



Panduan Pengguna

AWS Transfer Family



AWS Transfer Family: Panduan Pengguna

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan untuk yang berhubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan bagi para pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Transfer Family?	1
Bagaimana cara AWS Transfer Family kerja	4
Posting blog yang relevan untuk Transfer Family	5
Prasyarat	9
Wilayah, titik akhir, dan kuota	9
Mendaftar untuk AWS	10
Mengonfigurasi penyimpanan	10
Konfigurasi bucket Amazon S3	11
Konfigurasi sistem file Amazon EFS	16
Buat peran dan kebijakan IAM	19
Membuat peran pengguna	21
Bagaimana kebijakan sesi bekerja	24
Contoh kebijakan read/write akses	27
Tutorial Transfer Family	31
Memulai dengan titik akhir server	32
Prasyarat	32
Langkah 1: Masuk ke AWS Transfer Family konsol	33
Langkah 2: Buat SFTP-enabled server	33
Langkah 3: Tambahkan pengguna yang dikelola layanan	34
Langkah 4: Transfer file menggunakan klien	36
Buat Alur Kerja dekripsi	38
Langkah 1: Konfigurasi peran eksekusi	38
Langkah 2: Buat alur kerja terkelola	40
Langkah 3: Tambahkan alur kerja ke server dan buat pengguna	41
Langkah 4: Buat key pair PGP	42
Langkah 5: Simpan kunci pribadi PGP di AWS Secrets Manager	43
Langkah 6: Enkripsi file	44
Langkah 7: Jalankan alur kerja dan lihat hasilnya	45
Buat dan gunakan konektor SFTP	46
Jenis jalan keluar konektor	47
Langkah 1: Buat sumber daya pendukung yang diperlukan	48
Langkah 2: Buat dan uji konektor SFTP	54
Langkah 3: Kirim dan ambil file menggunakan konektor SFTP	59

Prosedur untuk membuat server Transfer Family untuk digunakan sebagai server SFTP jarak jauh Anda	64
Menggunakan penyedia identitas kustom	66
Prasyarat	67
Langkah 1: Buat CloudFormation tumpukan	67
Langkah 2: Periksa konfigurasi metode API Gateway untuk server Anda	68
Langkah 3: Lihat detail server Transfer Family	69
Langkah 4: Uji apakah pengguna Anda dapat terhubung ke server	71
Langkah 5: Uji koneksi SFTP dan transfer file	71
Langkah 6: Batasi akses ke ember	72
Perbarui Lambda jika menggunakan Amazon EFS	74
Siapkan konfigurasi AS2	75
Langkah 1: Buat sertifikat untuk AS2	77
Langkah 2: Impor sertifikat sebagai sumber sertifikat Transfer Family	80
Langkah 3: Buat profil untuk Anda dan mitra dagang Anda	82
Langkah 4: Buat server Transfer Family yang menggunakan protokol AS2	83
Langkah 5: Buat kesepakatan antara Anda dan pasangan	86
Langkah 6: Buat konektor antara Anda dan pasangan	88
Langkah 7: Uji pertukaran file melalui AS2 dengan menggunakan Transfer Family	89
Menyiapkan aplikasi web dasar	91
Prasyarat	91
Langkah 1: Buat sumber daya pendukung yang diperlukan	92
Langkah 2: Buat aplikasi web Transfer Family	92
Langkah 3: Konfigurasi berbagi Cross-origin sumber daya (CORS) untuk bucket Anda	93
Langkah 4: Tambahkan pengguna ke aplikasi web Transfer Family	95
Langkah 5: Daftarkan lokasi di Amazon S3 dan buat hibah akses	96
Langkah 6: Akses aplikasi web Transfer Family Anda sebagai pengguna	99
Langkah selanjutnya	100
Integrasikan Okta sebagai penyedia identitas Anda untuk aplikasi web	101
Siapkan aplikasi web dengan akses multi-bucket selektif	103
Prasyarat	103
Langkah 1: Buat aplikasi web Transfer Family	104
Langkah 2: Konfigurasi peran IAM untuk akses S3	105
Langkah 3: Siapkan Hibah Akses S3	107
Langkah 4: Daftarkan lokasi bucket S3	107
Langkah 5: Buat Hibah Akses	108

Langkah 6: Konfigurasi kebijakan CORS untuk bucket S3	108
Langkah 7: Uji konfigurasi	110
Kesimpulan	110
Transfer Family untuk SFTP, FTPS, FTP	111
Opsional penyedia identitas	111
AWS Transfer Family matriks tipe titik akhir	113
Konfigurasi titik akhir server Transfer Family	117
Buat SFTP-enabled server	119
Buat FTPS-enabled server	127
Buat FTP-enabled server	135
Buat server di VPC	144
Bekerja dengan nama host khusus	169
FTP/FTPS Pertimbangan NLB	173
Mentransfer file melalui titik akhir server	173
SFTP/FTPS/FTP Perintah yang Tersedia	176
Temukan titik akhir Amazon VPC Anda	178
Hindari setstat kesalahan	179
Gunakan OpenSSH	37
Gunakan WinSCP	182
Gunakan Cyberduck	36
Gunakan FileZilla	185
Gunakan klien Perl	186
Gunakan LFTP	186
Pemrosesan unggahan pasca	186
Pesan SFTP	188
Mengelola pengguna	190
Amazon EFS vs Amazon S3	191
Direktori logis	192
Kuota grup Direktori Aktif	193
Service-managed pengguna	194
Penyedia identitas khusus	204
Layanan direktori untuk MS AD	242
Layanan direktori untuk Entra ID	253
Gunakan direktori logis	261
Memahami struktur chroot dan direktori	261
Aturan untuk menggunakan direktori logis	262

Menerapkan direktori logis	264
Konfigurasi contoh direktori logis	267
Konfigurasi direktori logis untuk Amazon EFS	269
AWS Lambda Tanggapan khusus	269
Akses fsX untuk sistem file NetApp ONTAP	270
Ikhtisar	271
Prasyarat	272
Bagaimana penyimpanan FSx bekerja dengan Transfer Family	273
Membuat titik akses S3 untuk FSx	274
Menggunakan alias titik akses S3 dengan FSx	276
Mengkonfigurasi Transfer Family untuk penyimpanan FSx	278
Mengelola pengguna untuk penyimpanan FSx	279
Mengkonfigurasi klien transfer file	281
Memecahkan masalah penyimpanan FSx	282
Aplikasi web Transfer Family	284
Wilayah AWS untuk aplikasi web Transfer Family	285
Kompatibilitas browser untuk aplikasi AWS Transfer Family web	285
Cara membuat aplikasi web Transfer Family	285
Konfigurasi penyedia identitas Anda	288
Konfigurasi peran IAM	290
Mengkonfigurasi aplikasi web Transfer Family	293
Membuat aplikasi web Transfer Family	293
Penentuan alamat IP	295
Membuat aplikasi web Transfer Family di VPC	296
Membuat aplikasi web Transfer Family	297
Post-creation langkah	298
Cross-origin kebijakan berbagi sumber daya (CORS)	299
Membatasi akses ke titik akhir VPC kustom	300
Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family	301
Siapkan berbagi Cross-origin sumber daya (CORS) untuk bucket Anda	304
Konfigurasi Hibah Akses Amazon S3	306
Gunakan URL khusus	312
Logging untuk aplikasi web Transfer Family	315
Mengaktifkan peristiwa data Amazon S3	315
Contoh log otentikasi	318
Melihat entri log	325

Memecahkan masalah aplikasi web Anda	326
Memecahkan masalah kesalahan jaringan	326
Memecahkan masalah bucket yang dikonfigurasi tidak muncul	327
Memecahkan masalah kesalahan URL kustom	327
Memecahkan masalah kesalahan lain-lain	328
Bucket S3 duplikat muncul di aplikasi web	329
Instruksi pengguna akhir	330
Kuota aplikasi web	330
Pengguna Pusat Identitas IAM	330
Third-party pengguna akhir	331
Antarmuka pengguna akhir Transfer Family	332
Tindakan yang tersedia	333
Konektor SFTP	335
Membuat konektor SFTP	335
Memilih jenis jalan keluar konektor SFTP	336
Memilih mode pengalamatan IP	337
Simpan kredensial di Secrets Manager	338
Buat konektor SFTP dengan jalan keluar yang dikelola layanan	340
Buat konektor SFTP dengan jalan keluar VPC-based	350
Uji konektor SFTP	361
Konektivitas VPC	363
Menggunakan konektor SFTP	364
Transfer file	364
Daftar isi direktori jarak jauh	366
Memindahkan dan menghapus file di server jauh	368
Memantau konektor SFTP	370
Gunakan API konektor untuk menanyakan status permintaan transfer file	370
Lihat acara konektor SFTP di Amazon EventBridge	371
Lihat log konektor SFTP di Amazon CloudWatch	371
Memantau konektor tipe jalan keluar VPC	371
Mengelola konektor SFTP	373
Perbarui konektor SFTP	374
Lihat detail konektor SFTP	375
Kuota untuk konektor SFTP	376
Kuota untuk konektor SFTP	376
Menskalakan konektor SFTP Anda	377

Arsitektur referensi	378
Unggahan blog	379
Lokakarya	379
Solusi	379
Arsitektur referensi VPC	380
Transfer Family untuk AS2	382
Kasus penggunaan AS2	383
Template AS2 CloudFormation	388
Menyesuaikan Templat AS2	388
Menguji penerapan AS2 Anda	389
Praktik terbaik untuk penerapan template AS2	389
Konfigurasikan AS2	390
Konfigurasi AS2	391
Kuota AS2	393
Fitur dan kemampuan AS2	396
Kelola sertifikat AS2	398
Impor sertifikat AS2	398
Rotasi sertifikat AS2	400
Buat profil AS2	402
Buat server AS2	403
Membuat server AS2 menggunakan konsol Transfer Family	404
Buat server AS2 menggunakan template	407
Buat perjanjian AS2	410
Konfigurasikan konektor AS2	412
Buat konektor AS2	413
Algoritma konektor AS2	416
Otentikasi dasar untuk konektor AS2	417
Aktifkan otentikasi dasar untuk konektor AS2	418
Lihat detail konektor	421
Transfer pesan AS2	424
Terima pesan AS2	425
Konfigurasikan HTTPS untuk AS2	426
Transfer file dengan konektor AS2	432
Nama dan lokasi file	434
Kode status	437
Contoh file JSON	438

Kustom HTTP Header untuk AS2	440
Gambaran Umum Templat	440
Cara Kerjanya	441
Fitur Utama	441
Detail Implementasi	441
Penerapan dan Penggunaan	442
Monitor AS2	443
Kode Status AS2	445
Kode kesalahan AS2	446
Pemantauan kedaluwarsa sertifikat	459
DaysUntilExpiry metrik	459
Praktik terbaik untuk pemantauan sertifikat	460
Contoh konfigurasi alarm	460
Mengelola alur kerja pemrosesan file	462
Buat alur kerja	464
Konfigurasi dan jalankan alur kerja	465
Lihat detail alur kerja	468
Gunakan langkah-langkah yang telah ditentukan	471
Salin berkas	471
Dekripsi file	476
Berkas tag	482
Hapus berkas	483
Variabel bernama untuk alur kerja	484
Contoh tag dan hapus alur kerja	484
Gunakan langkah-langkah pemrosesan file khusus	489
Menggunakan beberapa fungsi Lambda secara berurutan	491
Mengakses file setelah pemrosesan kustom	491
Contoh peristiwa dikirim ke AWS Lambda saat file upload	492
Contoh fungsi Lambda untuk langkah alur kerja khusus	493
Izin IAM untuk langkah khusus	494
Kebijakan IAM untuk alur kerja	495
Hubungan kepercayaan alur kerja	497
Contoh peran eksekusi: Dekripsi, salin, dan tag	497
Contoh peran eksekusi: Jalankan fungsi dan hapus	499
Penanganan pengecualian untuk alur kerja	500
Pantau eksekusi alur kerja	501

CloudWatch logging untuk alur kerja	501
CloudWatch metrik untuk alur kerja	504
Buat alur kerja dari template	504
Menghapus alur kerja dari server Transfer Family	508
Pembatasan dan batasan	509
Mengelola server	512
Lihat daftar server	512
Hapus server	513
Lihat detail server SFTP	514
Lihat detail server AS2	515
Dukungan IPv6	517
Keterbatasan IPv6	517
Mengkonfigurasi IPv6 untuk server	518
Gunakan ALB untuk server publik AS2 dual-stack	518
Edit detail server	520
Edit protokol transfer file	523
Edit titik akhir server	525
Edit pencatatan	526
Edit kebijakan keamanan	527
Mengubah alur kerja terkelola	529
Ubah spanduk tampilan untuk server Anda	530
Menempatkan server Anda secara online atau offline	530
Edit konfigurasi penyedia identitas	531
Mengubah ke penyedia identitas yang dikelola layanan	532
Mengubah ke AWS Directory Service	532
Mengubah ke penyedia identitas khusus	532
Pelestarian pengguna selama transisi penyedia identitas	537
Pertimbangan penting saat mengganti penyedia identitas	537
Kelola kunci host server	537
Kapan harus mengimpor kunci host	539
Tambahkan kunci host server tambahan	539
Hapus kunci host server	541
Putar kunci host server	542
Informasi kunci host server tambahan	544
Pantau penggunaan dalam konsol	544
Mengelola kontrol akses	551

Membuat kebijakan akses bucket S3	552
Membuat kebijakan sesi	553
Contoh kebijakan sesi	554
Substitusi bersarang untuk kebijakan sesi	557
Manajemen izin dinamis	557
Memahami arsitektur izin Transfer Family	557
Dua pendekatan untuk manajemen izin	558
Menerapkan kebijakan sesi	559
Implementasi menurut tipe pengguna	560
Contoh: Menyederhanakan manajemen peran dengan kebijakan sesi	560
CloudTrail penebangan	564
Mengaktifkan pencatatan CloudTrail	566
Mengaktifkan peristiwa data Amazon S3	566
Contoh entri log untuk membuat server	567
Log akses data	568
Contoh entri log untuk akses data yang berhasil	568
Operasi akses data umum	571
CloudWatch penebangan	572
Jenis CloudWatch pencatatan untuk Transfer Family	572
Membuat logging untuk server	574
Membuat logging untuk server	577
Memperbarui logging untuk server	578
Melihat konfigurasi server	581
Mengelola logging untuk alur kerja	583
Mengkonfigurasi peran untuk CloudWatch	586
Melihat aliran log Transfer Family	588
Membuat CloudWatch alarm Amazon	592
Logging panggilan API S3 ke log akses S3	593
Contoh untuk membatasi masalah wakil yang membingungkan	593
CloudWatch struktur log untuk Transfer Family	595
Log terstruktur JSON untuk Transfer Family	595
Log lama untuk Transfer Family	598
Contoh entri CloudWatch log	601
Contoh entri log sesi transfer	602
Contoh entri log untuk konektor SFTP	603
Contoh entri log untuk konektor VPC Lattice	605

Contoh entri log untuk kegagalan algoritma pertukaran Kunci	606
Menggunakan CloudWatch metrik	607
Dimensi Transfer Family	611
Notifikasi pengguna	612
CloudWatch kueri	612
Mengelola acara menggunakan EventBridge	615
Transfer Family peristiwa	616
Acara server SFTP, FTPS, dan FTP	616
Acara konektor SFTP	619
Acara AS2	620
Mengirim Transfer Family acara	621
Membuat pola peristiwa	623
Menguji pola acara untuk Transfer Family acara	624
Izin	624
Sumber daya tambahan	624
Referensi detail acara	625
Acara server	626
Acara konektor	633
Acara AS2	640
Keamanan	646
Manfaat keamanan konektivitas VPC	647
Model keamanan VPC Lattice	647
Praktik terbaik keamanan untuk konektivitas VPC	648
Kebijakan keamanan untuk server	648
Algoritma kriptografi	650
Detail kebijakan keamanan	661
Kebijakan keamanan untuk konektor SFTP	679
Algoritma kriptografi	679
Rincian kebijakan keamanan konektor SFTP	680
Post-Quantum kebijakan keamanan	682
Tentang pertukaran kunci hibrida pasca-kuantum di SSH	683
Cara menggunakannya	683
Bagaimana cara mengujinya	685
Perlindungan data	688
Enkripsi data di Transfer Family	689
Enkripsi saat diam	691

Manajemen kunci	692
Ikhtisar algoritma	692
Otentikasi SSH	693
Algoritma PGP	694
Hasilkan kunci SSH	695
Putar tombol SSH	701
Hasilkan kunci PGP	704
Kelola kunci PGP	705
Klien PGP yang didukung	709
Manajemen identitas dan akses	710
Audiens	711
Mengautentikasi dengan identitas	711
Mengelola akses menggunakan kebijakan	713
Bagaimana AWS Transfer Family bekerja dengan IAM	715
Identity-based contoh kebijakan	719
Tag-based contoh kebijakan	722
Pemecahan masalah identitas dan akses	726
Kunci kondisi IAM	728
Validasi kepatuhan	730
Ketahanan	731
Titik akhir VPC untuk API	732
Mengontrol akses menggunakan kebijakan titik akhir VPC	732
Buat titik akhir VPC	733
Keamanan infrastruktur	733
Pertimbangan NLB dan NAT	734
Keamanan infrastruktur konektivitas VPC	735
Firewall aplikasi web	736
Cross-service pencegahan wakil bingung	738
Peran pengguna Transfer Family	739
Peran alur kerja Transfer Family	741
Peran konektor Transfer Family	742
logging/invocationPeran Transfer Family	744
AWS kebijakan terkelola	745
AWSTransferConsoleFullAccess	746
AWSTransferFullAccess	746
AWSTransferLoggingAccess	746

AWSTransferReadOnlyAccess	746
Pembaruan kebijakan	747
Modul Transfer Family Terraform	748
Server SFTP	748
Konektor SFTP	748
AS2	749
Pertukaran Data B2B	749
Pemecahan Masalah Transfer Family	750
Masalah otentikasi	750
Kegagalan otentikasi— SSH/SFTP	751
Masalah alam tidak cocok AD terkelola	751
Batas grup Active Directory terlampaui	752
Masalah otentikasi lain-lain	752
Memecahkan masalah Amazon API Gateway	753
Memecahkan masalah pengujian penyedia identitas Anda	755
Duplikat bucket Amazon S3 di aplikasi web	329
Masalah konektor SFTP	756
Memecahkan masalah menambahkan kunci host tepercaya untuk konektor SFTP Anda	756
Negosiasi kunci gagal	757
Pelambatan konektor SFTP	757
Mengoptimalkan kinerja konektor SFTP	758
Memecahkan masalah konektivitas VPC	759
Masalah konektor SFTP lain-lain	762
Masalah konektivitas SFTP	762
Memecahkan masalah konektivitas SFTP	763
Memecahkan masalah klien SFTP	763
Memecahkan masalah pengunggahan file	763
Memecahkan masalah konektor SFTP tipe jalan keluar VPC	765
Masalah penyedia identitas khusus	767
Memecahkan masalah kesalahan integrasi API Gateway	767
Memecahkan masalah batas waktu fungsi Lambda	768
Memecahkan masalah batas waktu Lambda yang konsisten	769
Memecahkan masalah pengecualian <code>KeyError</code>	770
Masalah alur kerja	770
Memecahkan masalah alur kerja terkelola	770
Memecahkan masalah dekripsi alur kerja	773

Masalah EFS	777
Memecahkan masalah Amazon EFS	777
Masalah penyimpanan dan enkripsi	779
Memecahkan masalah kebijakan untuk bucket Amazon S3 terenkripsi	780
Memecahkan masalah pengecualian ResourceNotFound	780
Memantau dan memperingatkan masalah	781
Memecahkan masalah metrik yang hilang atau tidak lengkap CloudWatch	781
Memecahkan masalah peristiwa yang hilang EventBridge	782
Cross-region masalah transfer	783
Memecahkan masalah izin transfer lintas wilayah	783
Memecahkan masalah performa transfer lintas wilayah	785
Masalah penerapan Terraform	786
Memecahkan masalah kegagalan pembuatan sumber daya Terraform	786
Memecahkan masalah manajemen status Terraform	787
Masalah integrasi WAF	788
Memecahkan masalah WAF memblokir lalu lintas yang sah	788
Memecahkan masalah integrasi WAF dengan penyedia identitas khusus	789
Service-managed masalah pengguna	790
Memecahkan masalah pengguna yang dikelola layanan	790
Masalah AS2	791
Memecahkan masalah AS2	792
Masalah sertifikat AS2	792
Masalah penerimaan AS2 MDN	792
Masalah pemantauan kedaluwarsa sertifikat	793
Referensi API	795
Membuat permintaan API	796
Transfer Family membutuhkan header permintaan	797
Transfer Family meminta masukan dan penandatanganan	797
Tanggapan kesalahan	798
Pustaka yang tersedia	800
Penyedia Identitas	800
Kesepakatan	802
Format ID	802
Format ARN	802
DNS dan Endpoint	803
Titik Akhir API	804

Titik Akhir Server	804
Riwayat dokumen	806
.....	dcccxxiii

Apa itu AWS Transfer Family?

AWS Transfer Family adalah layanan transfer aman yang memungkinkan Anda mentransfer file masuk dan keluar dari layanan AWS penyimpanan. Transfer Family adalah bagian dari AWS Cloud platform. AWS Transfer Family menawarkan dukungan yang dikelola sepenuhnya untuk transfer file melalui SFTP, AS2, FTPS, FTP, dan transfer berbasis browser web langsung masuk dan keluar dari layanan penyimpanan. AWS Anda dapat memigrasi, mengotomatisasi, dan memantau alur kerja transfer file dengan mempertahankan konfigurasi sisi klien yang ada untuk autentikasi, akses, dan firewall—sehingga tidak ada perubahan bagi pelanggan, mitra, dan tim internal Anda, atau aplikasi mereka. Lihat [Memulai AWS](#) untuk mempelajari lebih lanjut dan mulai membangun aplikasi cloud dengan Amazon Web Services.

AWS Transfer Family mendukung transfer data dari atau ke layanan AWS penyimpanan berikut.

- Penyimpanan Amazon Simple Storage Service (Amazon S3). Untuk informasi tentang Amazon S3, lihat [Memulai Layanan Penyimpanan Sederhana Amazon](#).
- Sistem file Sistem File Jaringan Amazon Elastic File System (Amazon EFS) (NFS). Untuk informasi tentang Amazon EFS, lihat [Apa itu Amazon Elastic File System?](#)

AWS Transfer Family mendukung transfer data melalui protokol berikut:

- Protokol Transfer File Aman (SFTP): versi 3

Dokumen IETF resmi ada di sini: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Protokol Transfer File Aman (FTPS)
- Protokol Transfer File (FTP)
- Pernyataan Penerapan 2 (AS2)
- Browser-based transfer

Note

Untuk koneksi data FTP dan FTPS, rentang port yang digunakan Transfer Family untuk membuat saluran data adalah 8192-8200.

Protokol transfer file digunakan dalam alur kerja pertukaran data di berbagai industri seperti layanan keuangan, perawatan kesehatan, periklanan, dan ritel, antara lain. Transfer Family menyederhanakan migrasi alur kerja transfer file ke AWS.

