자열입니다. 값은 다음 형식으로 표시됩니다.
access_key/YYYYMMDD/region/service/aws4_request.

자세한 내용은 IAM 사용 설명서의 [서명된 AWS API 요청 생성](#)을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Date

서명을 만드는 데 사용되는 날짜입니다. 형식은 ISO 8601 기본 형식(YYYYMMDD'T'HHMMSS'Z')이어야 합니다. 예를 들어 다음 날짜 시간은 유효한 X-Amz-Date 값: 20120325T120000Z.

조건: X-Amz-Date는 모든 요청에서 옵션이지만 서명 요청에 사용되는 날짜보다 우선할 때 사용됩니다. 날짜 헤더가 ISO 8601 기본 형식으로 지정된 경우 X-Amz-Date가 필요하지 않습니다. X-Amz-Date를 사용하는 경우 항상 Date 헤더의 값을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 [AWS API 요청 서명의 요소](#)를 참조하세요.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Security-Token

AWS Security Token Service(AWS STS)에 대한 호출을 통해 받은 임시 보안 토큰입니다. AWS STS의 임시 보안 인증 정보를 지원하는 서비스 목록은 IAM 사용 설명서의 [IAM으로 작업하는 AWS 서비스](#)를 참조하세요.

조건: AWS STS의 임시 보안 인증 정보를 사용하는 경우 보안 토큰을 포함시켜야 합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Signature

서명할 문자열과 파생된 서명 키에서 계산된 16진수로 인코딩된 서명을 지정합니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-SignedHeaders

표준 요청의 일부로 포함된 모든 HTTP 헤더를 지정합니다. 서명된 헤더 지정에 대한 자세한 내용은 IAM 사용 설명서의 [서명된 AWS API 요청 생성](#)을 참조하세요.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

일반적인 오류

이 단원에는 모든 AWS 서비스의 API 작업에 대한 일반 오류가 나와 있습니다. 이 서비스의 API 작업에 대한 오류는 해당 API 작업 항목을 참조하십시오.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

IncompleteSignature

요청 서명이 AWS 표준을 준수하지 않습니다.

HTTP 상태 코드: 400

InternalFailure

알 수 없는 오류, 예외 또는 장애 때문에 요청 처리가 실패했습니다.

HTTP 상태 코드: 500

InvalidAction

요청된 동작 또는 작업이 유효하지 않습니다. 작업을 올바르게 입력했는지 확인합니다.

HTTP 상태 코드: 400

InvalidClientTokenId

제공된 X.509 인증서 또는 AWS 액세스 키 ID가 AWS의 레코드에 존재하지 않습니다.

HTTP 상태 코드: 403

NotAuthorized

이 작업을 수행하려면 권한이 있어야 합니다.

HTTP 상태 코드: 400

OptInRequired

AWS 액세스 키 ID는 서비스에 대한 구독이 필요합니다.

HTTP 상태 코드: 403

RequestExpired

요청이 요청상의 날짜 스탬프로부터 15분 이상, 또는 요청 만료 날짜(예: 미리 서명된 URL)로부터 15분 이상 경과한 후 서비스에 도달했거나, 요청상의 날짜 스탬프가 15분 이상 미래입니다.

HTTP 상태 코드: 400

ServiceUnavailable

서버의 일시적 장애로 인해 요청이 실패하였습니다.

HTTP 상태 코드: 503

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

ValidationError

입력이 AWS 서비스에서 지정한 제약에 충족되지 않습니다.

HTTP 상태 코드: 400

에 대한 문서 기록 AWS Transfer Family

다음 표에서는 이번 릴리스에 대한 설명서를 설명합니다 AWS Transfer Family.

- API 버전: transfer-2018-11-05
- 최신 설명서 업데이트: 2024년 1월 16일

변경 사항	설명	날짜
Amazon과 통합 EventBridge	AWS Transfer Family 이제 모든 파일 전송 작업에 EventBridge 대해 Amazon에 이벤트를 자동으로 게시합니다. 세부 정보는 를 사용하여 Transfer Family 이벤트 관리 Amazon EventBridge 을 참조하세요.	2024년 2월 8일
새 보안 정책 추가	AWS Transfer Family 에 새 보안 정책 FIPS 및 비FIPS보안 정책이 추가되었습니다. 또한 서버에 할당된 기본 보안 정책은 항상 최신 보안 정책입니다. 세부 정보는 에 대한 보안 정책 AWS Transfer Family 을 참조하세요.	2024년 2월 5일
SFTP 커넥터 및 에 대한 정적 IP 주소 지원 AS2	Transfer Family는 이제 SFTP 커넥터 및 에 대한 정적 IP 주소를 제공합니다AS2. 이렇게 하면 IP 허용 목록 제어로 보호되는 원격 SFTP 서버와 연결할 수 있습니다. AS2에서는 AS2 서버의 비동기 MDN 응답에 대한 정적 IP 주소를 소개합니다.	2024년 1월 16일