Berikut ini adalah beberapa kasus penggunaan umum untuk menggunakan Transfer Family dengan Amazon S3:

- Data digunakan AWS untuk diunggah dari pihak ketiga seperti vendor dan mitra.
- Subscription-based distribusi data dengan pelanggan Anda.
- Transfer internal dalam organisasi Anda.

Berikut ini adalah beberapa kasus penggunaan umum untuk menggunakan Transfer Family dengan Amazon EFS:

- Distribusi data
- Rantai pasokan
- Manajemen konten
- Aplikasi penyajian web

Berikut ini adalah beberapa kasus penggunaan umum untuk menggunakan Transfer Family dengan AS2:

- Alur kerja dengan persyaratan kepatuhan yang bergantung pada perlindungan data dan fitur keamanan yang dibangun ke dalam protokol
- Logistik rantai pasokan
- Alur kerja pembayaran
- Business-to-business (B2B) transaksi
- Integrasi dengan sistem perencanaan sumber daya perusahaan (ERP) dan manajemen hubungan pelanggan (CRM)

Berikut ini adalah beberapa kasus penggunaan umum untuk menggunakan aplikasi web Transfer Family:

- Akses yang disederhanakan ke data di Amazon S3 ke berbagai pengguna bisnis yang lebih luas dan beragam

- Manajemen akses data terpusat untuk tenaga kerja Anda
- Visualisasi Hibah Akses Amazon S3 melalui antarmuka yang dikelola

Dengan Transfer Family, Anda mendapatkan akses ke server yang mendukung protokol transfer file di AWS (atau antarmuka web transfer file terkelola), tanpa perlu menjalankan infrastruktur server apa pun. Anda dapat menggunakan layanan ini untuk memigrasikan alur kerja berbasis transfer file AWS sambil mempertahankan klien dan konfigurasi pengguna akhir Anda apa adanya. Untuk server, pertama-tama Anda mengaitkan nama host Anda dengan titik akhir server, lalu tambahkan pengguna Anda dan berikan mereka tingkat akses yang tepat. Setelah Anda melakukan ini, permintaan transfer pengguna Anda dilayani langsung dari titik akhir server Transfer Family Anda.

Untuk aplikasi web Transfer Family, tentukan setelan konfigurasi Anda dan terapkan penyesuaian opsional. Setelah Anda melakukan ini, pengguna Anda dapat masuk dan langsung mentransfer data ke dan dari Amazon S3.

Transfer Family memberikan manfaat sebagai berikut:

- Layanan terkelola penuh yang menskalakan secara real time untuk memenuhi kebutuhan Anda.
- Anda tidak perlu memodifikasi aplikasi Anda atau menjalankan infrastruktur protokol transfer file apa pun.
- Dengan data Anda dalam penyimpanan Amazon S3 yang tahan lama, Anda dapat menggunakan native Layanan AWS untuk fungsi pemrosesan, analitik, pelaporan, audit, dan arsip.
- Dengan Amazon EFS sebagai penyimpanan data, Anda mendapatkan sistem file elastis yang dikelola sepenuhnya untuk digunakan dengan AWS Cloud layanan dan sumber daya lokal. Amazon EFS dibangun untuk menskalakan sesuai permintaan ke petabyte tanpa mengganggu aplikasi, tumbuh dan menyusut secara otomatis saat Anda menambahkan dan menghapus file. Ini membantu menghilangkan kebutuhan untuk menyediakan dan mengelola kapasitas untuk mengakomodasi pertumbuhan.
- Layanan Alur Kerja Transfer File tanpa server yang dikelola sepenuhnya yang memudahkan untuk mengatur, menjalankan, mengotomatisasi, dan memantau pemrosesan file yang diunggah menggunakan. AWS Transfer Family
- Tidak ada biaya di muka, dan Anda hanya membayar untuk penggunaan layanan.

Di bagian berikut, Anda dapat menemukan deskripsi tentang berbagai fitur Transfer Family, tutorial memulai, petunjuk terperinci tentang cara mengatur berbagai server yang diaktifkan protokol, cara menggunakan berbagai jenis penyedia identitas, dan referensi API layanan.

Untuk memulai Transfer Family, lihat berikut ini:

- [Bagaimana cara AWS Transfer Family kerja](#)
- [Prasyarat](#)
- [Memulai dengan AWS Transfer Family titik akhir server](#)
- [Aplikasi web Transfer Family](#)

Bagaimana cara AWS Transfer Family kerja

AWS Transfer Family adalah AWS layanan terkelola penuh yang dapat Anda gunakan untuk mentransfer file masuk dan keluar dari penyimpanan Amazon Simple Storage Service (Amazon S3) atau sistem file Amazon Elastic File System (Amazon EFS) melalui protokol atau browser web berikut:

- Protokol Transfer File Aman (SFTP): versi 3

Dokumen IETF resmi ada di sini: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Protokol Transfer File Aman (FTPS)
- Protokol Transfer File (FTP)
- Pernyataan Penerapan 2 (AS2)
- Browser-based transfer

AWS Transfer Family mendukung hingga 3 Availability Zones dan didukung oleh auto scaling, armada redundan untuk koneksi Anda dan permintaan transfer. Untuk contoh tentang cara membangun redundansi yang lebih tinggi dan meminimalkan latensi jaringan dengan menggunakan Latency-based perutean, lihat posting blog [Minimalkan latensi jaringan dengan transfer Anda AWS](#) untuk server SFTP.

Transfer Family Managed File Transfer Workflows (MFTW) adalah layanan Alur Kerja Transfer File tanpa server yang dikelola sepenuhnya yang memudahkan untuk mengatur, menjalankan, mengotomatisasi, dan memantau pemrosesan file yang diunggah menggunakan AWS Transfer Family. Pelanggan dapat menggunakan MFTW untuk mengotomatiskan berbagai langkah pemrosesan seperti menyalin, menandai, memindai, memfilter compressing/decompressing, dan data yang ditransfer menggunakan Transfer encrypting/decrypting Family. Ini memberikan visibilitas ujung ke ujung untuk pelacakan dan auditabilitas. Untuk detail selengkapnya, lihat [AWS Transfer Family alur kerja terkelola](#).

AWS Transfer Family mendukung klien protokol transfer file standar apa pun. Beberapa klien yang umum digunakan adalah sebagai berikut:

- [OpenSSH](#) — Utilitas baris perintah Macintosh dan Linux.
- [WinSCP](#) — Windows-only Klien grafis.
- [Cyberduck](#) — Klien grafis Linux, Macintosh, dan Microsoft Windows.
- [FileZilla](#) — Klien grafis Linux, Macintosh, dan Windows.

AWS menawarkan lokakarya Transfer Family berikut.

- Buat solusi transfer file yang memanfaatkan SFTP/FTPS titik akhir terkelola dan Amazon Cognito dan DynamoDB AWS Transfer Family untuk manajemen pengguna. Anda dapat melihat detail untuk lokakarya ini [di sini](#).
- [Buat endpoint Transfer Family dengan AS2 diaktifkan, dan konektor Transfer Family AS2 Anda dapat melihat detail untuk lokakarya ini di sini.](#)
- Buat solusi yang memberikan panduan preskriptif dan lab langsung tentang bagaimana Anda dapat membangun arsitektur transfer file yang terukur dan aman AWS tanpa perlu memodifikasi aplikasi yang ada atau mengelola infrastruktur server. Anda dapat melihat detail untuk lokakarya ini [di sini](#).

Posting blog yang relevan untuk Transfer Family

Tabel berikut mencantumkan posting blog yang berisi informasi berguna bagi pelanggan Transfer Family. Tabel dalam urutan kronologis terbalik, sehingga posting terbaru ada di awal tabel.

Judul dan tautan posting blog	Date
Terapkan Okta sebagai penyedia identitas khusus untuk AWS Transfer Family	Agustus 11, 2025
Mengotomatiskan pemrosesan klaim perawatan kesehatan kertas-ke-elektronik dengan AWS	29 Mei 2025
Cara menggunakan AWS Transfer Family dan GuardDuty untuk perlindungan malware	April 30, 2025

Judul dan tautan posting blog	Date
Bagaimana FICO memodernisasi transfer file dengan otomatisasi ETL menggunakan AWS Transfer Family	April 24, 2025
Mengumumkan aplikasi AWS Transfer Family web untuk transfer file Amazon S3 yang dikelola sepenuhnya	Desember 1, 2024
Enam tips untuk meningkatkan keamanan AWS Transfer Family server Anda	September 24, 2024
Sederhanakan otentikasi Active Directory dengan penyedia identitas khusus untuk AWS Transfer Family	Agustus 12, 2024
Merancang transfer file terkelola yang aman dan sesuai dengan konektor AWS Transfer Family SFTP dan enkripsi PGP	16 Mei 2024
Menggunakan Amazon Cognito sebagai penyedia identitas dengan AWS Transfer Family dan Amazon S3	14 Mei 2024
Bagaimana Transfer Family dapat membantu Anda membangun solusi transfer file terkelola yang aman dan sesuai	Januari 3, 2024
Mendeteksi ancaman malware menggunakan AWS Transfer Family	Juli 20, 2023
Memperluas beban kerja SAP dengan AWS Transfer Family	13 Juli 2023
Enkripsi dan dekripsi file dengan PGP dan AWS Transfer Family	Juni 21, 2023

Judul dan tautan posting blog	Date
Mengautentikasi AWS Transfer Family dengan Azure Active Directory dan AWS Lambda	15 Desember 2022
Sesuaikan pemberitahuan pengiriman file menggunakan alur kerja AWS Transfer Family terkelola	14 Oktober 2022
Membangun platform transfer file cloud-native menggunakan alur kerja AWS Transfer Family	5 Januari 2022
Mengaktifkan manajemen kunci swalayan pengguna dengan A AWS Transfer Family dan AWS Lambda	Desember 17, 2021
Tingkatkan kontrol akses data dengan AWS Transfer Family dan Amazon S3	5 Oktober 2021
Meningkatkan throughput untuk pengguna n AWS Global Accelerator dan AWS Transfer Family layanan transfer file yang dihadapi internet	7 Juni 2021
Mengamankan AWS Transfer Family dengan Firewall Aplikasi AWS Web dan Amazon API Gateway	5 Mei 2021
Mengamankan AWS Transfer Family dengan Firewall Aplikasi AWS Web dan Amazon API Gateway	15 Januari 2021
AWS Transfer Family dukungan untuk Amazon Elastic File System	7 Januari 2021
Aktifkan otentikasi kata sandi untuk menggunakan AWS Transfer FamilyAWS Secrets Manager	5 November 2020

Judul dan tautan posting blog	Date
Memusatkan akses data menggunakan AWS Transfer Family dan AWS Storage Gateway	22 Juni 2020
Menggunakan Amazon EFS untuk AWS Lambda aplikasi tanpa server Anda	18 Juni 2020
Gunakan daftar izin IP untuk mengamankan AWS Transfer Family server Anda	8 April 2020
Minimalkan latensi jaringan dengan AWS transfer Anda untuk server SFTP	19 Februari 2020
Angkat dan Pergeseran migrasi server SFTP ke AWS	12 Februari 2020
Sederhanakan Struktur AWS SFTP Anda dengan direktori chroot dan logis	26 September 2019
Menggunakan Okta sebagai penyedia identitas dengan AWS Transfer Family	30 Mei 2019

Prasyarat

Bagian berikut menjelaskan prasyarat yang diperlukan untuk menggunakan layanan ini. AWS Transfer Family Minimal, Anda perlu membuat bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dan menyediakan akses ke bucket tersebut melalui AWS Identity and Access Management peran (IAM). Peran Anda juga perlu membangun hubungan kepercayaan. Hubungan kepercayaan ini memungkinkan Transfer Family untuk mengambil peran IAM untuk mengakses bucket Anda sehingga dapat melayani permintaan transfer file pengguna Anda.

Untuk informasi tentang dukungan IPv6 untuk AWS Transfer Family server, lihat [Dukungan IPv6 untuk server Transfer Family](#) di bagian Mengelola server.

Topik

- [AWS Wilayah, titik akhir, dan kuota yang didukung untuk server Transfer Family](#)
- [Mendaftar untuk AWS](#)
- [Konfigurasi penyimpanan untuk digunakan dengan AWS Transfer Family server](#)
- [Buat peran dan kebijakan IAM](#)

AWS Wilayah, titik akhir, dan kuota yang didukung untuk server Transfer Family

Untuk terhubung secara terprogram ke AWS layanan, Anda menggunakan titik akhir. Misalnya, titik akhir untuk pelanggan di wilayah AS Timur (Ohio) (us-east-2), adalah `transfer.us-east-2.amazonaws.com`. Kuota layanan, juga disebut sebagai batas, adalah jumlah maksimum sumber daya layanan atau operasi untuk Anda Akun AWS. Dalam panduan ini, Anda dapat menemukan kuota di [Kuota AS2](#) dan [Kuota untuk konektor SFTP](#).

Untuk informasi selengkapnya tentang AWS Wilayah, titik akhir, dan kuota layanan yang didukung, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum Amazon Web

Untuk aplikasi web Transfer Family, wilayah yang didukung dicantumkan [Wilayah AWS untuk aplikasi web Transfer Family](#). Untuk kuota yang berkaitan dengan aplikasi web Transfer Family, lihat. [Kuota aplikasi web](#)

Mendaftar untuk AWS

Saat Anda mendaftar ke Amazon Web Services (AWS), AWS akun Anda secara otomatis mendaftar untuk semua layanan AWS, termasuk AWS Transfer Family. Anda hanya membayar biaya layanan yang Anda gunakan.

Jika Anda sudah memiliki AWS akun, lompat ke tugas berikutnya. Jika Anda belum memiliki akun AWS, gunakan prosedur berikut untuk membuatnya.

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/signup>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

Untuk informasi tentang harga dan penggunaan AWS Kalkulator Harga untuk mendapatkan perkiraan biaya penggunaan Transfer Family, lihat [AWS Transfer Family harga](#).

Untuk informasi tentang ketersediaan AWS Wilayah, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS

Konfigurasi penyimpanan untuk digunakan dengan AWS Transfer Family server

Topik ini menjelaskan opsi penyimpanan yang dapat Anda gunakan AWS Transfer Family. Anda dapat menggunakan Amazon S3 atau Amazon EFS sebagai penyimpanan untuk server Transfer Family Anda.

Daftar Isi

- [Konfigurasi bucket Amazon S3](#)
 - [Titik akses Amazon S3](#)
 - [Perilaku Amazon S3 HeadObject](#)
 - [Memberikan kemampuan untuk hanya menulis dan membuat daftar file](#)
 - [Sejumlah besar objek nol-byte menyebabkan masalah latensi](#)
- [Konfigurasi sistem file Amazon EFS](#)
 - [Kepemilikan file Amazon EFS](#)
 - [Menyiapkan pengguna Amazon EFS untuk Transfer Family](#)
 - [Konfigurasi pengguna Transfer Family di Amazon EFS](#)
 - [Buat pengguna root Amazon EFS](#)
 - [Perintah Amazon EFS yang didukung](#)

Konfigurasi bucket Amazon S3

AWS Transfer Family mengakses bucket Amazon S3 untuk melayani permintaan transfer pengguna, jadi Anda perlu menyediakan bucket Amazon S3 sebagai bagian dari pengaturan server yang mendukung protokol transfer file. Anda dapat menggunakan bucket yang sudah ada, atau Anda dapat membuat yang baru.

Note

Anda tidak harus menggunakan server dan bucket Amazon S3 yang berada di AWS Wilayah yang sama, tetapi kami merekomendasikan ini sebagai praktik terbaik.

Saat Anda mengatur pengguna, Anda menetapkan masing-masing peran IAM kepada mereka. Peran ini menentukan tingkat akses yang mereka miliki ke bucket Amazon S3 Anda.

Untuk informasi tentang cara membuat bucket baru, lihat [Bagaimana cara membuat bucket S3?](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Note

Anda dapat menggunakan Amazon S3 Object Lock untuk mencegah objek ditimpa untuk jangka waktu yang tetap atau tanpa batas waktu. Ini bekerja dengan cara yang sama dengan

Transfer Family seperti layanan lainnya. Jika suatu objek ada dan dilindungi, menulis ke file itu atau menghapusnya tidak diperbolehkan. Untuk detail selengkapnya tentang Kunci Objek Amazon S3, lihat [Menggunakan Kunci Objek Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

Titik akses Amazon S3

AWS Transfer Family mendukung [Poin Akses Amazon S3](#), fitur Amazon S3 yang memungkinkan Anda mengelola akses granular ke kumpulan data bersama dengan mudah. Anda dapat menggunakan alias S3 Access Point di mana pun Anda menggunakan nama bucket S3. Anda dapat membuat ratusan titik akses di Amazon S3 untuk pengguna yang memiliki izin berbeda untuk mengakses data bersama di bucket Amazon S3.

Misalnya, Anda dapat menggunakan titik akses untuk memungkinkan tiga tim berbeda memiliki akses ke kumpulan data bersama yang sama di mana satu tim dapat membaca data dari S3, tim kedua dapat menulis data ke S3, dan tim ketiga dapat membaca, menulis, dan menghapus data dari S3. Untuk menerapkan kontrol akses granular seperti yang disebutkan di atas, Anda dapat membuat titik akses S3 yang berisi kebijakan yang memberikan akses asimetris ke tim yang berbeda. Anda dapat menggunakan titik akses S3 dengan server Transfer Family Anda untuk mencapai kontrol akses yang halus, tanpa membuat kebijakan bucket S3 kompleks yang mencakup ratusan kasus penggunaan. Untuk mempelajari lebih lanjut tentang cara menggunakan titik akses S3 dengan server Transfer Family, lihat [Tingkatkan kontrol akses data dengan AWS Transfer Family dan posting blog Amazon S3](#).

Note

AWS Transfer Family saat ini tidak mendukung Poin Multi-Region Akses Amazon S3.

Perilaku Amazon S3 HeadObject

Note

Saat membuat atau memperbarui server Transfer Family, Anda dapat mengoptimalkan kinerja untuk direktori Amazon S3, yang menghilangkan panggilan. HeadObject

Di Amazon S3, bucket dan objek adalah sumber daya utama, dan objek disimpan dalam bucket. Amazon S3 dapat meniru sistem file hierarkis, tetapi terkadang dapat berperilaku berbeda dari sistem file biasa. Misalnya, direktori bukan konsep kelas satu di Amazon S3 tetapi didasarkan pada kunci objek. AWS Transfer Family menyimpulkan jalur direktori dengan memisahkan kunci objek dengan karakter garis miring maju (/), memperlakukan elemen terakhir sebagai nama file, lalu mengelompokkan nama file yang memiliki awalan yang sama bersama-sama di bawah jalur yang sama. Zero-byte objek dibuat untuk mewakili jalur folder saat Anda membuat direktori kosong menggunakan `mkdir` atau dengan menggunakan konsol Amazon S3. Kunci untuk benda-benda ini berakhir dengan garis miring ke depan. Objek nol-byte ini dijelaskan dalam [Mengatur objek di konsol Amazon S3 menggunakan folder di Panduan Pengguna Amazon S3](#).

Saat Anda menjalankan `ls` perintah, dan beberapa hasilnya adalah objek zero-byte Amazon S3 (objek ini memiliki kunci yang diakhiri dengan karakter garis miring ke depan), Transfer Family mengeluarkan `HeadObject` permintaan untuk masing-masing objek ini (lihat di Referensi API Layanan Penyimpanan Sederhana Amazon untuk [HeadObject](#) detailnya). Hal ini dapat mengakibatkan masalah berikut saat menggunakan Amazon S3 sebagai penyimpanan Anda dengan Transfer Family.

Memberikan kemampuan untuk hanya menulis dan membuat daftar file

Dalam beberapa kasus, Anda mungkin hanya ingin menawarkan akses tulis ke objek Amazon S3 Anda. Misalnya, Anda mungkin ingin menyediakan akses untuk menulis (atau mengunggah) dan mencantumkan objek dalam ember, tetapi tidak untuk membaca (mengunduh) objek. Untuk melakukan `ls` dan `mkdir` memerintahkan dengan menggunakan klien transfer file, Anda harus memiliki Amazon S3 `ListObjects` dan `PutObject` izin. Namun, ketika Transfer Family perlu melakukan `HeadObject` panggilan untuk menulis atau membuat daftar file, panggilan gagal dengan kesalahan Akses ditolak, karena panggilan ini memerlukan `GetObject` izin.

Note

Saat membuat atau memperbarui server Transfer Family, Anda dapat mengoptimalkan kinerja untuk direktori Amazon S3, yang menghilangkan panggilan `HeadObject`

Dalam hal ini, Anda dapat memberikan akses dengan menambahkan kondisi kebijakan AWS Identity and Access Management (IAM) yang menambahkan `GetObject` izin hanya untuk objek yang diakhiri dengan garis miring (/). Kondisi ini mencegah `GetObject` panggilan pada file (sehingga tidak dapat dibaca), tetapi memungkinkan pengguna untuk membuat daftar dan melintasi folder.

Kebijakan contoh berikut hanya menawarkan akses tulis dan daftar ke bucket Amazon S3 Anda. Untuk menggunakan kebijakan ini, ganti *amzn-s3-demo-bucket* dengan nama bucket Anda.

 Note

Untuk mengatasi perilaku upload WinSCP, pastikan untuk menambahkan "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart" baris seperti yang tercantum dalam contoh kebijakan berikut. Baris ini memastikan penanganan objek .filepart yang tepat untuk mencegah kegagalan.

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

```
    ]  
  }  
]  
}
```

Note

Kebijakan ini tidak mengizinkan pengguna untuk menambahkan file. Dengan kata lain, pengguna yang diberi kebijakan ini tidak dapat membuka file untuk menambahkan konten ke dalamnya, atau memodifikasinya. Selain itu, jika kasus penggunaan Anda memerlukan `HeadObject` panggilan sebelum mengunggah file, kebijakan ini tidak akan berfungsi untuk Anda.

Sejumlah besar objek nol-byte menyebabkan masalah latensi

Jika bucket Amazon S3 Anda berisi sejumlah besar objek nol-byte ini, Transfer Family mengeluarkan banyak panggilan, yang dapat mengakibatkan `HeadObject` penundaan pemrosesan. Solusi yang disarankan untuk masalah ini adalah mengaktifkan Direktori yang Dioptimalkan untuk mengurangi latensi.

Misalnya, Anda masuk ke direktori home Anda, dan Anda memiliki 10.000 subdirektori. Dengan kata lain, bucket Amazon S3 Anda memiliki 10.000 folder. Dalam skenario ini, jika Anda menjalankan perintah `ls` (daftar), operasi daftar memakan waktu antara enam dan delapan menit. Namun, jika Anda mengoptimalkan direktori Anda, operasi ini hanya membutuhkan beberapa detik. Anda mengatur opsi ini di layar Konfigurasi detail tambahan selama pembuatan server atau prosedur pembaruan. Prosedur-prosedur ini dirinci di bawah [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#) topik.

Note

Klien GUI dapat mengeluarkan `ls` perintah di luar kendali Anda, jadi penting untuk mengaktifkan pengaturan ini jika Anda bisa.

Jika Anda tidak atau tidak dapat mengoptimalkan direktori Anda, solusi alternatif untuk masalah ini adalah menghapus semua objek zero-byte Anda. Perhatikan hal-hal berikut:

- Direktori kosong tidak akan ada lagi. Direktori hanya ada karena nama mereka berada di kunci suatu objek.
- Tidak mencegah seseorang menelepon `mkdir` dan merusak semuanya lagi. Anda dapat mengurangi ini dengan membuat kebijakan yang mencegah pembuatan direktori.
- Beberapa skenario menggunakan objek 0-byte ini. Misalnya, Anda memiliki struktur seperti `inboxes/customer1000` dan direktori kotak masuk dibersihkan setiap hari.

Terakhir, satu lagi solusi yang mungkin adalah membatasi jumlah objek yang terlihat melalui kondisi kebijakan untuk mengurangi jumlah `HeadObject` panggilan. Agar ini menjadi solusi yang bisa diterapkan, Anda harus menerima bahwa Anda mungkin hanya dapat melihat sekumpulan terbatas semua sub-direktori Anda.

Konfigurasikan sistem file Amazon EFS

AWS Transfer Family mengakses Amazon Elastic File System (Amazon EFS) untuk melayani permintaan transfer pengguna Anda. Jadi, Anda harus menyediakan sistem file Amazon EFS sebagai bagian dari pengaturan server yang mendukung protokol transfer file Anda. Anda dapat menggunakan sistem file yang ada, atau Anda dapat membuat yang baru.

Perhatikan hal-hal berikut:

- Saat Anda menggunakan server Transfer Family dan sistem file Amazon EFS, server dan sistem file harus sama Wilayah AWS.
- Server dan sistem file tidak perlu berada di akun yang sama. Jika server dan sistem file tidak berada dalam akun yang sama, kebijakan sistem file harus memberikan izin eksplisit untuk peran pengguna.

Untuk informasi tentang cara menyiapkan beberapa akun, lihat [Mengelola AWS akun di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

- Saat Anda mengatur pengguna, Anda menetapkan masing-masing peran IAM kepada mereka. Peran ini menentukan tingkat akses yang mereka miliki ke sistem file Amazon EFS Anda.
- Untuk detail tentang pemasangan sistem file Amazon EFS, lihat [Memasang sistem file Amazon EFS](#).

Untuk detail selengkapnya tentang cara AWS Transfer Family dan Amazon EFS bekerja sama, lihat [Menggunakan AWS Transfer Family untuk mengakses file di sistem file Amazon EFS Anda](#) di Panduan Pengguna Amazon Elastic File System.

Kepemilikan file Amazon EFS

Amazon EFS menggunakan model izin file Portable Operating System Interface (POSIX) untuk mewakili kepemilikan file.

Di POSIX, pengguna dalam sistem dikategorikan ke dalam tiga kelas izin yang berbeda: Ketika Anda mengizinkan pengguna untuk mengakses file yang disimpan dalam sistem file Amazon EFS menggunakan AWS Transfer Family, Anda harus menetapkan mereka “profil POSIX.” Profil ini digunakan untuk menentukan akses mereka ke file dan direktori di sistem file Amazon EFS.

- User (u): Pemilik file atau direktori. Biasanya, pencipta file atau direktori juga pemiliknya.
- Grup (g): Kumpulan pengguna yang membutuhkan akses identik ke file dan direktori yang mereka bagikan.
- Lainnya (o): Semua pengguna lain yang memiliki akses ke sistem kecuali pemilik dan anggota grup. Kelas izin ini juga disebut sebagai “Publik.”

Dalam model izin POSIX, setiap objek sistem file (file, direktori, tautan simbolis, pipa bernama, dan soket) dikaitkan dengan tiga set izin yang disebutkan sebelumnya. Objek Amazon EFS memiliki Unix-style mode yang terkait dengannya. Nilai mode ini mendefinisikan izin untuk melakukan tindakan pada objek tersebut.

Selain itu, pada Unix-style sistem, pengguna dan grup dipetakan ke pengidentifikasi numerik, yang digunakan Amazon EFS untuk mewakili kepemilikan file. Untuk Amazon EFS, objek dimiliki oleh satu pemilik dan satu grup. Amazon EFS menggunakan ID numerik yang dipetakan untuk memeriksa izin saat pengguna mencoba mengakses objek sistem file.

Menyiapkan pengguna Amazon EFS untuk Transfer Family

Sebelum mengatur pengguna Amazon EFS, Anda dapat melakukan salah satu hal berikut:

- Anda dapat membuat pengguna dan mengatur folder rumah mereka di Amazon EFS. Lihat [Konfigurasi pengguna Transfer Family di Amazon EFS](#) untuk detail.
- Jika Anda merasa nyaman menambahkan pengguna root, Anda bisa [Buat pengguna root Amazon EFS](#).

 Note

Server Transfer Family tidak mendukung jalur akses Amazon EFS untuk menetapkan izin POSIX. Profil POSIX pengguna Transfer Family (dijelaskan di bagian sebelumnya) menawarkan kemampuan untuk mengatur izin POSIX. Izin ini ditetapkan pada tingkat pengguna, untuk akses granular, berdasarkan UID, GID, dan GID sekunder.

Konfigurasi pengguna Transfer Family di Amazon EFS

Transfer Family memetakan pengguna ke direktori UID/GID dan direktori yang Anda tentukan. Jika UID/GID/directories tidak sudah ada di EFS, maka Anda harus membuatnya sebelum menetakannya di Transfer ke pengguna. Detail untuk membuat pengguna Amazon EFS dijelaskan dalam [Bekerja dengan pengguna, grup, dan izin di Tingkat Sistem File Jaringan \(NFS\)](#) di Panduan Pengguna Amazon Elastic File System.

Langkah-langkah untuk mengatur pengguna Amazon EFS di Transfer Family

1. Petakan EFS UID dan GID untuk pengguna Anda di Transfer Family menggunakan [PosixProfile](#) bidang.
2. Jika Anda ingin pengguna memulai di folder tertentu saat login, Anda dapat menentukan direktori EFS di bawah [HomeDirectory](#) bidang.

Anda dapat mengotomatiskan proses, dengan menggunakan CloudWatch aturan dan fungsi Lambda. Misalnya fungsi Lambda yang berinteraksi dengan EFS, lihat Menggunakan [Amazon EFS untuk AWS Lambda aplikasi tanpa server Anda](#).

Selain itu, Anda dapat mengonfigurasi direktori logis untuk pengguna Transfer Family Anda. Untuk detailnya, lihat [Konfigurasi direktori logis untuk Amazon EFS](#) bagian dalam [Menggunakan direktori logis untuk menyederhanakan struktur direktori Transfer Family Anda](#) topik.

Buat pengguna root Amazon EFS

Jika organisasi Anda merasa nyaman bagi Anda untuk mengaktifkan akses pengguna root melalui SFTP/FTPS konfigurasi pengguna Anda, Anda dapat membuat pengguna yang UID dan GID adalah 0 (pengguna root), kemudian gunakan pengguna root itu untuk membuat folder dan menetapkan pemilik ID POSIX untuk pengguna lainnya. Keuntungan dari opsi ini adalah tidak perlu memasang sistem file Amazon EFS.

Lakukan langkah-langkah yang dijelaskan dalam [Menambahkan pengguna yang dikelola layanan Amazon EFS](#), dan untuk ID Pengguna dan ID Grup, masukkan 0 (nol).

 Tip

Jangan biarkan akun superuser ini ada lebih lama dari yang diperlukan. Atau, jika Anda menyimpan akun pengguna root, pastikan Anda menjaganya tetap terlindungi dengan baik.

Perintah Amazon EFS yang didukung

Perintah berikut didukung untuk Amazon EFS untuk AWS Transfer Family.

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: Hanya root (yaitu, pengguna dengan uid=0) yang dapat mengubah kepemilikan dan izin file dan direktori.
- `chmod`: Hanya root yang dapat mengubah kepemilikan dan izin file dan direktori.
- `chgrp`: Didukung baik untuk root atau untuk pemilik file yang hanya dapat mengubah grup file menjadi salah satu grup sekunder mereka.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

Buat peran dan kebijakan IAM

Topik ini menjelaskan jenis kebijakan dan peran yang dapat digunakan AWS Transfer Family, dan berjalan melalui proses pembuatan peran pengguna. Ini juga menjelaskan cara kerja kebijakan sesi dan memberikan contoh peran pengguna.

AWS Transfer Family menggunakan jenis peran berikut:

- Peran pengguna — Memungkinkan pengguna yang dikelola layanan mengakses sumber daya Transfer Family yang diperlukan. AWS Transfer Family mengasumsikan peran ini dalam konteks ARN pengguna Transfer Family.
- Peran akses - Menyediakan akses hanya ke file Amazon S3 yang sedang ditransfer. Untuk transfer AS2 masuk, peran akses menggunakan Amazon Resource Name (ARN) untuk perjanjian. Untuk transfer AS2 keluar, peran akses menggunakan ARN untuk konektor.
- Peran pemanggilan — Untuk digunakan dengan Amazon API Gateway sebagai penyedia identitas kustom server. Transfer Family mengasumsikan peran ini dalam konteks ARN server Transfer Family.
- Peran logging - Digunakan untuk log entri ke Amazon CloudWatch. Transfer Family menggunakan peran ini untuk mencatat detail keberhasilan dan kegagalan bersama dengan informasi tentang transfer file. Transfer Family mengasumsikan peran ini dalam konteks ARN server Transfer Family. Untuk transfer AS2 keluar, peran logging menggunakan konektor ARN.
- Peran eksekusi — Memungkinkan pengguna Transfer Family memanggil dan meluncurkan alur kerja. Transfer Family mengasumsikan peran ini dalam konteks alur kerja Transfer Family ARN.

Selain peran ini, Anda juga dapat menggunakan kebijakan sesi. Kebijakan sesi digunakan untuk membatasi akses bila diperlukan. Perhatikan bahwa kebijakan ini berdiri sendiri: artinya, Anda tidak menambahkan kebijakan ini ke peran. Sebaliknya, Anda menambahkan kebijakan sesi langsung ke pengguna Transfer Family.

Note

Saat membuat pengguna Transfer Family yang dikelola layanan, Anda dapat memilih Auto-generate kebijakan berdasarkan folder beranda. Ini adalah pintasan yang berguna jika Anda ingin membatasi akses pengguna ke folder mereka sendiri. Selain itu, Anda dapat melihat detail tentang kebijakan sesi dan contoh di [Bagaimana kebijakan sesi bekerja](#). Anda juga dapat menemukan informasi selengkapnya tentang kebijakan [sesi dalam kebijakan Sesi](#) di Panduan Pengguna IAM.

Topik

- [Membuat peran pengguna](#)
- [Bagaimana kebijakan sesi bekerja](#)

- [Contoh kebijakan read/write akses](#)

Membuat peran pengguna

Saat Anda membuat pengguna, Anda membuat sejumlah keputusan tentang akses pengguna. Keputusan ini mencakup bucket Amazon S3 atau sistem file Amazon EFS mana yang dapat diakses pengguna, bagian mana dari setiap bucket Amazon S3 dan file mana dalam sistem file yang dapat diakses, dan izin apa yang dimiliki pengguna (misalnya, `PUT` `GET`).

Untuk menetapkan akses, Anda membuat kebijakan dan peran berbasis identitas AWS Identity and Access Management (IAM) yang menyediakan informasi akses tersebut. Sebagai bagian dari proses ini, Anda menyediakan akses bagi pengguna Anda ke bucket Amazon S3 atau sistem file Amazon EFS yang merupakan target atau sumber untuk operasi file. Untuk melakukan ini, ambil langkah-langkah tingkat tinggi berikut, yang dijelaskan secara rinci nanti:

Membuat peran pengguna

1. Buat kebijakan IAM untuk AWS Transfer Family. Ini dijelaskan dalam [Untuk membuat kebijakan IAM untuk AWS Transfer Family](#).
2. Buat peran IAM dan lampirkan kebijakan IAM baru. Sebagai contoh, lihat [Contoh kebijakan read/write akses](#).
3. Membangun hubungan kepercayaan antara AWS Transfer Family dan peran IAM. Ini dijelaskan dalam [Untuk membangun hubungan kepercayaan](#).

Prosedur berikut menjelaskan cara membuat kebijakan dan peran IAM.

Untuk membuat kebijakan IAM untuk AWS Transfer Family

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, pilih Kebijakan dan kemudian pilih Buat kebijakan.
3. Pada halaman Buat Kebijakan, pilih tab JSON.
4. Di editor yang muncul, ganti isi editor dengan kebijakan IAM yang ingin Anda lampirkan ke peran IAM.

Anda dapat memberikan read/write akses atau membatasi pengguna ke direktori home mereka. Untuk informasi selengkapnya, lihat [Contoh kebijakan read/write akses](#).

5. Pilih Kebijakan tinjauan dan berikan nama dan deskripsi untuk kebijakan Anda, lalu pilih Buat kebijakan.

Selanjutnya, Anda membuat peran IAM dan melampirkan kebijakan IAM baru ke dalamnya.

Untuk membuat peran IAM untuk AWS Transfer Family

1. Di panel navigasi, pilih Peran, lalu pilih Buat peran.

Pada halaman Buat peran, pastikan bahwa AWS layanan dipilih.

2. Pilih Transfer dari daftar layanan, lalu pilih Berikutnya: Izin. Ini membangun hubungan kepercayaan antara AWS Transfer Family dan AWS.
3. Di bagian Lampirkan kebijakan izin, cari dan pilih kebijakan yang baru saja Anda buat, lalu pilih Berikutnya: Tag.
4. (Opsional) Masukkan kunci dan nilai untuk tag, dan pilih Berikutnya: Tinjau.
5. Pada halaman Tinjauan, masukkan nama dan deskripsi untuk peran baru Anda, lalu pilih Buat peran.

Selanjutnya, Anda membangun hubungan kepercayaan antara AWS Transfer Family dan AWS.

Untuk membangun hubungan kepercayaan

Note

Dalam contoh kami, kami menggunakan keduanya `ArnLike` dan `ArnEquals`. Mereka identik secara fungsional, dan oleh karena itu Anda dapat menggunakan keduanya ketika Anda membuat kebijakan Anda. Dokumentasi Transfer Family digunakan `ArnLike` ketika kondisi berisi karakter wildcard, dan `ArnEquals` untuk menunjukkan kondisi kecocokan yang tepat.

1. Di konsol IAM, pilih peran yang baru saja Anda buat.
2. Pada halaman Ringkasan, pilih Trust relationship, lalu pilih Edit trust relationship.
3. Di editor Edit Trust Relationship, pastikan layanannya `"transfer.amazonaws.com"`. Kebijakan akses ditampilkan sebagai berikut.

```
{
```

```

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

```

Kami menyarankan Anda menggunakan kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi untuk melindungi diri Anda dari masalah wakil yang membingungkan. Akun sumber adalah pemilik server dan sumber ARN adalah ARN pengguna. Contoh:

```

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

```

Anda juga dapat menggunakan `ArnLike` kondisi ini jika Anda ingin membatasi ke server tertentu, bukan server apa pun di akun pengguna. Contoh:

```

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

```

Note

Dalam contoh di atas, ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

Untuk detail tentang masalah wakil yang membingungkan dan lebih banyak contoh, lihat [Cross-service pencegahan wakil bingung](#).

4. Pilih Perbarui Kebijakan Kepercayaan untuk memperbarui kebijakan akses.

Anda sekarang telah membuat peran IAM yang memungkinkan AWS Transfer Family untuk memanggil AWS layanan atas nama Anda. Anda melampirkan peran kebijakan IAM yang Anda buat untuk memberikan akses ke pengguna Anda. Di [Memulai dengan AWS Transfer Family titik akhir server](#) bagian ini, peran dan kebijakan ini ditetapkan untuk pengguna atau pengguna Anda.

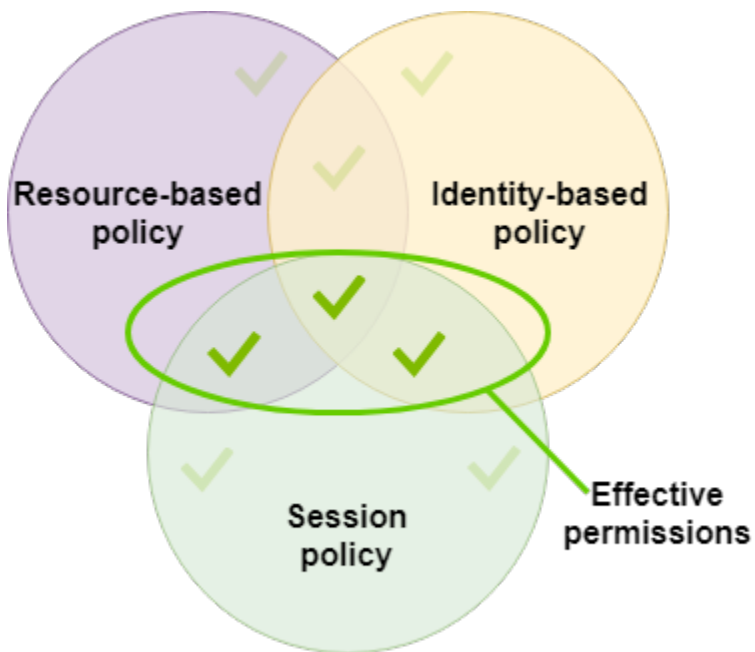
Lihat juga

- Untuk informasi umum selengkapnya tentang peran IAM, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan](#) Pengguna IAM.
- Untuk mempelajari selengkapnya tentang kebijakan berbasis identitas untuk sumber daya Amazon S3, lihat Manajemen [identitas dan akses di Amazon S3 di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- Untuk mempelajari lebih lanjut tentang kebijakan berbasis identitas untuk sumber daya Amazon EFS, lihat [Menggunakan IAM untuk mengontrol akses data sistem file](#) di Panduan Pengguna Amazon Elastic File System.

Bagaimana kebijakan sesi bekerja

Saat administrator membuat peran, peran tersebut sering menyertakan izin luas untuk mencakup beberapa kasus penggunaan atau anggota tim. Jika administrator mengonfigurasi [URL konsol](#), administrator dapat mengurangi izin untuk sesi yang dihasilkan dengan menggunakan kebijakan sesi. Misalnya, jika Anda membuat peran dengan [read/write akses](#), Anda dapat mengatur URL yang membatasi akses pengguna hanya ke direktori beranda mereka.

Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter saat Anda membuat sesi sementara untuk peran atau pengguna secara terprogram. Kebijakan sesi berguna untuk mengunci pengguna sehingga mereka hanya memiliki akses ke bagian bucket Anda di mana awalan objek berisi nama pengguna mereka. Diagram berikut menunjukkan bahwa izin kebijakan sesi adalah persimpangan kebijakan sesi dan kebijakan berbasis sumber daya ditambah persimpangan kebijakan sesi dan kebijakan berbasis identitas.



Untuk detail selengkapnya, lihat [Kebijakan sesi](#) di Panduan Pengguna IAM.

Di AWS Transfer Family, kebijakan sesi hanya didukung saat Anda mentransfer ke atau dari Amazon S3. Contoh kebijakan berikut adalah kebijakan sesi yang membatasi akses pengguna ke home direktori mereka saja. Perhatikan hal-hal berikut:

- PutObjectACL Pernyataan GetObjectACL dan pernyataan hanya diperlukan jika Anda perlu mengaktifkan Akses Lintas Akun. Artinya, server Transfer Family Anda perlu mengakses bucket di akun yang berbeda.
- Panjang maksimum kebijakan sesi adalah 2048 karakter. Untuk detail selengkapnya, lihat [parameter Permintaan kebijakan](#) untuk CreateUser tindakan dalam referensi API.
- Jika bucket Amazon S3 dienkripsi menggunakan AWS Key Management Service (AWS KMS), Anda harus menentukan izin tambahan dalam kebijakan Anda. Lihat perinciannya di [Perlindungan data dan enkripsi](#).
- Untuk menggunakan kebijakan sesi untuk membuat izin akses berdasarkan atribut pengguna tanpa membuat peran IAM terpisah untuk setiap pengguna, lihat. [Pendekatan manajemen izin dinamis](#)

```
{  
  "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

Contoh kebijakan sebelumnya mengasumsikan bahwa pengguna memiliki direktori home mereka diatur untuk menyertakan garis miring, untuk menandakan bahwa itu adalah direktori. Jika, di sisi lain, Anda menetapkan pengguna HomeDirectory tanpa garis miring, maka Anda harus memasukkannya sebagai bagian dari kebijakan Anda.

Dalam contoh kebijakan sebelumnya, perhatikan penggunaan `parameter:transfer:HomeFolder`, `transfer:HomeBucket`, dan `transfer:HomeDirectory` kebijakan. Parameter ini diatur untuk `HomeDirectory` yang dikonfigurasi untuk pengguna, seperti yang dijelaskan dalam [HomeDirectory](#) dan [Menerapkan metode API Gateway Anda](#). Parameter ini memiliki definisi berikut:

- `transfer:HomeBucketParameter` diganti dengan komponen pertama dari `HomeDirectory`.
- `transfer:HomeFolderParameter` diganti dengan bagian `HomeDirectory` parameter yang tersisa.
- `transfer:HomeDirectoryParameter` memiliki garis miring depan (/) yang dihapus sehingga dapat digunakan sebagai bagian dari Nama Sumber Daya Amazon S3 (ARN) dalam sebuah pernyataan. `Resource`

Note

Jika Anda menggunakan direktori logik—yaitu, pengguna adalah LOGICAL —parameter kebijakan ini (`HomeBucket`, `HomeDirectory`, dan `HomeFolder`) tidak didukung. `homeDirectoryType`

Misalnya, asumsikan bahwa `HomeDirectory` parameter yang dikonfigurasi untuk pengguna Transfer Family adalah `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` diatur ke `/home`.
- `transfer:HomeFolder` diatur ke `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` menjadi `home/bob/amazon/stuff/`.

Yang pertama "Sid" memungkinkan pengguna untuk membuat daftar semua direktori mulai dari `/home/bob/amazon/stuff/`.

Yang kedua "Sid" membatasi pengguna put dan get akses ke jalur yang sama, `/home/bob/amazon/stuff/`.

Contoh kebijakan read/write akses

Berikan read/write akses ke bucket Amazon S3

Contoh kebijakan berikut untuk AWS Transfer Family memberikan read/write akses ke objek di bucket Amazon S3 Anda.

Perhatikan hal-hal berikut:

- Ganti `amzn-s3-demo-bucket` dengan nama bucket Amazon S3 Anda.
- `PutObjectACL` Pernyataan `GetObjectACL` dan pernyataan hanya diperlukan jika Anda perlu mengaktifkan Akses Lintas Akun. Artinya, server Transfer Family Anda perlu mengakses bucket di akun yang berbeda.
- `DeleteObjectVersion` Pernyataan `GetObjectVersion` dan hanya diperlukan jika pembuatan versi diaktifkan di bucket Amazon S3 yang sedang diakses.

 Note

Jika Anda pernah mengaktifkan pembuatan versi untuk bucket, Anda memerlukan izin ini, karena Anda hanya dapat menangguhkan pembuatan versi di Amazon S3, dan tidak mematikannya sepenuhnya. Untuk detailnya, lihat Bucket [yang tidak berversi, berkemampuan versi, dan ditangguhkan versi](#).

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



```

        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
}
]
}

```

Berikan akses sistem file ke file dalam sistem file Amazon EFS

Note

Selain kebijakan, Anda juga harus memastikan izin file POSIX Anda memberikan akses yang sesuai. Untuk informasi selengkapnya, lihat [Bekerja dengan pengguna, grup, dan izin di Tingkat Network File System \(NFS\)](#) dalam Panduan Pengguna Amazon Elastic File System.

Contoh kebijakan berikut memberikan akses sistem file root ke file di sistem file Amazon EFS Anda.

Note

Dalam contoh berikut, ganti *region* dengan wilayah Anda, *account-id* dengan akun tempat file berada, dan *file-system-id* dengan ID Amazon Elastic File System (Amazon EFS) Anda.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RootFileSystemAccess",
      "Effect": "Allow",
      "Action": [

```

```

        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
    ],
    "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
}
]
}

```

Contoh kebijakan berikut memberikan akses sistem file pengguna ke file di sistem file Amazon EFS Anda.

```

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

```

Tutorial Transfer Family

Panduan AWS Transfer Family pengguna menyediakan penelusuran terperinci untuk beberapa kasus penggunaan.