변경 사항	설명	날짜
최신 버전의 와 더 밀접하게 일치하도록 사용 설명서가 재구성되었습니다 AWS Transfer Family.	Transfer Family는 가이드가 시작된 이후 여러 기능을 추가했으므로 가이드를 재구성해야 합니다.	2024년 1월 3일
논리적 디렉터리 매핑 개선 사항 Amazon S3 목록 성능 최적화	이제 Transfer Family는 최대 2.1MB의 논리적 디렉터리 매핑을 지원합니다. 이제 사용자 매핑이 파일에 있는지 여부를 선언할 수도 있습니다. 자세한 내용은 논리적 디렉터리 사용 규칙 단원을 참조하십시오. Amazon S3를 스토리지로 사용하는 서버를 생성하거나 업데이트할 때 이제 S3 디렉터리(또는 폴더)를 나열하는 성능을 최적화할 수 있습니다. 자세한 내용은 SFTP, FTPS 또는 FTP 서버 엔드포인트 구성 단원을 참조하십시오.	2023년 11월 17일
가상 프라이빗 클라우드(VPC) 엔드포인트가 있는 SFTP 서버의 대체 포트	이제 VPC 엔드포인트가 있는 SFTP Transfer Family 서버에 대해 표준이 아닌 대체 포트를 활성화할 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에 서버 생성 단원을 참조하십시오.	2023년 11월 17일

변경 사항	설명	날짜
SFTP 커넥터 지원	SFTP 커넥터는 의 기능을 확장 AWS Transfer Family 하여 클라우드 및 온프레미스 모두에서 원격 서버와 통신합니다. 자세한 내용은 SFTP 커넥터를 사용하여 파일 전송 및 검색 단원을 참조하십시오.	2023년 7월 25일
AS2 기본 인증 지원	이제 Transfer Family는 적응성 선언문 2(AS2) 프로토콜을 사용하는 서버에 대해 기본 인증 사용을 지원합니다. 자세한 내용은 AS2 커넥터에 대한 기본 인증 단원을 참조하십시오.	2023년 6월 30일
구조화된 JSON 로깅 지원	이제 Transfer Family는 Amazon 에 구조화된 JSON 로그 전송 CloudWatch, 로그 증기를 사용자 지정 로그 그룹으로 그룹화, 프로토콜 간 공통 로그 쿼리 수행을 지원합니다. 자세한 내용은 에 대한 Amazon CloudWatch 로깅 AWS Transfer Family 단원을 참조하십시오.	2023년 6월 24일
다양한 인증 방법 지원	Transfer Family는 암호, 퍼블릭/프라이빗 키 쌍 또는 둘 다를 사용한 인증을 지원합니다. 프로토콜 SFTP 및 사용자 지정 자격 증명 공급자를 사용하는 서버에서 사용할 수 있습니다. 자세한 내용은 SFTP 활성화 서버 생성 단원을 참조하십시오.	2023년 5월 17일

변경 사항	설명	날짜
Transfer Family가 워크플로로 처리하는 파일로 Pretty Good Privacy(PGP) 복호화 지원	Transfer Family에는 Pretty Good Privacy(PGP) 복호화에 대한 지원이 내장되어 있습니다. SFTP, FTPS또는 를 통해 Amazon Simple Storage Service(Amazon S3) 또는 Amazon Elastic File System(Amazon)FTP에 업로드된 파일에 PGP복호화를 사용할 수 있습니다EFS. 자세한 내용은 PGP 키 생성 및 관리 및 워크플로에서 PGP복호화 사용 단원을 참조하세요.	2022년 12월 21일
Transfer Family 서버를 사용한 적용성 선언문 2(AS2) 파일 전송 프로토콜에 대한 완전 관리형 지원	AWS 환경 내부 또는 외부에 있는 거래 파트너와 정보를 주고받기 위해 AS2 프로토콜을 사용하는 서버를 생성할 수 있습니다. 자세한 내용은 구성 AS2 단원을 참조하십시오.	2022년 7월 25일
서버 생성 시 디스플레이 배너 지원	서버를 생성할 때 사용자 지정 메시지를 추가할 수 있습니다. 사전 인증 메시지(모든 프로토콜)와 사후 인증 메시지(FTP 및 FTPS 서버의 경우)를 표시할 수 있습니다. 자세한 내용은 SFTP활성화 서버 생성 , FTPS 활성화 서버 생성 또는 FTP활성화 서버 생성 를 참조하세요.	2022년 2월 17일