- [Memulai dengan AWS Transfer Family titik akhir server](#)- Buat server Transfer Family SFTP dengan pengguna yang dikelola layanan dan transfer file menggunakan klien.
- [Menyiapkan dan menggunakan konektor SFTP](#)- Siapkan konektor SFTP untuk mentransfer file antara penyimpanan Amazon S3 dan server SFTP.
- [Menyiapkan metode Amazon API Gateway sebagai penyedia identitas kustom](#)- Konfigurasi metode Amazon API Gateway sebagai penyedia identitas khusus untuk mengunggah file ke AWS Transfer Family server.
- [Menyiapkan alur kerja terkelola untuk mendekripsi file](#)- Buat alur kerja terkelola untuk mendekripsi file, mengunggah file terenkripsi ke Amazon S3, dan melihat konten yang didekripsi.
- [Menyiapkan konfigurasi AS2](#)- Siapkan server AS2 Transfer Family, termasuk impor sertifikat, pembuatan profil dan perjanjian, konfigurasi konektor AS2 opsional, dan pengujian.
- Tutorial berikut memandu Anda melalui pembuatan dan konfigurasi aplikasi web Transfer Family. Pilih tutorial yang paling sesuai dengan kebutuhan Anda:

[Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#)- Pelajari cara membuat dan mengonfigurasi aplikasi web Transfer Family.

[Tutorial: Menyiapkan aplikasi AWS Transfer Family web dengan akses multi-bucket selektif](#)- Konfigurasi aplikasi web Transfer Family dengan izin bucket Amazon S3 granular untuk satu pengguna.

Topik

- [Memulai dengan AWS Transfer Family titik akhir server](#)
- [Menyiapkan alur kerja terkelola untuk mendekripsi file](#)
- [Menyiapkan dan menggunakan konektor SFTP](#)
- [Menyiapkan metode Amazon API Gateway sebagai penyedia identitas kustom](#)
- [Menyiapkan konfigurasi AS2](#)
- [Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#)
- [Tutorial: Menyiapkan aplikasi AWS Transfer Family web dengan akses multi-bucket selektif](#)

Memulai dengan AWS Transfer Family titik akhir server

Gunakan tutorial ini untuk memulai AWS Transfer Family (Transfer Family). Anda akan belajar cara membuat SFTP-enabled server dengan titik akhir yang dapat diakses publik menggunakan penyimpanan Amazon S3, menambahkan pengguna dengan otentikasi yang dikelola layanan, dan mentransfer file dengan Cyberduck.

Topik

- [Prasyarat](#)
- [Langkah 1: Masuk ke AWS Transfer Family konsol](#)
- [Langkah 2: Buat SFTP-enabled server](#)
- [Langkah 3: Tambahkan pengguna yang dikelola layanan](#)
- [Langkah 4: Transfer file menggunakan klien](#)

Prasyarat

Sebelum Anda mulai, pastikan untuk melengkapi persyaratan di[Prasyarat](#). Sebagai bagian dari penyiapan ini, Anda membuat bucket Amazon Simple Storage Service (Amazon S3) dan AWS Identity and Access Management peran pengguna (IAM).

Ada izin yang diperlukan untuk menggunakan AWS Transfer Family konsol, dan ada izin yang diperlukan untuk mengonfigurasi AWS layanan lain yang digunakan Transfer Family, seperti Amazon Simple Storage Service, Amazon Elastic File System AWS Certificate Manager, dan Amazon Route 53. Misalnya, untuk pengguna yang mentransfer file masuk dan keluar dari AWS penggunaan Transfer Family, AmazonS3FullAccessmemberikan izin untuk menyiapkan dan menggunakan bucket Amazon S3. Beberapa izin dalam kebijakan ini diperlukan untuk membuat bucket Amazon S3.

Untuk menggunakan konsol Transfer Family, Anda memerlukan yang berikut:

- AWSTransferConsoleFullAccessmemberikan izin bagi pengguna SFTP Anda untuk membuat sumber daya Transfer Family.
- IAMFullAccess(atau khususnya kebijakan yang memungkinkan pembuatan peran IAM) hanya diperlukan jika Anda ingin Transfer Family secara otomatis membuat peran logging untuk server Anda di CloudWatch Log Amazon atau peran pengguna untuk pengguna yang masuk ke server.
- Untuk membuat dan menghapus jenis server VPC, Anda perlu menambahkan tindakan ec2: CreateVpcEndpoint dan ec2: DeleteVpcEndpoints ke kebijakan Anda. Untuk informasi tentang

membatasi akses titik akhir VPC untuk tujuan keamanan, lihat. [Membatasi akses endpoint VPC untuk server Transfer Family](#)

Note

Kebijakan AmazonS3FullAccess dan IAMFullAccess kebijakan itu sendiri tidak diperlukan untuk penggunaan AWS Transfer Family umum. Mereka disajikan di sini sebagai cara sederhana untuk memastikan bahwa semua izin yang Anda butuhkan tercakup. Selain itu, ini adalah kebijakan AWS terkelola, yang merupakan kebijakan standar yang tersedia untuk semua AWS pelanggan. Anda dapat melihat izin individual dalam kebijakan ini dan menentukan set minimal yang Anda perlukan untuk tujuan Anda.

Langkah 1: Masuk ke AWS Transfer Family konsol

Untuk masuk ke Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Untuk ID Akun atau alias, masukkan ID untuk Anda Akun AWS.
3. Untuk nama pengguna IAM, masukkan nama peran pengguna yang Anda buat untuk Transfer Family.
4. Untuk Kata Sandi, masukkan kata sandi AWS akun Anda.
5. Pilih Masuk.

Langkah 2: Buat SFTP-enabled server

Secure Shell (SSH) File Transfer Protocol (SFTP) adalah protokol jaringan yang digunakan untuk transfer data yang aman melalui internet. Protokol ini mendukung fungsionalitas keamanan dan otentikasi penuh SSH. Ini banyak digunakan untuk bertukar data, termasuk informasi sensitif antara mitra bisnis di berbagai industri seperti layanan keuangan, perawatan kesehatan, ritel, dan periklanan.

Untuk membuat SFTP-enabled server

1. Pilih Server dari panel Navigasi lalu pilih Buat server.

2. Di Pilih protokol, pilih SFTP, lalu pilih Berikutnya.
3. Di Pilih penyedia identitas, pilih Layanan yang dikelola untuk menyimpan identitas dan kunci pengguna di Transfer Family, lalu pilih Berikutnya.
4. Di Pilih titik akhir, lakukan hal berikut:
 - a. Untuk tipe Endpoint, pilih tipe titik akhir yang dapat diakses publik.
 - b. Untuk nama host Kustom, pilih Tidak Ada.
 - c. Pilih Berikutnya.
5. Di Pilih domain, pilih Amazon S3.
6. Di Konfigurasikan detail tambahan, untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritme kriptografi yang diaktifkan untuk digunakan oleh server Anda. Kebijakan keamanan terbaru kami adalah default: untuk detailnya, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

 Note

Hanya jika Anda menambahkan alur kerja terkelola untuk server Anda, pilih Buat peran baru untuk CloudWatch pencatatan. Untuk mencatat peristiwa server, Anda tidak perlu membuat peran IAM.

7. Di Tinjau dan buat, pilih Buat server. Anda dibawa ke halaman Server.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file, tetapi Anda harus membuat pengguna terlebih dahulu. Untuk detail tentang membuat pengguna, lihat [Mengelola pengguna untuk titik akhir server](#).

Langkah 3: Tambahkan pengguna yang dikelola layanan

Untuk menambahkan pengguna ke SFTP-enabled server

1. Pada halaman Server, pilih server yang ingin Anda tambahkan pengguna.
2. Pilih Tambahkan pengguna.
3. Di bagian Konfigurasi pengguna, untuk Nama Pengguna, masukkan nama pengguna. Nama pengguna ini harus minimal 3 dan maksimal 100 karakter. Anda dapat menggunakan karakter berikut dalam nama pengguna: a—z, 0—9 A-Z, garis bawah '_', tanda hubung '-', titik '.' dan di tanda '@'. Nama pengguna tidak dapat dimulai dengan tanda hubung '-', titik '.' atau di tanda '@'.

4. Untuk Access, pilih peran IAM yang Anda buat. [Buat peran dan kebijakan IAM](#) Peran IAM ini mencakup kebijakan IAM yang berisi izin untuk mengakses bucket Amazon S3 Anda, serta hubungan kepercayaan dengan layanan. AWS Transfer Family Prosedur yang diuraikan dalam [Untuk membangun hubungan kepercayaan](#) menunjukkan bagaimana membangun hubungan kepercayaan yang tepat.
5. Untuk Kebijakan, pilih Tidak Ada.
6. Untuk direktori Home, pilih bucket Amazon S3 tempat Anda ingin menyimpan data yang Anda transfer gunakan. AWS Transfer Family Masukkan jalur ke home direktori. Ini adalah direktori yang dilihat pengguna Anda saat mereka masuk menggunakan klien mereka.

Sebaiknya gunakan jalur direktori yang berisi nama pengguna sehingga Anda memiliki opsi untuk menggunakan kebijakan sesi. Kebijakan sesi membatasi akses pengguna di bucket Amazon S3 ke direktori pengguna tersebut. home Untuk informasi selengkapnya tentang penggunaan kebijakan sesi, lihat [Bagaimana kebijakan sesi bekerja](#).

Jika mau, Anda dapat menyimpan parameter ini kosong untuk menggunakan direktori bucket Amazon S3 Anda. `root` Jika Anda memilih opsi ini, pastikan bahwa peran IAM Anda menyediakan akses ke `root` direktori.

7. Pilih kotak centang Dibatasi untuk mencegah pengguna mengakses apa pun di luar home direktori mereka. Ini juga mencegah pengguna melihat nama bucket Amazon S3 atau nama folder.
8. Untuk kunci publik SSH, masukkan bagian kunci SSH publik dari key pair SSH dalam format. `ssh-rsa <string>`

Kunci Anda harus divalidasi oleh layanan sebelum Anda dapat menambahkan pengguna baru Anda. Untuk informasi selengkapnya tentang cara menghasilkan key pair SSH, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

9. (Opsional) Untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, dan pilih Tambahkan tag.
10. Pilih Tambah untuk menambahkan pengguna baru Anda ke server yang Anda pilih.

Pengguna baru muncul di bagian Pengguna pada halaman detail Server.

Langkah 4: Transfer file menggunakan klien

Anda mentransfer file melalui AWS Transfer Family layanan dengan menentukan operasi transfer di klien. AWS Transfer Family mendukung beberapa klien. Untuk detailnya, lihat [Mentransfer file melalui titik akhir server menggunakan klien](#)

Bagian ini berisi prosedur untuk menggunakan Cyberduck dan OpenSSH.

Topik

- [Gunakan Cyberduck](#)
- [Gunakan OpenSSH](#)

Gunakan Cyberduck

Untuk mentransfer file AWS Transfer Family menggunakan Cyberduck

1. Buka klien [Cyberduck](#).
2. Pilih Buka Koneksi.
3. Dalam kotak dialog Open Connection, pilih SFTP (SSH File Transfer Protocol).
4. Untuk Server, masukkan endpoint server Anda. Titik akhir server terletak di halaman detail Server, lihat [Lihat detail server SFTP, FTPS, dan FTP](#).
5. Untuk nomor Port, masukkan **22** untuk SFTP.
6. Untuk Nama Pengguna, masukkan nama untuk pengguna yang Anda buat [Mengelola pengguna untuk titik akhir server](#).
7. Untuk SSH Private Key, pilih atau masukkan kunci pribadi SSH.
8. Pilih Hubungkan.
9. Lakukan transfer file Anda.

Tergantung di mana file Anda berada, lakukan salah satu hal berikut:

- Di direktori lokal Anda (sumber), pilih file yang ingin Anda transfer, dan seret dan jatuhkan ke direktori Amazon S3 (target).
- Di direktori Amazon S3 (sumber), pilih file yang ingin Anda transfer, dan seret dan jatuhkan ke direktori lokal Anda (target).

Gunakan OpenSSH

Gunakan instruksi yang mengikuti untuk mentransfer file dari baris perintah menggunakan OpenSSH.

Note

Klien ini hanya berfungsi dengan SFTP-enabled server.

Untuk mentransfer file AWS Transfer Family menggunakan utilitas baris perintah OpenSSH

1. Di Linux atau Macintosh, buka terminal perintah.
2. Pada prompt, masukkan perintah berikut: `% sftp -i transfer-key sftp_user@service_endpoint`

Pada perintah sebelumnya, `sftp_user` adalah nama pengguna dan `transfer-key` merupakan kunci pribadi SSH. Di sini, `service_endpoint` adalah titik akhir server seperti yang ditunjukkan di AWS Transfer Family konsol untuk server yang dipilih.

`sftpPrompt` akan muncul.

3. (Opsional) Untuk melihat direktori home pengguna, masukkan perintah berikut pada `sftp` prompt: `sftp> pwd`
4. Pada baris berikutnya, masukkan teks berikut: `sftp> cd /amzn-s3-demo-bucket/home/sftp_user`

Dalam latihan memulai ini, bucket Amazon S3 ini adalah target transfer file.

5. Pada baris berikutnya, masukkan perintah berikut: `sftp> put filename.txt`

`put` Perintah mentransfer file ke bucket Amazon S3.

Pesan seperti berikut ini muncul, menunjukkan bahwa transfer file sedang berlangsung, atau selesai.

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

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

Menyiapkan alur kerja terkelola untuk mendekripsi file

Tutorial ini menggambarkan cara mengatur alur kerja terkelola yang berisi langkah dekripsi. Tutorial ini juga menunjukkan cara mengunggah file terenkripsi ke bucket Amazon S3 dan kemudian melihat file yang didekripsi di bucket yang sama.

Note

Blog AWS penyimpanan memiliki posting yang menjelaskan cara mendekripsi file tanpa menulis kode apa pun menggunakan alur kerja Transfer Family Managed, [Enkripsi dan dekripsi file dengan PGP dan](#). AWS Transfer Family

Topik

- [Langkah 1: Konfigurasi peran eksekusi](#)
- [Langkah 2: Buat alur kerja terkelola](#)
- [Langkah 3: Tambahkan alur kerja ke server dan buat pengguna](#)
- [Langkah 4: Buat key pair PGP](#)
- [Langkah 5: Simpan kunci pribadi PGP di AWS Secrets Manager](#)
- [Langkah 6: Enkripsi file](#)
- [Langkah 7: Jalankan alur kerja dan lihat hasilnya](#)

Langkah 1: Konfigurasi peran eksekusi

Buat peran eksekusi AWS Identity and Access Management (IAM) yang dapat digunakan Transfer Family untuk meluncurkan alur kerja. Proses pembuatan peran eksekusi dijelaskan dalam [Kebijakan IAM untuk alur kerja](#).

Note

Sebagai bagian dari menciptakan peran eksekusi, pastikan untuk membangun hubungan kepercayaan antara peran eksekusi dan Transfer Family, seperti yang dijelaskan dalam [Untuk membangun hubungan kepercayaan](#).

Kebijakan peran eksekusi berikut berisi semua izin yang diperlukan untuk memulai alur kerja yang Anda buat dalam tutorial ini. Untuk menggunakan kebijakan contoh ini, ganti *user input placeholders* dengan informasi Anda sendiri. Ganti `amzn-s3-demo-bucket` dengan nama bucket Amazon S3 tempat Anda mengunggah file terenkripsi.

Note

Tidak setiap alur kerja memerlukan setiap izin yang tercantum dalam contoh ini. Anda dapat membatasi izin berdasarkan jenis langkah dalam alur kerja spesifik Anda. Izin yang diperlukan untuk setiap jenis langkah yang telah ditentukan dijelaskan dalam [Gunakan langkah-langkah yang telah ditentukan](#). Izin yang diperlukan untuk langkah kustom dijelaskan [diizin IAM untuk langkah khusus](#).

```
{
  "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:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "DecryptSecret",
      "Effect": "Allow",
      "Action": [
```

```

        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/
transfer/*"
    }
  ]
}

```

Langkah 2: Buat alur kerja terkelola

Sekarang Anda perlu membuat alur kerja yang berisi langkah dekripsi.

Untuk membuat alur kerja yang berisi langkah dekripsi

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Alur kerja, lalu pilih Buat alur kerja.
3. Masukkan detail berikut:
 - Masukkan deskripsi, misalnya **Decrypt workflow example**.
 - Di bagian Langkah nominal, pilih Tambah langkah.
4. Untuk Pilih jenis langkah, pilih Dekripsi file, lalu pilih Berikutnya.
5. Dalam kotak dialog Konfigurasi parameter, tentukan yang berikut ini:
 - Masukkan nama langkah deskriptif, misalnya, **decrypt-step**. Spasi tidak diperbolehkan dalam nama langkah.
 - Untuk Tujuan untuk file yang didekripsi, pilih Amazon S3.
 - Untuk nama bucket Tujuan, pilih bucket Amazon S3 yang sama dengan yang Anda tentukan seperti `amzn-s3-demo-bucket` dalam kebijakan IAM yang Anda buat di Langkah 1.
 - Untuk awalan kunci Destination, masukkan nama awalan (folder) tempat Anda ingin menyimpan file yang didekripsi di bucket tujuan, misalnya, **decrypted-files/**

Note

Pastikan untuk menambahkan trailing slash (/) ke awalan Anda.

- Untuk tutorial ini, biarkan Overwrite sudah dihapus. Saat pengaturan ini dihapus, jika Anda mencoba mendekripsi file dengan nama identik dari file yang ada, pemrosesan alur kerja berhenti, dan file baru tidak diproses.

Pilih Berikutnya untuk pindah ke layar ulasan.

6. Tinjau detail untuk langkahnya. Jika semuanya benar, pilih Buat langkah.
7. Alur kerja Anda hanya membutuhkan satu langkah dekripsi, jadi tidak ada langkah tambahan untuk mengonfigurasi. Pilih Buat alur kerja untuk membuat alur kerja baru.

Perhatikan ID alur kerja untuk alur kerja baru Anda. Anda akan memerlukan ID ini untuk langkah selanjutnya. Tutorial ini menggunakan *w-1234abcd5678efghi* sebagai contoh ID alur kerja.

Langkah 3: Tambahkan alur kerja ke server dan buat pengguna

Sekarang Anda memiliki alur kerja dengan langkah dekripsi, Anda harus mengaitkannya dengan server Transfer Family. Tutorial ini menunjukkan cara melampirkan alur kerja ke server Transfer Family yang ada. Atau, Anda dapat membuat server baru untuk digunakan dengan alur kerja Anda.

Setelah Anda melampirkan alur kerja ke server, Anda harus membuat pengguna yang dapat SFTP ke server dan memicu alur kerja untuk berjalan.

Untuk mengonfigurasi server Transfer Family untuk menjalankan alur kerja

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server, lalu pilih server dari daftar. Pastikan server ini mendukung protokol SFTP.
3. Pada halaman detail untuk server, gulir ke bawah ke bagian Detail tambahan, lalu pilih Edit.
4. Pada halaman Edit detail tambahan, di bagian Alur kerja terkelola, pilih alur kerja Anda, dan pilih peran eksekusi yang sesuai.
 - Untuk Alur Kerja untuk upload file lengkap, pilih alur kerja yang Anda buat [Langkah 2: Buat alur kerja terkelola](#), misalnya, **w-1234abcd5678efghi**
 - Untuk peran eksekusi alur kerja terkelola, pilih peran IAM yang Anda buat. [Langkah 1: Konfigurasi peran eksekusi](#)
5. Gulir ke bagian bawah halaman, dan pilih Simpan untuk menyimpan perubahan Anda.

Perhatikan ID untuk server yang Anda gunakan. Nama AWS Secrets Manager rahasia yang Anda gunakan untuk menyimpan kunci PGP Anda sebagian didasarkan pada ID server.

Untuk menambahkan pengguna yang dapat memicu alur kerja

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server, lalu pilih server yang Anda gunakan untuk mendekripsi alur kerja.
3. Pada halaman detail server, gulir ke bawah ke bagian Pengguna, dan pilih Tambah pengguna.
4. Untuk pengguna baru Anda, masukkan detail berikut:
 - Untuk Nama Pengguna, masukkan **decrypt-user**.
 - Untuk Peran, pilih peran pengguna yang dapat mengakses server Anda.
 - Untuk direktori Home, pilih bucket Amazon S3 yang Anda gunakan sebelumnya, misalnya, `amzn-s3-demo-bucket`
 - Untuk kunci publik SSH, tempelkan kunci publik yang sesuai dengan kunci pribadi yang Anda miliki. Lihat perinciannya di [Buat kunci SSH untuk pengguna yang dikelola layanan](#).
5. Pilih Tambah untuk menyimpan pengguna baru Anda.

Catat nama pengguna Transfer Family Anda untuk server ini. Rahasiannya sebagian didasarkan pada nama pengguna. Untuk kesederhanaan, tutorial ini menggunakan rahasia default yang dapat digunakan oleh setiap pengguna server.

Langkah 4: Buat key pair PGP

Gunakan salah satu [klien PGP yang didukung](#) untuk menghasilkan key pair PGP. Proses ini dijelaskan secara rinci dalam [Hasilkan kunci PGP](#).

Untuk menghasilkan key pair PGP

1. Untuk tutorial ini, Anda dapat menggunakan gpg (GnuPG) versi 2.0.22 klien untuk menghasilkan key pair PGP yang menggunakan RSA sebagai algoritma enkripsi. Untuk klien ini, jalankan perintah berikut, dan berikan alamat email dan frasa sandi. Anda dapat menggunakan nama atau alamat email apa pun yang Anda suka. Pastikan Anda mengingat nilai yang Anda gunakan, karena Anda harus memasukkannya nanti dalam tutorial.

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

 Note

Jika Anda menggunakan GnuPG versi 2.3.0 atau yang lebih baru, Anda harus menjalankannya. `gpg --full-gen-key` Ketika diminta untuk jenis kunci yang akan dibuat, pilih RSA atau ECC. Jika Anda memilih ECC, Anda dapat memilih dari NIST, BrainPool dan Curve25519 untuk kurva elips.

2. Ekspor kunci pribadi dengan menjalankan perintah berikut. Ganti `user@example.com` dengan alamat email yang Anda gunakan saat membuat kunci.

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

Perintah ini mengekspor kunci pribadi ke **workflow-tutorial-key.gpg** file. Anda dapat memberi nama file output apa pun yang Anda suka. Anda juga dapat menghapus file kunci pribadi setelah Anda menambahkannya AWS Secrets Manager.

Langkah 5: Simpan kunci pribadi PGP di AWS Secrets Manager

Anda perlu menyimpan kunci pribadi di Secrets Manager, dengan cara yang sangat spesifik, sehingga alur kerja dapat menemukan kunci pribadi saat alur kerja menjalankan langkah dekripsi pada file yang diunggah.

 Note

Ketika Anda menyimpan rahasia di Secrets Manager, Anda Akun AWS dikenakan biaya. Untuk informasi tentang harga, lihat [AWS Secrets Manager Harga](#).

Untuk menyimpan kunci pribadi PGP di Secrets Manager

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pada panel navigasi kiri, pilih Rahasia.
3. Pada halaman Rahasia, pilih Simpan rahasia baru.
4. Pada halaman Pilih jenis rahasia, untuk tipe Rahasia, pilih Jenis rahasia lainnya.
5. Di bagian Key/value pasangan, pilih Key/valueta.

- Kunci — Masukkan **PGPPrivateKey**.
 - nilai — Tempelkan teks kunci pribadi Anda ke bidang nilai.
6. Pilih Tambah baris, dan di bagian Key/value pasangan, pilih Key/value tab.
 - Kunci — Masukkan **PGPPassphrase**.
 - value — Masukkan kata sandi yang Anda gunakan saat membuat key pair PGP. [Langkah 4: Buat key pair PGP](#)
 7. Pilih Berikutnya.
 8. Pada halaman Konfigurasi rahasia, masukkan nama dan deskripsi untuk rahasia Anda. Anda dapat membuat rahasia untuk pengguna tertentu atau yang dapat digunakan oleh semua pengguna. Jika ID server Anda **s-11112222333344445**, beri nama rahasianya sebagai berikut.
 - Untuk membuat rahasia default untuk semua pengguna, beri nama rahasianya **aws/transfer/s-11112222333344445/@pgp-default**.
 - Untuk membuat rahasia hanya untuk pengguna yang Anda buat sebelumnya, beri nama rahasianya **aws/transfer/s-11112222333344445/decrypt-user**.
 9. Pilih Berikutnya, dan kemudian terima default pada halaman Konfigurasi rotasi. Lalu pilih Selanjutnya.
 10. Pada halaman Review, pilih Store untuk membuat dan menyimpan rahasia.

Untuk informasi selengkapnya tentang menambahkan kunci pribadi PGP ke Secrets Manager, lihat [Menggunakan AWS Secrets Manager untuk menyimpan kunci PGP Anda](#).

Langkah 6: Enkripsi file

Gunakan gpg program untuk mengenkripsi file untuk digunakan dalam alur kerja Anda. Jalankan perintah berikut untuk mengenkripsi file:

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

Sebelum menjalankan perintah ini, perhatikan hal berikut:

- Untuk **-r** argumennya, ganti **marymajor@example.com** dengan alamat email yang Anda gunakan saat membuat key pair PGP.

- `--openpgpBendera` adalah opsional. Bendera ini membuat file terenkripsi sesuai dengan standar [OpenPGP RFC4880](#).
- Perintah ini membuat file bernama **testfile.txt.gpg** di lokasi yang sama dengan **testfile.txt**.

Important

Saat mengenkripsi file untuk digunakan dengan AWS Transfer Family alur kerja, selalu pastikan Anda menentukan penerima non-anonim menggunakan parameter. `-r` Enkripsi anonim (tanpa menentukan penerima) dapat menyebabkan kegagalan dekripsi dalam alur kerja karena sistem tidak akan dapat mengidentifikasi kunci mana yang akan digunakan untuk dekripsi. Informasi debugging untuk masalah ini tersedia di [Memecahkan masalah enkripsi penerima anonim](#).

Langkah 7: Jalankan alur kerja dan lihat hasilnya

Untuk menjalankan alur kerja, Anda terhubung ke server Transfer Family dengan pengguna yang Anda buat di Langkah 3. Kemudian Anda dapat melihat di bucket Amazon S3 yang Anda tentukan di [Langkah 2.5, konfigurasi parameter tujuan](#) untuk melihat file yang didekripsi.

Untuk menjalankan alur kerja dekripsi

1. Buka terminal perintah.
2. Jalankan perintah berikut, ganti *your-endpoint* dengan endpoint Anda yang sebenarnya, dan *transfer-key* dengan kunci pribadi SSH pengguna Anda:

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

Misalnya, jika kunci pribadi disimpan `~/.ssh/decrypt-user`, dan titik akhir Anda, perintahnya adalah sebagai berikut: `s-11112222333344445.server.transfer.us-east-2.amazonaws.com`

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

3. Jalankan perintah `pwd`. Jika berhasil, perintah ini akan mengembalikan yang berikut:

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

Direktori Anda mencerminkan nama bucket Amazon S3 Anda.

4. Jalankan perintah berikut untuk mengunggah file dan memicu alur kerja untuk dijalankan:

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

5. Untuk tujuan file yang didekripsi, Anda menentukan `decrypted-files/` folder saat Anda membuat alur kerja. Sekarang, Anda dapat menavigasi ke folder itu dan daftar isinya.

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

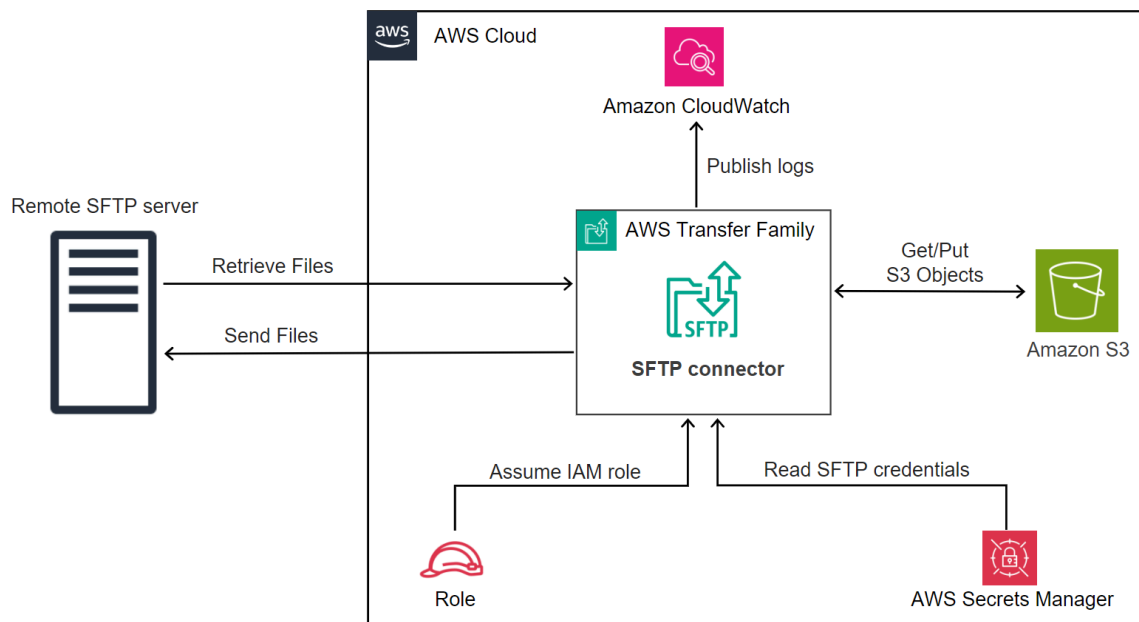
Jika berhasil, `ls` perintah mencantumkan `testfile.txt` file. Anda dapat mengunduh file ini dan memverifikasi bahwa itu sama dengan file asli yang Anda enkripsi sebelumnya.

Menyiapkan dan menggunakan konektor SFTP

Tujuan dari konektor adalah untuk membangun hubungan antara AWS penyimpanan Anda dan server SFTP mitra. Anda dapat mengirim file dari Amazon S3 ke tujuan eksternal milik mitra. Anda juga dapat menggunakan konektor SFTP untuk mengambil file dari server SFTP mitra.

Tutorial ini menggambarkan cara mengatur konektor SFTP dengan jenis jalan keluar yang dikelola layanan dan VPC_LATTICE, lalu mentransfer file antara penyimpanan Amazon S3 dan server SFTP.

Konektor SFTP mengambil kredensi SFTP dari AWS Secrets Manager untuk mengautentikasi ke server SFTP jarak jauh dan membuat koneksi. Konektor mengirim file ke atau mengambil file dari server jarak jauh, dan menyimpan file di Amazon S3. Anda dapat memilih antara jalan keluar yang dikelola layanan (menggunakan infrastruktur AWS terkelola) atau jalan keluar VPC (perutean melalui VPC menggunakan Resource Access). Cross-VPC Peran IAM digunakan untuk mengizinkan akses ke bucket Amazon S3 dan ke kredensial yang disimpan di Secrets Manager. Dan Anda dapat masuk ke Amazon CloudWatch.



Posting blog berikut menyediakan arsitektur referensi untuk membangun alur kerja MFT menggunakan konektor SFTP, termasuk enkripsi file menggunakan PGP sebelum mengirimnya ke server SFTP jarak jauh menggunakan konektor SFTP: [Merancang transfer file terkelola yang aman dan sesuai dengan konektor SFTP dan](#) enkripsi PGP. AWS Transfer Family

Jenis jalan keluar konektor

Konektor SFTP mendukung dua jenis jalan keluar yang menentukan bagaimana konektor Anda merutekan lalu lintas ke server SFTP jarak jauh:

- **SERVICE_MANAGED (default):** Menggunakan infrastruktur terkelola AWS Transfer Family dengan alamat IP statis untuk koneksi keluar.
- **VPC:** Rutekan lalu lintas melalui VPC Anda menggunakan Akses Cross-VPC Sumber Daya, memungkinkan konektivitas titik akhir pribadi dan penggunaan gateway NAT Anda sendiri.

Tutorial ini mencakup kedua jenis jalan keluar. Pilih jenis jalan keluar VPC saat Anda perlu:

- Connect ke server SFTP pribadi di VPC Anda (alamat IP pribadi)
- Connect ke server SFTP lokal melalui Direct Connect atau VPN
- Rutekan lalu lintas titik akhir publik melalui VPC Anda untuk kontrol keamanan
- Gunakan alamat IP Elastis Anda sendiri untuk koneksi keluar

Topik

- [Langkah 1: Buat sumber daya pendukung yang diperlukan](#)
- [Langkah 2: Buat dan uji konektor SFTP](#)
- [Langkah 3: Kirim dan ambil file menggunakan konektor SFTP](#)
- [Prosedur untuk membuat server Transfer Family untuk digunakan sebagai server SFTP jarak jauh Anda](#)

Langkah 1: Buat sumber daya pendukung yang diperlukan

Anda dapat menggunakan konektor SFTP untuk menyalin file antara Amazon S3 dan server SFTP jarak jauh apa pun. Untuk tutorial ini, kami menggunakan AWS Transfer Family server sebagai server SFTP jarak jauh kami. Kita perlu membuat dan mengkonfigurasi sumber daya berikut:

- Buat bucket Amazon S3 untuk menyimpan file di AWS lingkungan Anda, dan untuk mengirim dan mengambil file dari server SFTP jarak jauh.: [Buat ember Amazon S3](#)
- Buat AWS Identity and Access Management peran untuk mengakses penyimpanan Amazon S3 dan rahasia kami di Secrets Manager.: [Buat peran IAM dengan izin yang diperlukan](#)
- Buat server Transfer Family yang menggunakan protokol SFTP, dan pengguna yang dikelola layanan yang menggunakan konektor SFTP untuk mentransfer file ke atau dari server SFTP: [Buat server SFTP Transfer Family dan pengguna](#)
- Buat AWS Secrets Manager rahasia yang menyimpan kredensial yang digunakan oleh konektor SFTP untuk masuk ke server SFTP jarak jauh.: [Buat dan simpan rahasia di AWS Secrets Manager](#)

Untuk konektor tipe jalan keluar VPC, Anda juga membutuhkan:

- VPC dengan subnet dan grup keamanan yang sesuai
- Gerbang Sumber Daya (diperlukan minimal 2 Availability Zone): [Buat Resource Gateway \(hanya tipe jalan keluar VPC\)](#).
- Konfigurasi Sumber Daya yang menunjuk ke server SFTP Anda.: [Buat Konfigurasi Sumber Daya \(hanya tipe jalan keluar VPC\)](#) Untuk informasi selengkapnya, lihat [Konfigurasi sumber daya](#) di Panduan Pengguna Amazon VPC Lattice.

Buat ember Amazon S3

Untuk membuat bucket Amazon S3

1. Masuk ke AWS Transfer Family konsol di <https://console.aws.amazon.com/s3/>.
2. Pilih Wilayah dan masukkan nama.

Untuk tutorial ini, ember kami ada di **US East (N. Virginia) us-east-1**, dan namanya **sftp-server-storage-east**.

3. Terima defaultnya dan pilih Buat bucket.

Untuk detail selengkapnya tentang membuat bucket Amazon S3, lihat [Bagaimana cara membuat bucket S3?](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Buat peran IAM dengan izin yang diperlukan

Untuk peran akses, buat kebijakan dengan izin berikut.

JSON

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

```

```

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

```

Ganti item sebagai berikut:

- Untuk `amzn-s3-demo-bucket`, tutorial menggunakan **sftp-server-storage-east**.
- Untuk *region*, tutorial menggunakan **us-east-1**.
- Untuk *account-id*, gunakan Akun AWS ID Anda.
- Karena *SecretName-6RandomCharacters*, kami **using sftp-connector1** untuk nama (Anda akan memiliki enam karakter acak Anda sendiri untuk rahasia Anda).

Anda juga harus memastikan bahwa peran ini berisi hubungan kepercayaan yang memungkinkan konektor mengakses sumber daya Anda saat melayani permintaan transfer pengguna Anda. Untuk detail tentang membangun hubungan kepercayaan, lihat [Untuk membangun hubungan kepercayaan](#).

Note

Untuk melihat detail untuk peran yang kita gunakan untuk tutorial, lihat [Gabungan peran pengguna dan akses](#).

Buat dan simpan rahasia di AWS Secrets Manager

Kita perlu menyimpan rahasia di Secrets Manager untuk menyimpan kredensial pengguna untuk konektor SFTP Anda. Anda dapat menggunakan kata sandi, kunci pribadi SSH, atau keduanya. Untuk tutorial, kita menggunakan kunci pribadi.

Note

Ketika Anda menyimpan rahasia di Secrets Manager, Anda Akun AWS dikenakan biaya. Untuk informasi tentang harga, lihat [AWS Secrets Manager Harga](#).

Sebelum Anda memulai prosedur untuk menyimpan rahasia, mengambil dan memformat kunci pribadi Anda. Kunci pribadi harus sesuai dengan kunci publik yang dikonfigurasi untuk pengguna di server SFTP jarak jauh. Untuk tutorial kami, kunci pribadi harus sesuai dengan kunci publik yang disimpan untuk pengguna uji kami di server SFTP Transfer Family yang kami gunakan sebagai server jarak jauh.

Untuk melakukan ini, jalankan perintah berikut:

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

Misalnya, jika file kunci pribadi Anda berada di `~/ssh/sftp-testuser-privatekey`, perintahnya adalah sebagai berikut.

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

Ini menghasilkan kunci dalam format yang benar (dengan karakter baris baru yang disematkan) ke output standar. Salin teks ini di suatu tempat, karena Anda harus menempelkannya dalam prosedur berikut (pada langkah 6).

Untuk menyimpan kredensi pengguna di Secrets Manager untuk konektor SFTP

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pada panel navigasi kiri, pilih Rahasia.
3. Pada halaman Rahasia, pilih Simpan rahasia baru.
4. Pada halaman Pilih jenis rahasia, untuk tipe Rahasia, pilih Jenis rahasia lainnya.

5. Di bagian Key/value pasangan, pilih Key/valuetaab.
 - Kunci — Masukkan**Username**.
 - nilai — Masukkan nama pengguna kami,**sftp-testuser**.
6. Untuk memasukkan kunci, kami sarankan Anda menggunakan tab Plaintext.
 - a. Pilih Tambah baris, lalu masukkan**PrivateKey**.
 - b. Pilih tab Plaintext. Bidang sekarang berisi teks berikut:

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

- c. Tempelkan teks untuk kunci pribadi Anda (disimpan sebelumnya) di antara tanda kutip ganda kosong ("").

Layar Anda akan terlihat sebagai berikut (data kunci berwarna abu-abu).



7. Pilih Berikutnya.
8. Pada halaman Konfigurasi rahasia, masukkan nama untuk rahasia Anda. Untuk tutorial ini, kami beri nama rahasianya**aws/transfer/sftp-connector1**.
9. Pilih Berikutnya, dan kemudian terima default pada halaman Konfigurasi rotasi. Lalu pilih Selanjutnya.
10. Pada halaman Review, pilih Store untuk membuat dan menyimpan rahasia.

Buat Resource Gateway (hanya tipe jalan keluar VPC)

Untuk konektor tipe jalan keluar VPC, Anda perlu membuat Resource Gateway di VPC Anda. Resource Gateway berfungsi sebagai titik masuk untuk Akses Cross-VPC Sumber Daya.

Untuk membuat Resource Gateway

1. Jalankan perintah berikut untuk membuat Resource Gateway (ganti ID VPC dan ID subnet dengan nilai Anda):

```
aws vpc-lattice create-resource-gateway \  
  --name my-sftp-resource-gateway \  
  --vpc-identifier vpc-12345678 \  
  --subnet-ids subnet-12345678 subnet-87654321
```

Note

Resource Gateways memerlukan subnet di setidaknya 2 Availability Zone.

2. Perhatikan ID Resource Gateway dari respons untuk digunakan pada langkah berikutnya.

Buat Konfigurasi Sumber Daya (hanya tipe jalan keluar VPC)

Buat Konfigurasi Sumber Daya yang mengarah ke server SFTP Anda. Ini bisa berupa alamat IP pribadi untuk server di VPC Anda, atau nama DNS publik untuk server eksternal. Untuk informasi selengkapnya tentang Konfigurasi Sumber Daya, lihat [Konfigurasi sumber daya](#) di Panduan Pengguna Amazon VPC Lattice.

Untuk membuat Konfigurasi Sumber Daya

1. Untuk server SFTP pribadi, jalankan:

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

2. Untuk server SFTP publik (hanya nama DNS), jalankan:

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

Note

Titik akhir publik harus menggunakan nama DNS, bukan alamat IP.

3. Perhatikan ARN Konfigurasi Sumber Daya dari respons untuk digunakan saat membuat konektor.

Langkah 2: Buat dan uji konektor SFTP

Di bagian ini, kami membuat konektor SFTP yang menggunakan semua sumber daya yang kami buat sebelumnya. Untuk detail selengkapnya, lihat [Membuat konektor SFTP](#).

Untuk membuat konektor SFTP

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor SFTP, lalu pilih Buat konektor SFTP.
3. Untuk tipe Egress, pilih salah satu dari berikut ini:
 - Layanan dikelola (default): Menggunakan infrastruktur terkelola AWS Transfer Family dengan alamat IP statis untuk koneksi keluar.
 - Kisi VPC: Rutekan lalu lintas melalui VPC Anda menggunakan Akses Sumber Daya. Cross-VPC Pilih opsi ini untuk konektivitas titik akhir pribadi atau untuk menggunakan gateway NAT Anda sendiri.

Important

Anda tidak dapat mengubah jenis jalan keluar setelah membuat konektor. Pilih dengan hati-hati berdasarkan persyaratan konektivitas Anda.

4. Di bagian Konfigurasi konektor, berikan informasi berikut:

- Untuk URL, masukkan URL server SFTP jarak jauh. Untuk tutorialnya, kami memasukkan URL server Transfer Family yang kami gunakan sebagai server SFTP jarak jauh.

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

Ganti **1111aaaa2222bbbb3** dengan ID server Transfer Family Anda.

- Untuk peran Access, masukkan peran yang kita buat sebelumnya, **sftp-connector-role**.
- Untuk ARN Konfigurasi Sumber Daya (hanya tipe jalan keluar VPC Lattice), masukkan ARN Konfigurasi Sumber Daya yang Anda buat sebelumnya:

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

- Untuk peran Logging, pilih peran yang menyertakan kebijakan kepercayaan dengan `transfer.amazonaws.com` elemen Principal.

Tip: Selain menambahkan Transfer Family sebagai entitas tepercaya, Anda dapat menambahkan kebijakan `AWSTransferLoggingAccess` AWS terkelola ke peran. Kebijakan ini dijelaskan secara rinci dalam [AWSTransferLoggingAccess](#).

Connector configuration

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

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

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

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

URL of the remote (target) SFTP server

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

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

5. Di bagian Konfigurasi SFTP, berikan informasi berikut:

- Untuk kredensi Connector, pilih nama sumber daya Secrets Manager Anda yang berisi kredensial SFTP. Untuk tutorialnya, pilih **aws/transfer/sftp-connector1**.
- Untuk kunci host Tepercaya, tempel di bagian publik dari kunci host. Anda dapat mengambil kunci ini dengan menjalankan `ssh-keyscan` server SFTP Anda. Untuk detail tentang cara memformat dan menyimpan kunci host tepercaya, lihat dokumentasi tipe [SftpConnectorConfig](#) data.
- Untuk Koneksi bersamaan maksimum, pilih nilai integer dari 1 hingga 5: nilai defaultnya adalah 5.

SFTP configuration Info

Connector credentials Info

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

aws/transfer/sftp-connector1
Store a new secret

Trusted host keys - optional Info

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

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

ssh-rsa AAAAE
Remove

Add trusted host key

Maximum concurrent connections Info

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

5

- Setelah Anda mengkonfirmasi semua pengaturan Anda, pilih **Buat konektor** untuk membuat konektor SFTP.

Anda juga dapat membuat konektor menggunakan AWS Command Line Interface.

- Untuk membuat konektor SFTP dengan jalan keluar yang dikelola layanan, jalankan perintah berikut:

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
```

```
--sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa AAAAB3NzaC..."
```

- Untuk membuat konektor SFTP dengan jalan keluar VPC-based , jalankan perintah berikut:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

Setelah Anda membuat konektor SFTP, kami sarankan Anda mengujinya sebelum mencoba mentransfer file apa pun menggunakan konektor baru Anda.