변경 사항	설명	날짜
자격 증명 공급자 AWS Lambda 로 에 대한 지원	이제 Transfer Family 서버 AWS Lambda 와 함께 를 사용하여 사용자 지정 자격 증명 공급자에 연결할 수 있습니다. 이전에는 사용자 지정 자격 증명 공급자를 통합하기 Amazon API Gateway URL 위해 를 제공해야 했습니다. 자세한 내용은 AWS Lambda 를 사용하여 자격 증명 공급자 통합 단원을 참조하십시오.	2021년 11월 16일
관리형 File Transfer 워크플로 지원	관리형 File Transfer 워크플로는 현재 수동으로 수행하는 일반적인 작업에 대한 업로드 후 처리 추상화를 제공합니다. 자세한 내용은 AWS Transfer Family 관리형 워크플로 를 참조하세요.	2021년 9월 2일
에 대한 지원 AWS Directory Service for Microsoft Active Directory	이제 를 사용하여 서비스 관리형 및 사용자 지정 자격 증명 공급자 외에도 인증 및 권한 부여 AWS Directory Service for Microsoft Active Directory 를 위한 사용자 액세스를 관리할 수 있습니다. 자세한 내용은 AWS 디렉터리 서비스 자격 증명 공급자 사용 단원을 참조하십시오.	2021년 5월 24일

변경 사항	설명	날짜
신규 AWS 리전	AWS Transfer Family 는 이제 아프리카(케이프타운) 리전에서 사용할 수 있습니다. Transfer Family 엔드포인트에 대한 자세한 내용은 AWS 일반 참조의 AWS Transfer Family 엔드포인트 및 할당량 을 참조하세요.	2021년 2월 24일
신규 AWS 리전	AWS Transfer Family 이제 아시아 태평양(홍콩) 및 중동(바레인) 리전에서 사용할 수 있습니다. Transfer Family 엔드포인트에 대한 자세한 내용은 AWS 일반 참조의 AWS Transfer Family 엔드포인트 및 할당량 을 참조하세요.	2021년 2월 17일
Amazon을 데이터 스토어EFS로 지원	이제 Transfer Family 는 Amazon Elastic File System(Amazon)을 송수신하는 파일 전송을 지원합니다 EFS. AmazonEFS은 단순하고 확장 가능하며 완전 관리형 탄력적 NFS 파일 시스템입니다. 자세한 내용은 Amazon EFS 파일 시스템 구성 단원을 참조하십시오.	2021년 1월 6일

변경 사항	설명	날짜
에 대한 지원 AWS WAF	이제 Transfer Family는 공격으로부터 웹 애플리케이션 및 API 작업을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽 AWS WAF인 를 지원합니다. 자세한 내용은 웹 애플리케이션 방화벽 추가 단원을 참조하십시오.	2020년 11월 24일
가상 프라이빗 클라우드에서 여러 보안 그룹 지원(VPC)	이제 의 서버에 여러 보안 그룹을 연결할 수 있습니다VPC. 자세한 내용은 Virtual Private Cloud(VPC)에 서버 생성 단원을 참조하십시오.	2020년 10월 15일
신규 AWS 리전	이제 AWS GovCloud (US) 리전에서 Transfer Family를 사용할 수 있습니다. AWS GovCloud (US) 리전의 Transfer Family 엔드포인트에 대한 자세한 내용은 의 AWS Transfer Family 엔드포인트 및 할당량 을 참조하세요AWS 일반 참조. AWS GovCloud (US) 리전에서 Transfer Family를 사용하는 방법에 대한 자세한 내용은 사용 설명서 AWS Transfer Family 의 섹션을 참조하세요. AWS GovCloud (US)	2020년 9월 30일
이제 지원되는 암호화 알고리즘이 포함된 보안 정책을 서버에 연결할 수 있습니다.	이제 지원되는 암호화 알고리즘이 포함된 보안 정책을 서버에 연결할 수 있습니다. 자세한 내용은 에 대한 보안 정책 AWS Transfer Family 를 참조하세요.	2020년 8월 12일