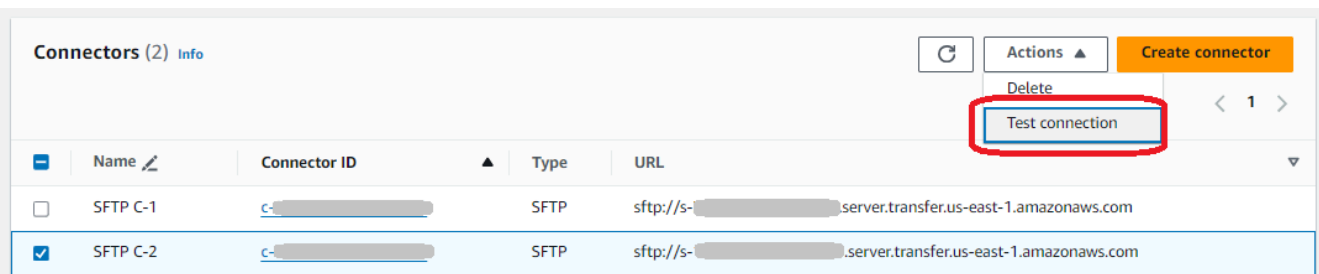
Note

Untuk konektor tipe jalan keluar VPC, resolusi DNS mungkin memakan waktu beberapa menit setelah pembuatan. Selama waktu ini, status konektor akan PENDING dan TestConnection akan kembali “Konektor tidak tersedia”. Tunggu status menjadi ACTIVE sebelum mencoba transfer file.

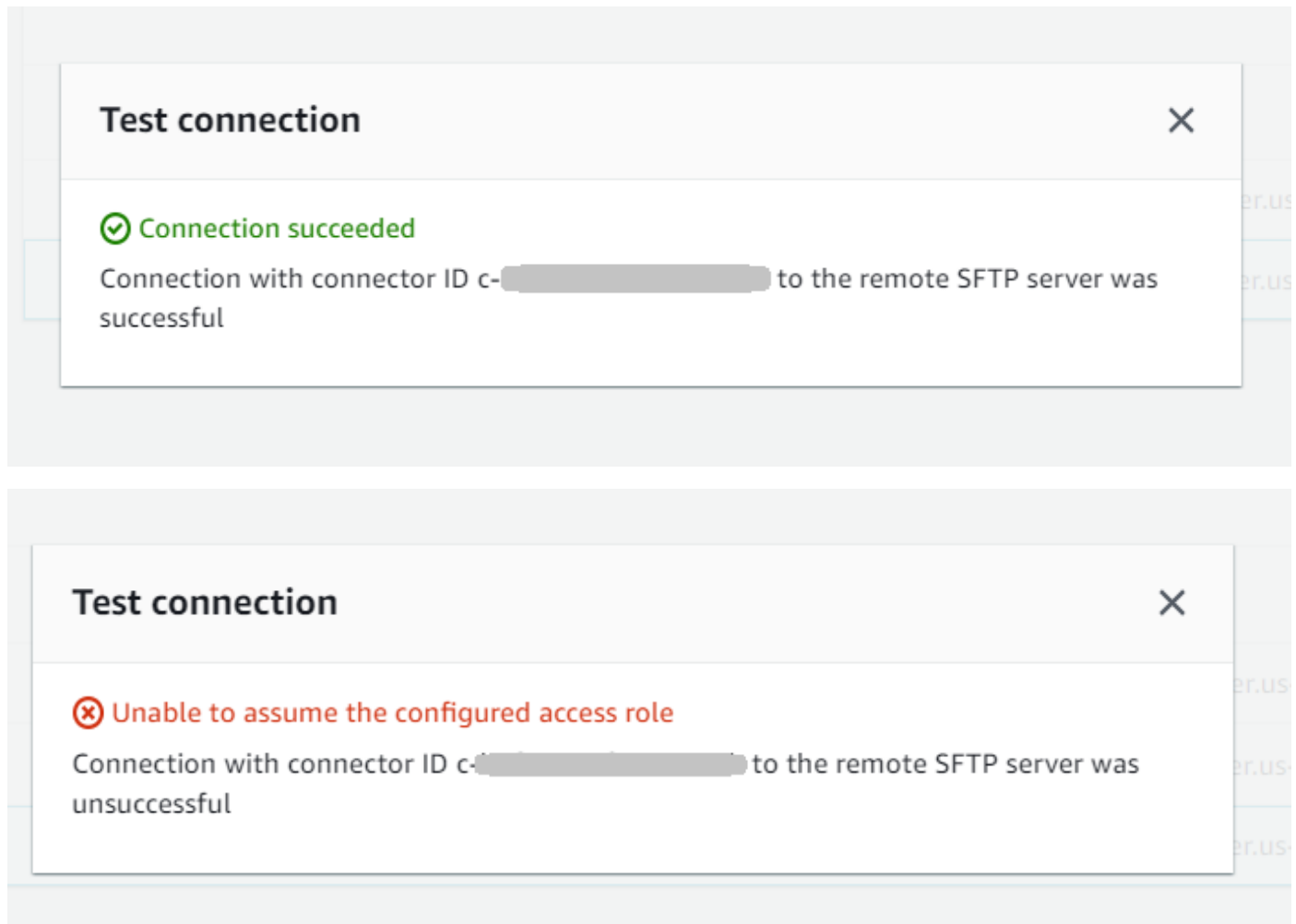
Test a connector using the console

Untuk menguji konektor SFTP

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor SFTP, dan pilih konektor.
3. Dari menu Tindakan, pilih Uji koneksi.



Sistem mengembalikan pesan, menunjukkan apakah tes lulus atau gagal. Jika tes gagal, sistem memberikan pesan kesalahan berdasarkan alasan pengujian gagal.



Test a connector using the CLI

Untuk menguji konektor menggunakan AWS Command Line Interface, jalankan perintah berikut pada prompt perintah (ganti *connector-id* dengan ID konektor Anda yang sebenarnya):

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

Jika tes berhasil, baris berikut dikembalikan:

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

Jika tes tidak berhasil, Anda menerima pesan kesalahan deskriptif, misalnya:

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

Saat Anda menjelaskan konektor tipe jalan keluar VPC, responsnya mencakup bidang baru:

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

Perhatikan bahwa `ServiceManagedEgressIpAddresses` nol untuk konektor tipe jalan keluar VPC karena rute lalu lintas melalui VPC Anda alih-alih infrastruktur terkelola. AWS

Langkah 3: Kirim dan ambil file menggunakan konektor SFTP

Untuk mempermudah, kami berasumsi bahwa Anda sudah memiliki file di bucket Amazon S3 Anda.

Note

Tutorial ini menggunakan bucket Amazon S3 untuk lokasi penyimpanan sumber dan tujuan. Jika server SFTP Anda tidak menggunakan penyimpanan Amazon S3, maka di mana pun

Anda `sftp-server-storage-east` melihat dalam perintah berikut, Anda dapat mengganti jalur dengan jalur ke lokasi file yang dapat diakses dari server SFTP Anda.

- Kami mengirim file bernama `SEND-to-SERVER.txt` dari penyimpanan Amazon S3 ke server SFTP.
- Kami mengambil file bernama `RETRIEVE-to-S3.txt` dari server SFTP ke penyimpanan Amazon S3.

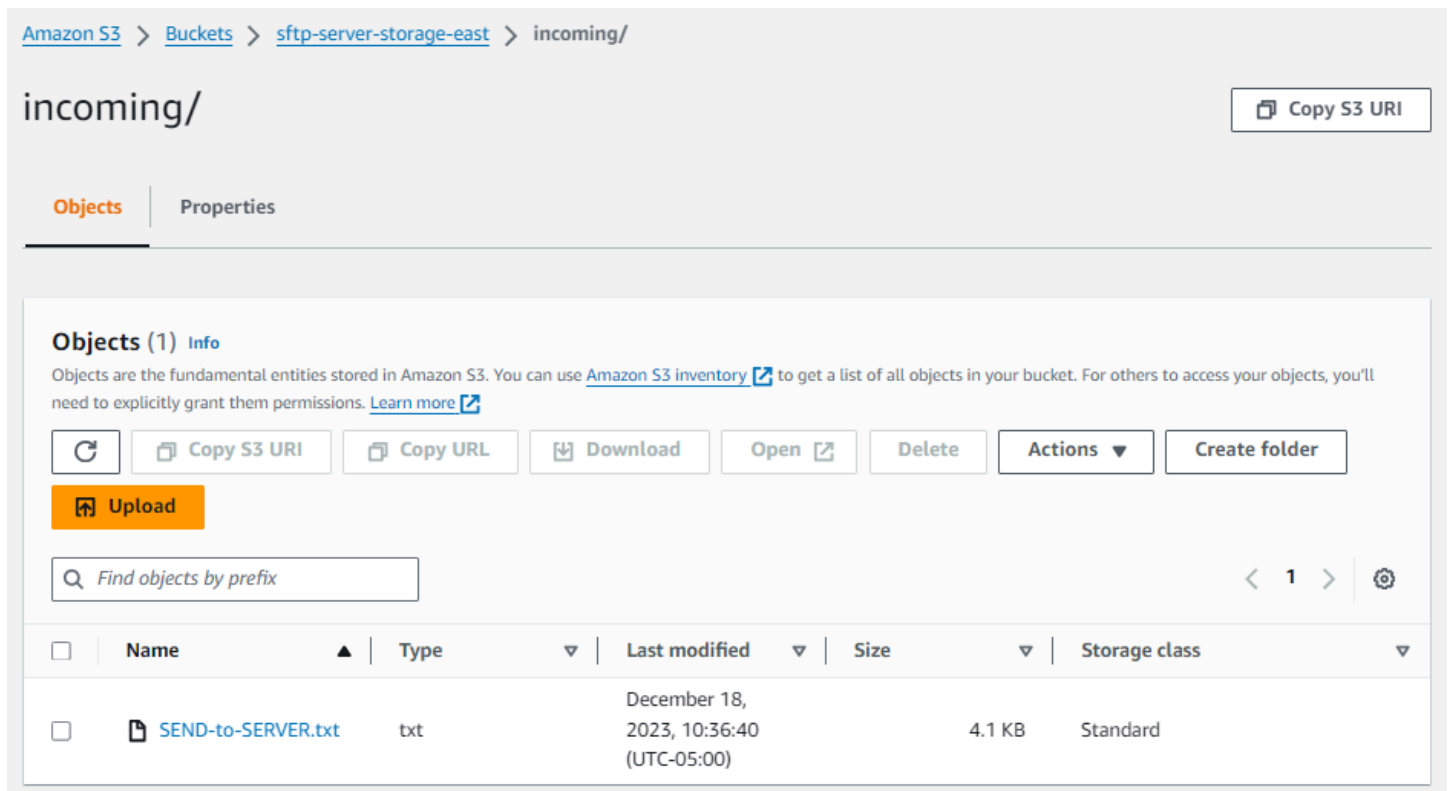
 Note

Dalam perintah berikut, ganti *connector-id* dengan ID konektor Anda.

Pertama, kami mengirim file dari bucket Amazon S3 kami ke server SFTP jarak jauh. Dari command prompt, jalankan perintah berikut:

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

`sftp-server-storage-east` Ember Anda sekarang akan terlihat seperti ini.



Jika Anda tidak melihat file seperti yang diharapkan, periksa CloudWatch log Anda.

Untuk memeriksa CloudWatch log Anda

1. Buka CloudWatch konsol Amazon di <https://console.aws.amazon.com/cloudwatch/>
2. Pilih Grup log dari menu navigasi kiri.
3. Masukkan ID konektor Anda di bilah pencarian untuk menemukan log Anda.
4. Pilih aliran Log yang dikembalikan dari pencarian.
5. Perluas entri log terbaru.

Jika berhasil, entri log terlihat seperti berikut:

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

```

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

```

Jika transfer file gagal, entri log berisi pesan kesalahan yang menentukan masalah. Penyebab umum kesalahan adalah masalah dengan izin IAM dan jalur file yang salah.

Selanjutnya, kami mengambil file dari server SFTP ke bucket Amazon S3. Dari command prompt, jalankan perintah berikut:

```

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

```

Jika transfer berhasil, bucket Amazon S3 Anda berisi file yang ditransfer, seperti yang ditunjukkan di sini.

The screenshot shows the Amazon S3 console interface. The breadcrumb navigation at the top reads: [Amazon S3](#) > [Buckets](#) > [sftp-server-storage-east](#) > [incoming/](#). The main heading is 'incoming/' with a 'Copy S3 URI' button. Below this are tabs for 'Objects' (selected) and 'Properties'. The 'Objects (1) Info' section explains that objects are fundamental entities in Amazon S3 and provides a link to 'Amazon S3 inventory'. Below the text are several action buttons: Refresh, Copy S3 URI, Copy URL, Download, Open, Delete, Actions (dropdown), and Create folder. An 'Upload' button is also present. A search bar with the placeholder 'Find objects by prefix' is shown. At the bottom, a table lists the objects in the bucket:

☐	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

Jika berhasil, entri log terlihat seperti berikut:

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

Memecahkan masalah konektor tipe jalan keluar VPC

Jika Anda mengalami masalah dengan konektor tipe jalan keluar VPC, periksa hal berikut:

- Status konektor TERTUNDA: Resolusi DNS untuk konektor VPC dapat memakan waktu beberapa menit. Tunggu status menjadi AKTIF sebelum mencoba koneksi.
- Batas waktu koneksi: Verifikasi bahwa grup keamanan mengizinkan lalu lintas di port 22 antara subnet Resource Gateway Anda dan server SFTP target.
- Kesalahan Konfigurasi Sumber Daya: Pastikan Konfigurasi Sumber Daya Anda menunjuk ke alamat IP atau nama DNS yang benar, dan bahwa Resource Gateway berada di VPC yang sama dengan server SFTP Anda (untuk titik akhir pribadi). Untuk informasi selengkapnya, lihat [Konfigurasi sumber daya](#) di Panduan Pengguna Amazon VPC Lattice.
- Masalah titik akhir publik: Untuk titik akhir publik, pastikan Anda menggunakan nama DNS, bukan alamat IP, dalam Konfigurasi Sumber Daya Anda. Verifikasi bahwa VPC Anda memiliki NAT Gateway untuk akses internet keluar.
- Ketersediaan AZ: Resource Gateways memerlukan subnet di setidaknya 2 Availability Zone. Tidak semua AZ mendukung VPC Lattice - periksa AZ yang didukung di wilayah Anda.

Pertimbangan biaya untuk jenis jalan keluar VPC:

- VPC Lattice mengenakan biaya \$0.006/GB untuk pemrosesan data sebagai penyedia sumber daya (ditagih langsung oleh VPC Lattice)

- AWS Transfer Family menyerap \$0.01/GB biaya konsumen sumber daya (1 PB pertama)
- Untuk titik akhir publik melalui VPC, Gateway NAT tambahan dan biaya transfer data mungkin berlaku
- Tidak ada biaya Transfer Family tambahan di luar standar \$0.40/GB biaya pemrosesan data

Prosedur untuk membuat server Transfer Family untuk digunakan sebagai server SFTP jarak jauh Anda

Berikut ini, kami menguraikan langkah-langkah untuk membuat server Transfer Family yang berfungsi sebagai server SFTP jarak jauh Anda untuk tutorial ini. Perhatikan hal-hal berikut:

- Kami menggunakan server Transfer Family untuk mewakili server SFTP jarak jauh. Pengguna konektor SFTP yang khas memiliki server SFTP jarak jauh mereka sendiri. Lihat [Buat server SFTP Transfer Family dan pengguna](#).
- Karena kami menggunakan server Transfer Family, kami juga menggunakan pengguna SFTP yang dikelola layanan. Dan, untuk kesederhanaan, kami menggabungkan izin yang dibutuhkan pengguna ini untuk mengakses server Transfer Family dengan izin yang mereka butuhkan untuk menggunakan konektor kami. Sekali lagi, sebagian besar kasus penggunaan konektor SFTP memiliki pengguna SFTP terpisah yang tidak terkait dengan server Transfer Family. Lihat [Buat server SFTP Transfer Family dan pengguna](#).
- Untuk tutorial, karena kita menggunakan penyimpanan Amazon S3 untuk server SFTP jarak jauh kita, kita perlu membuat ember kedua, **sftp-server-storage-east**, sehingga kita dapat mentransfer file dari satu ember ke ember lainnya.

Buat server SFTP Transfer Family dan pengguna

Sebagian besar pengguna tidak perlu membuat server SFTP Transfer Family dan pengguna, karena Anda sudah memiliki server SFTP dengan pengguna, dan Anda dapat menggunakan server ini untuk mentransfer file ke dan dari. Namun, untuk tutorial ini, untuk kesederhanaan, kami menggunakan server Transfer Family untuk berfungsi sebagai server SFTP jarak jauh.

Ikuti prosedur yang dijelaskan dalam [Buat SFTP-enabled server](#) untuk membuat server, dan [Langkah 3: Tambahkan pengguna yang dikelola layanan](#) untuk menambahkan pengguna. Ini adalah detail pengguna yang kami gunakan untuk tutorial:

- Buat pengguna yang dikelola layanan Anda, **sftp-testuser**

- Mengatur direktori home ke `/sftp-server-storage-east/sftp-testuser`
- Saat Anda membuat pengguna, Anda menyimpan kunci publik. Kemudian, ketika Anda membuat rahasia di Secrets Manager, Anda perlu memberikan kunci pribadi yang sesuai.
- Peran: `sftp-connector-role`. Untuk tutorial, kami menggunakan peran IAM yang sama untuk pengguna SFTP kami dan untuk mengakses konektor SFTP. Saat membuat konektor untuk organisasi, Anda mungkin memiliki peran pengguna dan akses yang terpisah.
- Kunci host server: Anda perlu menggunakan kunci host server saat membuat konektor. Anda dapat mengambil kunci ini dengan menjalankan `ssh-keyscan` server Anda. Misalnya, jika ID server Anda `s-1111aaaa2222bbbb3`, dan titik akhirnya `masukus-east-1`, perintah berikut mengambil kunci host server:

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

Salin teks ini di suatu tempat, karena Anda harus menempelkannya dalam [Langkah 2: Buat dan uji konektor SFTP](#) prosedur.

Gabungan peran pengguna dan akses

Untuk tutorial, kita menggunakan peran tunggal gabungan. Kami menggunakan peran ini baik untuk pengguna SFTP kami, maupun untuk akses ke konektor. Contoh berikut berisi rincian untuk peran ini, jika Anda ingin melakukan tugas-tugas dalam tutorial.

Contoh berikut memberikan izin yang diperlukan untuk mengakses dua bucket kami di Amazon S3, dan rahasia bernama disimpan di `aws/transfer/sftp-connector1` Secrets Manager. Untuk tutorial, peran ini diberi nama `sftp-connector-role`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::sftp-server-storage-east",
```

```

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

```

Untuk detail lengkap tentang membuat peran untuk Transfer Family, ikuti prosedur yang dijelaskan [Membuat peran pengguna](#) untuk membuat peran.

Menyiapkan metode Amazon API Gateway sebagai penyedia identitas kustom

Tutorial ini menggambarkan cara menyiapkan metode Amazon API Gateway dan menggunakannya sebagai penyedia identitas khusus untuk mengunggah file ke AWS Transfer Family server. Tutorial ini menggunakan [template stack Dasar](#), dan fungsi dasar lainnya sebagai contoh saja.

Topik

- [Prasyarat](#)
- [Langkah 1: Buat CloudFormation tumpukan](#)
- [Langkah 2: Periksa konfigurasi metode API Gateway untuk server Anda](#)
- [Langkah 3: Lihat detail server Transfer Family](#)
- [Langkah 4: Uji apakah pengguna Anda dapat terhubung ke server](#)
- [Langkah 5: Uji koneksi SFTP dan transfer file](#)
- [Langkah 6: Batasi akses ke ember](#)
- [Perbarui Lambda jika menggunakan Amazon EFS](#)

Prasyarat

Sebelum Anda membuat resource Transfer Family di CloudFormation, buat penyimpanan dan peran pengguna Anda.

Untuk menentukan penyimpanan dan membuat peran pengguna

1. Bergantung pada penyimpanan yang Anda gunakan, lihat dokumentasi berikut:
 - Untuk membuat bucket Amazon S3, lihat [Bagaimana cara membuat bucket S3?](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
 - Untuk membuat sistem file Amazon EFS, lihat [Konfigurasi sistem file Amazon EFS](#).
2. Untuk membuat peran pengguna, lihat [Buat peran dan kebijakan IAM](#)

Anda memasukkan detail untuk penyimpanan Anda dan peran pengguna Anda ketika Anda membuat CloudFormation tumpukan Anda di bagian berikutnya.

Langkah 1: Buat CloudFormation tumpukan

Untuk membuat AWS CloudFormation tumpukan dari template yang disediakan

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pilih Buat tumpukan, dan pilih Dengan sumber daya baru (standar).
3. Di panel Prasyarat - Siapkan templat, pilih Pilih templat yang ada.
4. Salin tautan ini, [template tumpukan dasar](#), dan tempel ke bidang URL Amazon S3.

5. Klik Berikutnya.
6. Tentukan parameter, termasuk nama untuk tumpukan Anda. Pastikan untuk melakukan hal berikut:
 - Ganti nilai default untuk UserNamedan UserPassword.
 - Untuk UserHomeDirectory, masukkan detail penyimpanan (baik bucket Amazon S3 atau sistem file Amazon EFS) yang Anda buat sebelumnya.
 - Ganti default UserRoleArndengan peran pengguna yang Anda buat sebelumnya. Peran AWS Identity and Access Management (IAM) harus memiliki izin yang sesuai. Untuk contoh peran IAM dan kebijakan bucket, lihat[Langkah 6: Batasi akses ke ember](#).
 - Jika Anda ingin mengautentikasi menggunakan kunci publik alih-alih kata sandi, masukkan kunci publik Anda di UserPublicKey1bidang. Pertama kali Anda terhubung ke server menggunakan SFTP, Anda kemudian memberikan kunci pribadi alih-alih kata sandi.
7. Pilih Berikutnya, lalu pilih Berikutnya lagi di halaman Configure stack options.
8. Tinjau detail tumpukan yang Anda buat, lalu pilih Buat tumpukan.

 Note

Di bagian bawah halaman, di bawah Kemampuan, Anda harus mengakui bahwa CloudFormation mungkin membuat sumber daya IAM.

Langkah 2: Periksa konfigurasi metode API Gateway untuk server Anda

 Note

Untuk meningkatkan keamanan, Anda dapat mengkonfigurasi firewall aplikasi web. AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke Amazon API Gateway. Lihat perinciannya di [Tambahkan firewall aplikasi web](#).

Jangan aktifkan caching API Gateway

Jangan aktifkan caching untuk metode API Gateway Anda saat menggunakannya sebagai penyedia identitas khusus untuk Transfer Family. Caching tidak pantas dan tidak valid untuk permintaan otentikasi karena:

- Setiap permintaan otentikasi unik dan memerlukan respons langsung, bukan respons yang di-cache
- Caching tidak memberikan manfaat karena Transfer Family tidak pernah mengirimkan permintaan duplikat atau berulang ke API Gateway
- Mengaktifkan caching akan menyebabkan API Gateway merespons dengan data yang tidak cocok, sehingga respons yang tidak valid terhadap permintaan otentikasi

Untuk memeriksa konfigurasi metode API Gateway untuk server Anda dan menerapkannya

1. Buka konsol API Gateway di <https://console.aws.amazon.com/apigateway/>.
2. Pilih API template dasar Transfer Custom Identity Provider yang dihasilkan CloudFormation template.
3. Di panel Resources, pilih GET, lalu pilih Method Request.
4. Untuk Tindakan, pilih Deploy API. Untuk tahap Deployment, pilih prod, lalu pilih Deploy.

Setelah metode API Gateway berhasil diterapkan, lihat kinerjanya di bagian Editor Panggung.

Note

Salin alamat URL Invoke yang muncul di bagian atas halaman. Anda akan membutuhkannya untuk langkah selanjutnya.

Langkah 3: Lihat detail server Transfer Family

Saat Anda menggunakan template untuk membuat CloudFormation tumpukan, server Transfer Family dibuat secara otomatis.

Untuk melihat detail server Transfer Family

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pilih tumpukan yang Anda buat.
3. Pilih tab Sumber Daya.

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	

Server ARN ditampilkan di kolom Physical ID untuk baris. TransferServer ID server terkandung dalam ARN, misalnya s-11112222333344445.

4. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>, dan pada halaman Server, pilih server baru.

ID server cocok dengan ID yang ditampilkan untuk TransferServersumber daya di CloudFormation.

Langkah 4: Uji apakah pengguna Anda dapat terhubung ke server

Untuk menguji apakah pengguna Anda dapat terhubung ke server, menggunakan konsol Transfer Family

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Pada halaman Server, pilih server baru Anda, pilih Tindakan, lalu pilih Uji.
3. Masukkan teks untuk kredensi login Anda ke dalam bidang Nama Pengguna, dan ke bidang Kata Sandi. Ini adalah nilai yang Anda tetapkan saat Anda menerapkan CloudFormation tumpukan.
4. Untuk Protokol Server, pilih SFTP, dan untuk IP Sumber, masukkan. **127.0.0.1**
5. Pilih Uji.

Jika otentikasi pengguna berhasil, pengujian mengembalikan respons StatusCode: 200 HTML dan objek JSON yang berisi rincian peran dan izin pengguna. Contoh:

```
{
  "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\"
}
```

Jika pengujian gagal, tambahkan salah satu kebijakan yang AWS dikelola API Gateway ke peran yang Anda gunakan untuk API Anda.

Langkah 5: Uji koneksi SFTP dan transfer file

Untuk menguji koneksi SFTP

1. Pada perangkat Linux atau macOS, buka terminal perintah.

2. Masukkan salah satu perintah berikut, tergantung pada apakah Anda menggunakan kata sandi atau key pair untuk otentikasi.

- Jika Anda menggunakan kata sandi, masukkan perintah ini:

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

Saat diminta, masukkan kata sandi Anda.

- Jika Anda menggunakan key pair, masukkan perintah ini:

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

Note

Untuk sftp perintah ini, masukkan kode Wilayah AWS tempat server Transfer Family Anda berada. Misalnya, jika server Anda berada di AS Timur (Ohio), masukkan **us-east-2**.

3. Pada sftp> prompt, pastikan bahwa Anda dapat meng-upload (put), download (get), dan melihat direktori dan file (pwd dan ls).

Langkah 6: Batasi akses ke ember

Anda dapat membatasi siapa yang dapat mengakses bucket Amazon S3 tertentu. Contoh berikut menunjukkan setelan yang akan digunakan di CloudFormation tumpukan Anda dan dalam kebijakan yang Anda pilih untuk pengguna Anda.

Dalam contoh ini, kami menetapkan parameter berikut untuk CloudFormation tumpukan:

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

⚠ Important

Ini adalah contoh kata sandi. Saat mengonfigurasi metode API Gateway, pastikan Anda memasukkan kata sandi yang kuat.

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

UserPublicKey1Ini adalah kunci publik yang telah Anda hasilkan sebagai bagian dari public/private key pair.

*role-id*Ini unik untuk peran pengguna yang Anda buat. Kebijakan yang dilampirkan myuser-api-gateway-role adalah sebagai berikut:

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

Untuk terhubung ke server menggunakan SFTP, masukkan salah satu perintah berikut pada prompt.

- Jika Anda menggunakan kata sandi untuk mengautentikasi, jalankan perintah berikut:

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

Saat diminta, masukkan kata sandi Anda.

- Jika Anda menggunakan key pair untuk mengautentikasi, jalankan perintah berikut:

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

Note

Untuk sftp perintah ini, gunakan ID Wilayah AWS tempat server Transfer Family Anda berada. Misalnya, jika server Anda berada di AS Timur (Ohio), gunakan us-east-2.

Pada sftp prompt, Anda diarahkan ke direktori home Anda, yang dapat Anda lihat dengan menjalankan pwd perintah. Contoh:

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

Pengguna tidak dapat melihat direktori apa pun di atas direktori home. Contoh:

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

Perbarui Lambda jika menggunakan Amazon EFS

Jika Anda memilih Amazon EFS sebagai opsi penyimpanan untuk server Transfer Family, Anda perlu mengedit fungsi lambda untuk tumpukan Anda.

Untuk menambahkan profil Posix ke fungsi Lambda Anda

1. Buka konsol Lambda di <https://console.aws.amazon.com/lambda/>
2. Pilih fungsi Lambda yang Anda buat sebelumnya. Fungsi Lambda memiliki format **stack-name-GetUserConfigLambda-lambda-identifier**, di mana **stack-name** nama CloudFormation tumpukan dan **lambda-identifier** merupakan pengidentifikasi untuk fungsi tersebut.
3. Di tab Kode, pilih index.js untuk menampilkan kode untuk fungsi tersebut.
4. Dalam response, tambahkan baris berikut antara Policy dan HomeDirectory:

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

Dimana **uid-value** dan **gid-value** merupakan bilangan bulat, 0 atau lebih besar, yang mewakili ID Pengguna dan ID Grup masing-masing.

Misalnya, setelah Anda menambahkan profil Posix, bidang respons mungkin terlihat seperti berikut:

```
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 '/'  
};
```

Menyiapkan konfigurasi AS2

Tutorial ini membahas cara mengatur konfigurasi Applicability Statement 2 (AS2) dengan AWS Transfer Family. Setelah Anda menyelesaikan langkah-langkah yang dijelaskan di sini, Anda akan memiliki AS2-enabled server yang siap menerima pesan AS2 dari mitra dagang sampel. Anda juga akan memiliki konektor yang dapat digunakan untuk mengirim pesan AS2 ke mitra dagang sampel.

Note

Beberapa bagian dari pengaturan contoh menggunakan AWS Command Line Interface (AWS CLI). Jika Anda belum menginstal AWS CLI, lihat [Menginstal atau memperbarui versi terbaru dari AWS CLI](#) Panduan AWS Command Line Interface Pengguna.

1. Buat sertifikat untuk diri sendiri dan mitra dagang Anda. Jika Anda memiliki sertifikat yang dapat Anda gunakan, Anda dapat melewati bagian ini.

Proses ini dijelaskan di [Langkah 1: Buat sertifikat untuk AS2](#).

2. Impor sertifikat yang Anda buat di langkah 1.

Proses ini dijelaskan di [Langkah 2: Impor sertifikat sebagai sumber sertifikat Transfer Family](#).

3. Untuk mengatur mitra dagang Anda, buat profil lokal dan profil mitra.

Proses ini dijelaskan di [Langkah 3: Buat profil untuk Anda dan mitra dagang Anda](#).

4. Buat AWS Transfer Family server yang menggunakan protokol AS2. Secara opsional, Anda dapat menambahkan alamat IP Elastis ke server untuk membuatnya menghadap ke internet.

Proses ini dijelaskan di [Langkah 4: Buat server Transfer Family yang menggunakan protokol AS2](#).

 Note

Anda harus membuat server Transfer Family hanya untuk transfer masuk. Jika Anda hanya melakukan transfer keluar, Anda tidak memerlukan server Transfer Family.

5. Buat perjanjian antara Anda dan mitra dagang Anda.

Proses ini dijelaskan di [Langkah 5: Buat kesepakatan antara Anda dan pasangan](#).

 Note

Anda harus membuat perjanjian untuk transfer masuk saja. Jika Anda hanya melakukan transfer keluar, Anda tidak memerlukan perjanjian.

6. Buat konektor antara Anda dan mitra dagang Anda.

Proses ini dijelaskan di [Langkah 6: Buat konektor antara Anda dan pasangan](#).

 Note

Anda harus membuat konektor untuk transfer keluar saja. Jika Anda hanya melakukan transfer masuk, Anda tidak memerlukan konektor.

7. Uji pertukaran file AS2.

Proses ini dijelaskan di [Langkah 7: Uji pertukaran file melalui AS2 dengan menggunakan Transfer Family](#).

Setelah Anda menyelesaikan langkah-langkah ini, Anda dapat melakukan hal berikut:

- Kirim file ke server AS2-enabled mitra jarak jauh dengan perintah Transfer Family `start-file-transfer` AWS Command Line Interface (AWS CLI).
- Terima file dari server AS2-enabled mitra jarak jauh di port 5080 melalui titik akhir virtual private cloud (VPC) Anda.

Langkah 1: Buat sertifikat untuk AS2

Kedua belah pihak dalam pertukaran AS2 membutuhkan X.509 sertifikat. Anda dapat membuat sertifikat ini dengan cara apa pun yang Anda sukai. Topik ini menjelaskan cara menggunakan [OpenSSL](#) dari baris perintah untuk membuat sertifikat root, dan kemudian menandatangani sertifikat bawahan. Kedua belah pihak harus membuat sertifikat mereka sendiri.

Note

Panjang kunci untuk sertifikat AS2 harus minimal 2048 bit, dan paling banyak 4096.

Untuk mentransfer file dengan mitra, perhatikan hal-hal berikut:

- Anda dapat melampirkan sertifikat ke profil. Sertifikat berisi kunci publik atau pribadi.
- Mitra dagang Anda mengirimkan Anda kunci publik mereka, dan Anda mengirimkannya milik Anda.
- Mitra dagang Anda mengenkripsi pesan dengan kunci publik Anda dan menandatangani dengan kunci pribadi mereka. Sebaliknya, Anda mengenkripsi pesan dengan kunci publik mitra Anda dan menandatangani dengan kunci pribadi Anda.

Note

Jika Anda lebih suka mengelola kunci dengan GUI, [Portecle](#) adalah salah satu opsi yang dapat Anda gunakan.

Untuk menghasilkan contoh sertifikat

Important

Jangan mengirim kunci pribadi Anda kepada pasangan Anda. Dalam contoh ini, Anda membuat satu set kunci publik dan pribadi yang ditandatangani sendiri untuk satu pihak. Jika Anda akan bertindak sebagai mitra dagang untuk tujuan pengujian, Anda dapat mengulangi instruksi ini untuk menghasilkan dua set kunci: satu untuk setiap mitra dagang. Dalam hal ini, Anda tidak perlu menghasilkan dua otoritas sertifikat root (CA).

1. Jalankan perintah berikut untuk menghasilkan kunci pribadi RSA dengan modulus 2048-bit-long.

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

2. Jalankan perintah berikut untuk membuat sertifikat yang ditandatangani sendiri dengan root-ca-key.pem file Anda.

```
/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 Argumen terdiri dari nilai-nilai berikut.

	Nama	Deskripsi
C	Kode negara	Kode dua huruf untuk negara tempat organisasi Anda berada.
ST	Negara bagian, wilayah, atau provinsi	Negara bagian, wilayah, atau provinsi tempat organisasi Anda berada. (Dalam hal ini, wilayah tidak mengacu pada Anda Wilayah AWS.)

	Nama	Deskripsi
L	Nama lokal	Kota tempat organisasi Anda berada.
O	Nama Organisasi	Nama resmi lengkap organisasi Anda, termasuk sufiks, seperti LLC, Corp, dan sebagainya.
OU	Nama unit organisasi	Divisi dalam organisasi Anda yang berhubungan dengan sertifikat ini.
CN	Nama umum atau nama domain yang sepenuhnya memenuhi syarat (FQDN)	Dalam hal ini, kami membuat sertifikat root, jadi nilainya R00TCA. Dalam contoh-contoh ini, kami menggunakan CN untuk menggambarkan tujuan sertifikat.

3. Buat kunci penandatanganan dan kunci enkripsi untuk profil lokal Anda.

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

Note

Beberapa AS2-enabled server, seperti OpenAS2, mengharuskan Anda menggunakan sertifikat yang sama untuk penandatanganan dan enkripsi. Dalam hal ini, Anda dapat mengimpor kunci pribadi dan sertifikat yang sama untuk kedua tujuan. Untuk melakukannya, jalankan perintah ini alih-alih dua perintah sebelumnya:

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

4. Jalankan perintah berikut untuk membuat Permintaan Penandatanganan Sertifikat (CSR) agar kunci root ditandatangani.

```
/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. Selanjutnya, Anda harus membuat `signing-cert.conf` file dan `encryption-cert.conf` file.

- Gunakan editor teks untuk membuat `signing-cert.conf` file dengan konten berikut:

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

- Gunakan editor teks untuk membuat `encryption-cert.conf` file dengan konten berikut:

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

6. Terakhir, Anda membuat sertifikat yang ditandatangani dengan menjalankan perintah berikut.

```
/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
```

Langkah 2: Impor sertifikat sebagai sumber sertifikat Transfer Family

Prosedur ini menjelaskan cara mengimpor sertifikat dengan menggunakan AWS CLI. Jika Anda ingin menggunakan konsol Transfer Family sebagai gantinya, lihat [the section called “Impor sertifikat AS2”](#).

Untuk mengimpor sertifikat penandatanganan dan enkripsi yang Anda buat di langkah 1, jalankan `import-certificate` perintah berikut. Jika Anda menggunakan sertifikat yang sama untuk

enkripsi dan penandatanganan, impor sertifikat yang sama dua kali (sekali dengan SIGNING penggunaan dan sekali lagi dengan ENCRYPTION penggunaan).

Note

Jika Anda memiliki file yang berisi sertifikat dan rantainya, Anda dapat memberikan file itu ke `import-certificate` perintah hanya menggunakan `certificate` parameter. Contoh:

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

Jika Anda menggunakan `certificate` parameter untuk mengunggah sertifikat dan rantainya, jangan gunakan `certificate-chain` parameter.

Jika Anda menggabungkan sertifikat dan rantainya, kunci Anda diformat menggunakan standar PEM konvensional, yang mencakup baris baru “\n” setiap 64 karakter. Sertifikat yang disimpan secara fungsional setara dengan yang Anda unggah, dengan satu-satunya perbedaan bahwa `DescribeCertificate` respons melalui AWS CLI akan berisi karakter baris baru ini.

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

Perintah ini mengembalikan penandatanganan `AndaCertificateId`. Pada bagian selanjutnya, ID sertifikat ini disebut sebagai *my-signing-cert-id*.

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

Perintah ini mengembalikan enkripsi `AndaCertificateId`. Pada bagian selanjutnya, ID sertifikat ini disebut sebagai *my-encrypt-cert-id*.

Selanjutnya, impor enkripsi mitra Anda dan tandatangani sertifikat dengan menjalankan perintah berikut.

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

```
--certificate-chain file://partner-root-ca.pem
```

Perintah ini mengembalikan enkripsi pasangan AndaCertificateId. Pada bagian selanjutnya, ID sertifikat ini disebut sebagai*partner-encrypt-cert-id*.

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

Perintah ini mengembalikan penandatanganan pasangan AndaCertificateId. Pada bagian selanjutnya, ID sertifikat ini disebut sebagai*partner-signing-cert-id*.

Langkah 3: Buat profil untuk Anda dan mitra dagang Anda

Prosedur ini menjelaskan cara membuat profil AS2 dengan menggunakan AWS CLI. Jika Anda ingin menggunakan konsol Transfer Family sebagai gantinya, lihat [the section called “Buat profil AS2”](#).

Buat profil AS2 lokal Anda dengan menjalankan perintah berikut. Perintah ini mereferensikan sertifikat yang berisi kunci publik dan pribadi Anda.

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

Perintah ini mengembalikan ID profil Anda. Pada bagian selanjutnya, ID ini disebut sebagai*my-profile-id*.

Sekarang buat profil mitra dengan menjalankan perintah berikut. Perintah ini hanya menggunakan sertifikat kunci publik mitra Anda. Untuk menggunakan perintah ini, ganti *user input placeholders* dengan informasi Anda sendiri; misalnya, nama AS2 mitra Anda dan ID sertifikat.

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

Perintah ini mengembalikan ID profil mitra Anda. Pada bagian selanjutnya, ID ini disebut sebagai*partner-profile-id*.

 Note

Dalam perintah sebelumnya, ganti **MYCORP** dengan nama organisasi Anda, dan **PARTNER-COMPANY** dengan nama organisasi mitra dagang Anda.

Langkah 4: Buat server Transfer Family yang menggunakan protokol AS2

Prosedur ini menjelaskan cara membuat AS2-enabled server dengan menggunakan Transfer Family AWS CLI.

 Note

Banyak contoh langkah menggunakan perintah yang memuat parameter dari file. Untuk detail selengkapnya tentang menggunakan file untuk memuat parameter, lihat [Cara memuat parameter dari file](#).

Jika Anda ingin menggunakan konsol sebagai gantinya, lihat [Membuat server AS2 menggunakan konsol Transfer Family](#).

Mirip dengan cara Anda membuat AWS Transfer Family server SFTP atau FTPS, Anda membuat AS2-enabled server dengan menggunakan `--protocols AS2` parameter perintah `create-server` AWS CLI. Saat ini, Transfer Family hanya mendukung tipe titik akhir VPC dan penyimpanan Amazon S3 dengan protokol AS2.

Saat Anda membuat AS2-enabled server untuk Transfer Family dengan menggunakan `create-server` perintah, titik akhir VPC secara otomatis dibuat untuk Anda. Endpoint ini mengekspos port TCP 5080 sehingga dapat menerima pesan AS2.

Jika Anda ingin mengekspos titik akhir VPC Anda secara publik ke internet, Anda dapat mengaitkan alamat IP Elastis dengan titik akhir VPC Anda.

Untuk menggunakan petunjuk ini, Anda memerlukan yang berikut:

- ID VPC Anda (misalnya, `vpc-abcdef01`).
- ID subnet VPC Anda (misalnya, `subnet-abcdef01`, `subnet-subnet-abcdef01`, `subnet-021345ab`).
- Satu atau lebih ID grup keamanan yang memungkinkan lalu lintas masuk pada port TCP 5080 dari mitra dagang Anda (misalnya, `sg-1234567890abcdef0` dan `sg-abcdef01234567890`).

- (Opsional) Alamat IP Elastis yang ingin Anda kaitkan dengan titik akhir VPC Anda.
- Jika mitra dagang Anda tidak terhubung ke VPC Anda melalui VPN, Anda memerlukan gateway internet. Untuk informasi selengkapnya, lihat [Hubungkan ke internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

Untuk membuat AS2-enabled server

1. Jalankan perintah berikut. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
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. (Opsional) Anda dapat membuat titik akhir VPC menjadi publik. Anda dapat melampirkan alamat IP Elastis ke server Transfer Family hanya melalui update-server operasi. Perintah berikut menghentikan server, memperbaruinya dengan alamat IP Elastis, dan kemudian mulai lagi.

```
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-abcd012345cccccc
```

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

start-serverPerintah ini secara otomatis membuat catatan DNS untuk Anda yang berisi alamat IP publik untuk server Anda. Untuk memberi mitra dagang Anda akses ke server, Anda memberi mereka informasi berikut. Dalam hal ini, *your-region* mengacu pada Anda Wilayah AWS.

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

URL lengkap yang Anda berikan kepada mitra dagang Anda adalah sebagai berikut:


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

3. Untuk menguji apakah AS2-enabled server Anda dapat diakses, gunakan perintah berikut. Pastikan server Anda dapat diakses baik melalui alamat DNS pribadi titik akhir VPC Anda, atau melalui titik akhir publik Anda (jika Anda mengaitkan alamat IP Elastis dengan titik akhir Anda).

Jika server Anda dikonfigurasi dengan benar, koneksi akan berhasil. Namun, Anda akan menerima respons kode status HTTP 400 (Permintaan Buruk) karena Anda tidak mengirim pesan AS2 yang valid.

- Untuk titik akhir publik (jika Anda mengaitkan alamat IP Elastis pada langkah sebelumnya), jalankan perintah berikut, ganti ID server dan Region Anda.

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

- Jika Anda terhubung dalam VPC Anda, cari nama DNS pribadi titik akhir VPC Anda dengan menjalankan perintah berikut.

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

`describe-server` Perintah ini mengembalikan ID titik akhir VPC Anda dalam parameter `VpcEndpointId`. Gunakan nilai ini untuk menjalankan perintah berikut.

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

`describe-vpc-endpoints` Perintah ini mengembalikan `DNSEntries` array, dengan beberapa `DnsName` parameter. Gunakan nama DNS Regional (yang tidak menyertakan Availability Zone) dalam perintah berikut.

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

Misalnya, perintah berikut menunjukkan nilai sampel untuk placeholder di perintah sebelumnya.

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

4. (Opsional) Konfigurasi peran logging. Transfer Family mencatat status pesan yang dikirim dan diterima dalam format JSON terstruktur ke CloudWatch log Amazon. Untuk memberi Transfer Family akses ke CloudWatch log di akun Anda, Anda harus mengonfigurasi peran pencatatan di server Anda.

Buat peran AWS Identity and Access Management (IAM) yang dipercayai `transfer.amazonaws.com`, dan lampirkan kebijakan `AWSTransferLoggingAccess` terkelola. Lihat perinciannya di [Buat peran dan kebijakan IAM](#). Perhatikan Nama Sumber Daya Amazon (ARN) dari peran IAM yang baru saja Anda buat, dan kaitkan dengan server dengan menjalankan perintah berikut: `update-server`

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

Note

Meskipun peran logging bersifat opsional, kami sangat menyarankan untuk mengaturnya sehingga Anda dapat melihat status pesan Anda dan memecahkan masalah konfigurasi.

Langkah 5: Buat kesepakatan antara Anda dan pasangan

Prosedur ini menjelaskan cara membuat perjanjian AS2 dengan menggunakan AWS CLI. Jika Anda ingin menggunakan konsol Transfer Family sebagai gantinya, lihat [the section called “Buat perjanjian AS2”](#).

Perjanjian menyatukan dua profil (lokal dan mitra), sertifikat mereka, dan konfigurasi server yang memungkinkan transfer AS2 masuk antara dua pihak. Anda dapat membuat daftar item Anda dengan menjalankan perintah berikut.

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

Langkah ini memerlukan bucket Amazon S3 dan peran IAM dengan read/write akses ke dan dari bucket. Instruksi untuk membuat peran ini sama dengan protokol Transfer Family SFTP, FTP, dan FTPS dan tersedia di [Buat peran dan kebijakan IAM](#).

Untuk membuat perjanjian, Anda memerlukan item berikut:

- Nama bucket Amazon S3 (dan awalan objek, jika ditentukan) untuk menyimpan file AS2 Anda. Kami menyarankan Anda menentukan direktori terpisah untuk jenis file yang berbeda.
- ARN dari peran IAM dengan akses ke bucket
- ID server Transfer Family Anda
- ID profil Anda dan ID profil mitra Anda

Simpan kode berikut ke dalam file, misalnya, `agreementDetails.json`. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

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

Note

Untuk menggunakan direktori dasar tunggal alih-alih direktori terpisah, hapus `CustomDirectories` baris dan baris direktori individualnya dari kode sebelumnya dan gunakan parameter berikut sebagai gantinya:

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

Jangan gunakan direktori dasar dan parameter direktori terpisah, atau perintah akan gagal.

Kemudian, jalankan perintah berikut.

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

Jika berhasil, perintah ini mengembalikan ID untuk perjanjian. Anda kemudian dapat melihat detail perjanjian dengan perintah berikut.

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

Langkah 6: Buat konektor antara Anda dan pasangan

Prosedur ini menjelaskan cara membuat konektor AS2 dengan menggunakan AWS CLI. Jika Anda ingin menggunakan konsol Transfer Family sebagai gantinya, lihat [the section called “Konfigurasi konektor AS2”](#).

Anda dapat menggunakan operasi `StartFileTransfer` API untuk mengirim file yang disimpan di Amazon S3 ke titik akhir AS2 mitra dagang Anda dengan menggunakan konektor. Anda dapat menemukan profil yang Anda buat sebelumnya dengan menjalankan perintah berikut.