변경 사항	설명	날짜
연방 정보 처리 표준(FIPS) 엔드포인트 지원	FIPS이제 복미 에서 -활성화된 엔드포인트를 사용할 수 있습니다 AWS 리전. 사용할 수 있는 리전은 AWS 일반 참조의 AWS Transfer Family 엔드포인트 및 할당량 을 참조하세요. SFTP활성화된 서버 엔드포인트에 FIPS 대해 를 활성화하려면 섹션을 참조하세요 SFTP활성화 서버 생성 . FTPS활성화된 서버 엔드포인트에 FIPS 대해 를 활성화하려면 섹션을 참조하세요 FTPS활성화 서버 생성 . FTP활성화된 서버 엔드포인트에 FIPS 대해 를 활성화하려면 섹션을 참조하세요 FTP활성화 서버 생성 .	2020년 8월 12일
사용자 이름 문자 길이 증가 및 추가 허용 문자	이제 사용자 이름에 @ 기호(@)와 마침표(.)를 포함할 수 있으며 최대 길이는 100자일 수 있습니다. 사용자를 추가하려면 서버 엔드포인트에 대한 사용자 관리 를 참조하세요.	2020년 8월 12일
자동 Amazon CloudWatch 로깅 AWS Identity and Access Management (IAM) 역할 생성 지원	Transfer Family는 이제 최종 사용자 활동을 보기 위한 CloudWatch 로깅 IAM 역할의 자동 생성을 지원합니다. 자세한 내용은 SFTP활성화 서버 생성 , FTPS활성화 서버 생성 또는 FTP활성화 서버 생성 를 참조하세요.	2020년 7월 30일

변경 사항	설명	날짜
AWS Transfer Family 이제 는 소스 IP를 권한 부여의 요소로 지원합니다.	Transfer Family는 최종 사용자의 소스 IP 주소를 권한 부여 요인으로 사용할 수 있는 지원을 추가하므로 보안 파일 전송 프로토콜(SFTP), 파일 전송 프로토콜SSL(FTPS) 또는 파일 전송 프로토콜()을 통한 액세스를 승인할 때 추가 보안 계층을 적용할 수 있습니다FTP. 자세한 내용은 사용자 지정 자격 증명 공급자와 작업 단원을 참조하십시오.	2020년 6월 9일
AWS 에 대한 전송SFTP은 이제 AWS Transfer Family 이며 FTP 및 에 대한 지원을 추가합니다FTPS.	이제 사용자의 파일 전송에 파일 전송 프로토콜 보안(FTPS)과 파일 전송 프로토콜()이라는 두 개의 추가 프로토콜을 사용할 수 있습니다FTP. 사용자는 기존 보안 파일 전송 프로토콜SSL(FTPS) 지원 외에도 의 (SFTP) 및 일반 텍스트 FTP 기반 워크플로를 FTP 통해 이동, 실행 AWS, 보안 및 통합할 수 있습니다.	2020년 4월 23일

변경 사항	설명	날짜
가상 프라이빗 클라우드(VPC) 보안 그룹 및 탄력적 IP 주소 지원	이제 보안 그룹을 사용하여 수신 IP 주소에 대한 허용 목록을 생성하여 서버에 추가 보안 계층을 제공할 수 있습니다. 엘라스틱 IP 주소를 서버의 엔드포인트와 연결할 수도 있습니다. 이렇게 하면 방화벽을 사용하는 사용자가 해당 엔드포인트에 대한 액세스를 허용할 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에 서버 생성 을 참조하세요.	2020년 1월 10일
에서 작업 지원 VPC	이제 에서 서버를 생성할 수 있습니다VPC. 퍼블릭 인터넷을 거치지 않고 서버를 사용하여 클라이언트를 통해 Amazon S3 버킷과 데이터를 주고 받을 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에 서버 생성 을 참조하세요.	2019년 3월 27일
첫 번째 버전의 AWS Transfer Family 릴리스.	이 최초 릴리스는 방향 설정을 포함하며, 시작 방법을 설명하고, 클라이언트 구성과 사용자 구성 및 모니터링 활동 관련 정보를 제공합니다.	2018년 11월 25일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 [AWS 용어집](#)을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.