```
aws transfer list-profiles
```

Saat Anda membuat konektor, Anda harus memberikan URL server AS2 mitra Anda. Salin teks berikut ke file bernama `testAS2Config.json`.

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

Note

Untuk `EncryptionAlgorithm`, jangan tentukan `DES_EDE3_CBC` algoritme kecuali Anda harus mendukung klien lama yang membutuhkannya, karena ini adalah algoritma enkripsi yang lemah.

Kemudian jalankan perintah berikut untuk membuat konektor.

```
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
```

Langkah 7: Uji pertukaran file melalui AS2 dengan menggunakan Transfer Family

Menerima file dari mitra dagang Anda

Jika Anda mengaitkan alamat IP Elastis publik dengan titik akhir VPC Anda, Transfer Family secara otomatis membuat nama DNS yang berisi alamat IP publik Anda. Subdomain adalah ID AWS Transfer Family server Anda (dari format `s-1234567890abcdef0`). Berikan URL server Anda kepada mitra dagang Anda dalam format berikut.

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

Jika Anda tidak mengaitkan alamat IP Elastis publik dengan titik akhir VPC Anda, cari nama host dari titik akhir VPC yang dapat menerima pesan AS2 melalui HTTP POST dari mitra dagang Anda di port 5080. Untuk mengambil detail titik akhir VPC, gunakan perintah berikut.

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

Misalnya, asumsikan perintah sebelumnya mengembalikan ID titik akhir VPC dari.

`vpce-1234abcd5678efghi` Kemudian, Anda akan menggunakan perintah berikut untuk mengambil nama DNS.

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

Perintah ini mengembalikan semua detail untuk titik akhir VPC yang Anda butuhkan untuk menjalankan perintah berikut.

Nama DNS tercantum dalam `DnsEntries` array. Mitra dagang Anda harus berada dalam VPC Anda untuk mengakses titik akhir VPC Anda (misalnya melalui AWS PrivateLink atau VPN). Berikan URL titik akhir VPC Anda kepada mitra Anda dalam format berikut.

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

Misalnya, URL berikut menunjukkan nilai sampel untuk placeholder di perintah sebelumnya.

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

Dalam contoh ini, transfer yang berhasil disimpan di lokasi yang ditentukan dalam base-directory parameter yang Anda tentukan [Langkah 5: Buat kesepakatan antara Anda dan pasangan](#). Jika kami berhasil menerima file bernama myfile1.txt dan myfile2.txt, file disimpan sebagai *path-defined-in-the-agreement/processed/original_filename.messageId.original_extension*. Di sini, file disimpan sebagai /amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.*messageId*.txt dan /amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.*messageId*.txt.

Jika Anda mengonfigurasi peran logging saat membuat server Transfer Family, Anda juga dapat memeriksa CloudWatch log untuk status pesan AS2.

Kirim file ke mitra dagang Anda

Anda dapat menggunakan Transfer Family untuk mengirim pesan AS2 dengan mereferensikan ID konektor dan jalur ke file, seperti yang diilustrasikan dalam perintah start-file-transfer AWS Command Line Interface (AWS CLI) berikut:

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

Untuk mendapatkan detail konektor Anda, jalankan perintah berikut:

```
aws transfer list-connectors
```

`list-connectors` Perintah mengembalikan ID konektor, URL, dan Nama Sumber Daya Amazon (ARN) untuk konektor Anda.

Untuk mengembalikan properti konektor tertentu, jalankan perintah berikut dengan ID yang ingin Anda gunakan:

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

`describe-connector` Perintah mengembalikan semua properti untuk konektor, termasuk URL, peran, profil, Pemberitahuan Disposisi Pesan (mDNS), tag, dan metrik pemantauan.

Anda dapat mengonfirmasi bahwa mitra berhasil menerima file dengan melihat file JSON dan MDN. File-file ini diberi nama sesuai dengan konvensi yang dijelaskan dalam [Nama dan lokasi file](#). Jika Anda mengonfigurasi peran logging saat membuat konektor, Anda juga dapat memeriksa CloudWatch log Anda untuk status pesan AS2.

Tutorial: Menyiapkan aplikasi web Transfer Family dasar

Tutorial ini membahas cara mengatur aplikasi web Transfer Family. Aplikasi web Transfer Family memungkinkan antarmuka sederhana untuk mentransfer data ke dan dari Amazon S3 melalui browser web. Untuk dokumentasi rinci untuk fitur ini, lihat [Aplikasi web Transfer Family](#).

Tutorial aplikasi web: prasyarat

- Buat instance akun atau instance organisasi dari AWS IAM Identity Center. Lihat perinciannya di [Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family](#).

Jika Anda tidak menggunakan IAM Identity Center sebagai penyedia identitas Anda, [Integrasikan Okta sebagai penyedia identitas Anda untuk aplikasi web](#) ilustrasikan cara menggunakan penyedia identitas alternatif (dalam hal ini Okta).

- Anda memerlukan bucket Amazon S3 untuk digunakan untuk berinteraksi dengan aplikasi web Transfer Family Anda. Untuk detailnya, lihat [Konfigurasi bucket Amazon S3](#)

Note

Tutorial ini mengasumsikan bahwa Anda menggunakan direktori IAM Identity Center untuk penyedia identitas Anda, Jika itu tidak terjadi, lihat [Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family](#) sebelum melanjutkan dengan tutorial ini.

Setelah Anda menyelesaikan tutorial, pengguna Anda dapat masuk dan berinteraksi dengan aplikasi web yang Anda buat.

Langkah 1: Buat sumber daya pendukung yang diperlukan

Anda perlu menambahkan pengguna ke direktori Pusat Identitas IAM Anda. Anda juga memerlukan dua peran: satu untuk digunakan sebagai peran pembawa identitas untuk aplikasi web Anda, dan yang kedua digunakan untuk mengonfigurasi hibah akses Amazon S3. Untuk tutorial, kami mengizinkan AWS layanan untuk membuat peran ini untuk kami.

Untuk menambahkan pengguna

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Dari panel navigasi kiri, pilih Pengguna.
3. Pilih Tambahkan pengguna dan tentukan detail pengguna.

Tentukan nama pengguna, alamat email, dan informasi lain yang diperlukan. Anda dapat memilih untuk mengirim email ke pengguna dengan instruksi untuk mengatur kata sandi mereka, atau Anda dapat membuat kata sandi satu kali untuk dibagikan dengan mereka.

4. Pilih Berikutnya dan secara opsional menetapkan pengguna baru ke satu atau beberapa grup.
5. Pilih Berikutnya dan tinjau pilihan Anda.

Jika semuanya terlihat baik, pilih Tambahkan pengguna untuk membuat pengguna baru dengan detail yang Anda tentukan.

Untuk tutorial, contoh pengguna adalah Bob Stiles, nama pengguna bobstiles dan alamat email bobstiles@example.com.

Langkah 2: Buat aplikasi web Transfer Family

Untuk membuat aplikasi web Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Aplikasi Web.
3. Pilih Buat aplikasi web.

Untuk akses autentikasi, perhatikan bahwa layanan secara otomatis menemukan AWS IAM Identity Center instance yang Anda atur sebagai prasyarat.

4. Di panel Jenis izin, pilih Buat dan gunakan peran layanan baru. Layanan ini menciptakan peran pembawa identitas untuk Anda. Peran pembawa identitas mencakup identitas pengguna yang diautentikasi dalam sesinya.
5. Di panel unit aplikasi Web, terima nilai default 1, atau sesuaikan ke nilai yang lebih tinggi jika diperlukan.
6. Tambahkan tag untuk membantu Anda mengatur aplikasi web Anda. Untuk tutorial, masukkan Nama untuk kunci dan aplikasi web Tutorial untuk nilainya.

 Tip

Anda dapat mengedit nama aplikasi web langsung dari halaman daftar aplikasi Web setelah Anda membuatnya.

7. Pilih Berikutnya untuk membuka halaman aplikasi web Desain. Di layar ini, berikan informasi berikut.

Anda dapat memberikan judul untuk aplikasi web Anda secara opsional. Anda juga dapat mengunggah file gambar untuk logo dan favicon Anda.

- Untuk judul halaman, sesuaikan judul untuk tab browser yang dilihat pengguna Anda saat mereka terhubung ke aplikasi web. Jika Anda tidak memasukkan apa pun untuk judul halaman, defaultnya adalah Transfer Web App.
- Untuk logo, unggah file gambar. Ukuran file maksimum untuk gambar logo Anda adalah 50 KB.
- Untuk favicon, unggah file gambar. Ukuran file maksimum untuk favicon Anda adalah 20 KB.

8. Pilih Berikutnya, lalu pilih Buat aplikasi web.

Untuk memberikan pengalaman bermerek, Anda dapat memberikan URL khusus bagi pengguna untuk mengakses aplikasi web Transfer Family Anda. Lihat perinciannya di [Perbarui titik akhir akses Anda dengan URL khusus](#).

Langkah 3: Konfigurasi berbagi Cross-origin sumber daya (CORS) untuk bucket Anda

Anda harus menyiapkan berbagi sumber daya lintas asal (CORS) untuk semua bucket yang digunakan oleh aplikasi web Anda. Konfigurasi CORS adalah dokumen yang mendefinisikan aturan

yang mengidentifikasi asal yang Anda izinkan untuk mengakses bucket Anda. Untuk informasi selengkapnya tentang CORS, lihat [Mengonfigurasi berbagi sumber daya lintas asal \(CORS\)](#).

Untuk menyiapkan berbagi Cross-origin sumber daya (CORS) untuk bucket Amazon S3 Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Pilih Bucket dari panel navigasi kiri dan cari bucket Anda di dialog pencarian, lalu pilih tab Izin.
3. Dalam berbagi Cross-origin sumber daya (CORS), pilih Edit dan tempel dalam kode berikut. Ganti *AccessEndpoint* dengan titik akhir akses aktual untuk aplikasi web Anda. Pastikan untuk tidak memasukkan garis miring, karena hal itu menyebabkan kesalahan saat pengguna mencoba masuk ke aplikasi web Anda.
 - Contoh yang salah: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Contoh yang benar: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Jika Anda menggunakan kembali bucket untuk beberapa aplikasi web, tambahkan titik akhir akses aplikasi web mereka ke daftar `AllowedOrigins`

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://AccessEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
```

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

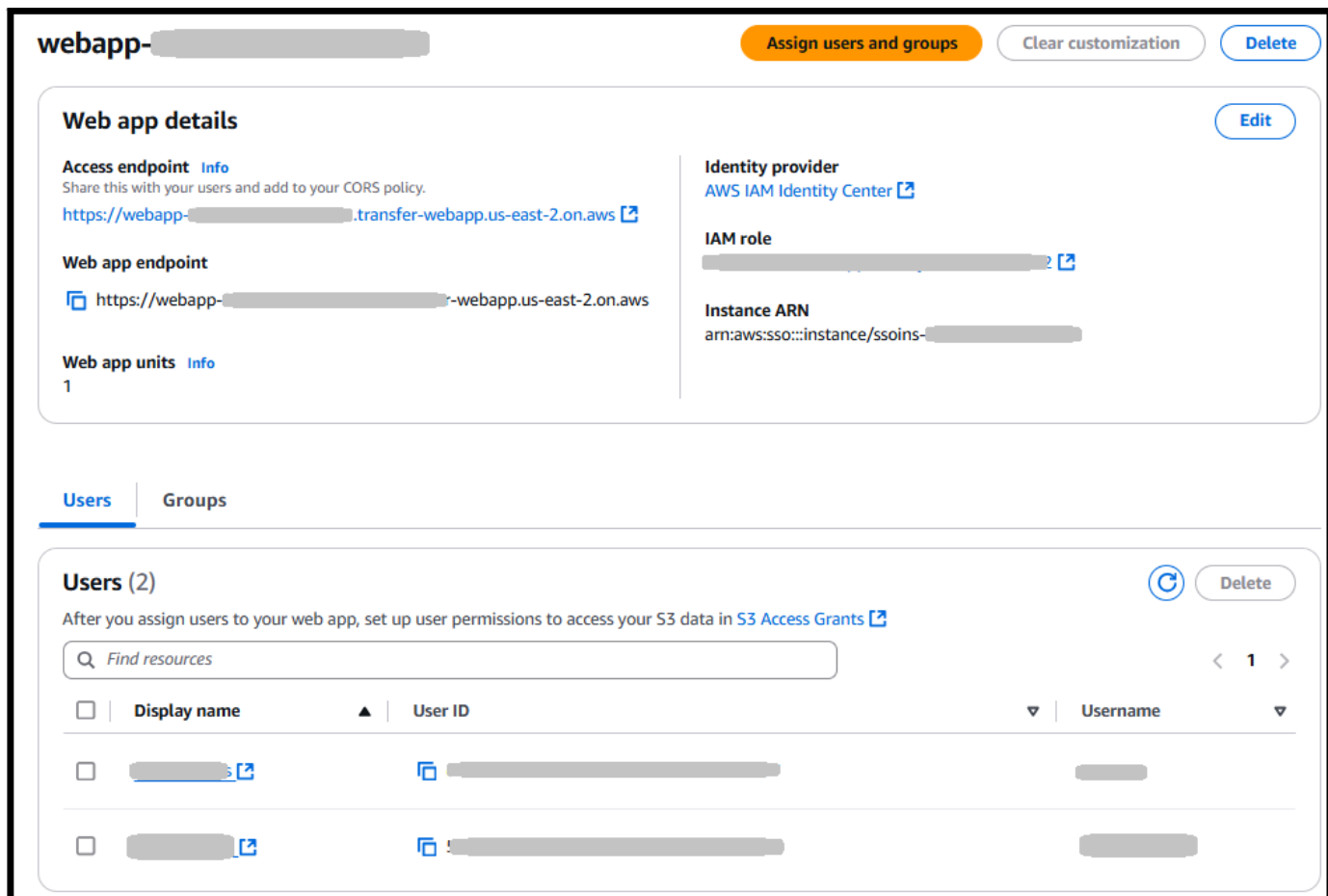
4. Pilih Simpan perubahan untuk memperbarui CORS.

Langkah 4: Tambahkan pengguna ke aplikasi web Transfer Family

Tambahkan pengguna yang sebelumnya Anda buat di IAM Identity Center.

Untuk menetapkan pengguna ke aplikasi web Transfer Family

1. Arahkan ke aplikasi web yang Anda buat sebelumnya.
2. Pilih Tetapkan pengguna dan grup.



3. Untuk menetapkan pengguna yang sebelumnya Anda buat di Pusat Identitas IAM, pilih Tetapkan pengguna dan grup yang ada dan pilih Berikutnya.
 - a. Cari pengguna dengan nama tampilan. Perhatikan bahwa tidak ada pengguna yang muncul sampai Anda mulai memasukkan kriteria pencarian Anda. Untuk menambahkan **Bob Stiles**, masukkan bob di kotak pencarian. Jika Anda tidak dapat menemukan pengguna Anda, navigasikan ke konsol manajemen Pusat Identitas IAM, temukan pengguna, lalu salin dan tempel nama tampilannya di sini.
 - b. Pilih **Bob Stiles** pengguna, lalu pilih Tetapkan.

Langkah 5: Daftarkan lokasi di Amazon S3 dan buat hibah akses

Setelah menetapkan pengguna ke aplikasi web, Anda perlu mendaftarkan bucket dan membuat hibah akses untuk pengguna tersebut.

 Note

Anda harus memiliki instance S3 Access Grants sebelum Anda dapat melanjutkan. Untuk detailnya, lihat [Membuat instance S3 Access Grants](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk mendaftarkan lokasi dan membuat hibah akses

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon S3 di. <https://console.aws.amazon.com/s3/>
2. Pilih Access Grants dari panel navigasi kiri.
3. Pilih Lihat detail untuk melihat detail instans S3 Access Grants Anda.
4. Pilih tab Lokasi, lalu pilih Daftar lokasi.
5. Berikan informasi berikut.
 - Untuk Lingkup, telusuri bucket atau masukkan nama bucket Anda, dan secara opsional awalan. Perhatikan bahwa ruang lingkup dimulai dengan string **s3://**.
 - Untuk peran IAM, pilih Buat peran baru agar Amazon S3 membuat peran. Peran ini memungkinkan S3 Access Grants untuk mengakses cakupan lokasi yang Anda tentukan.

Pilih Daftar lokasi untuk melanjutkan.

6. Pilih tab Hibah, lalu pilih Buat Hibah dan berikan detail berikut.

- Untuk Lokasi, pilih Jelajahi lokasi dan pilih lokasi yang Anda daftarkan di langkah sebelumnya.
- Untuk Subprefix, masukkan * untuk menunjukkan bahwa hibah akses berlaku untuk seluruh bucket.
- Untuk Izin, pilih Baca dan Tulis.
- Untuk jenis Penerima Hibah, pilih Identitas direktori dari IAM Identity Center.
- Untuk jenis identitas Direktori, pilih Pengguna.
- Di pengguna/ID Pusat Identitas IAM, salin dan tempel ID pengguna untuk. **Bob Stiles** ID ini tersedia di panel Pengguna di aplikasi web Transfer Family Anda.

7. Pilih Buat Hibah.

Hibah akses dibuat.

Langkah 6: Akses aplikasi web Transfer Family Anda sebagai pengguna

Sekarang, kami menavigasi ke URL aplikasi web dan masuk sebagai pengguna yang kami tetapkan sebelumnya.

Untuk masuk ke aplikasi web Transfer Family

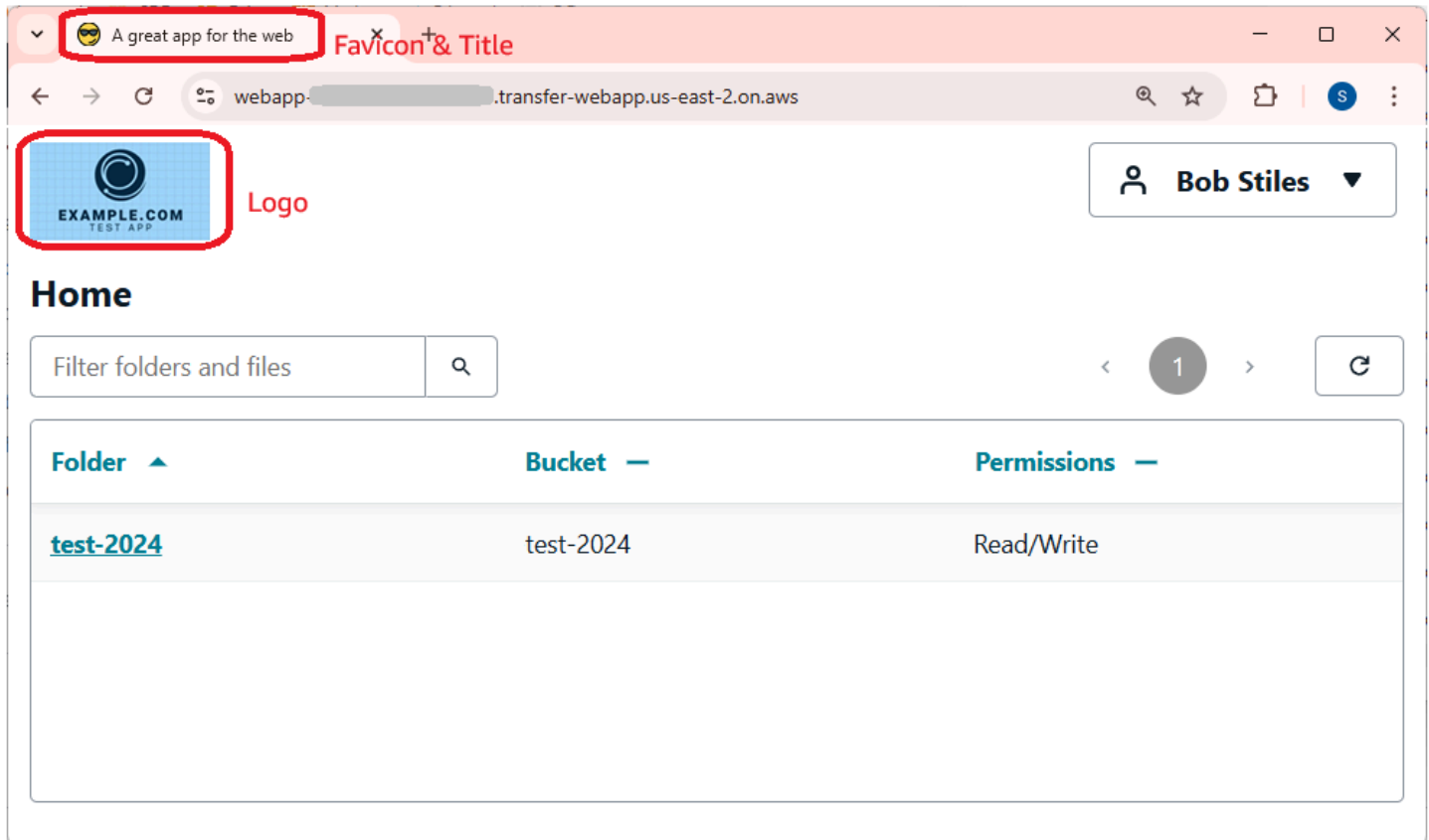
1. Arahkan ke aplikasi web Anda
2. Pilih titik akhir Access dari panel detail aplikasi Web.

The screenshot shows the AWS IAM console interface for a web application. At the top, there's a header with the application name 'webapp-' followed by a redacted ID. To the right are buttons: 'Assign users and groups' (orange), 'Clear customization' (blue), and 'Delete' (blue). Below this is a 'Web app details' section with an 'Edit' button. The 'Access endpoint' is highlighted with a red box and contains the URL 'https://webapp-[redacted].transfer-webapp.us-east-2.on.aws'. Other details include 'Web app endpoint', 'Web app units' (1), 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN'. Below the details is a tabbed interface with 'Users' and 'Groups'. The 'Users' tab is active, showing a list of users. One user, 'Bob Stiles', is highlighted with a red box. The user's details include a checkbox, a link to 'Bob Stiles', a redacted User ID, and the username 'bobstiles'.

3. Pada layar masuk, masukkan pengguna yang Anda buat **bobstiles**, lalu pilih Berikutnya.
4. Masukkan kata sandi yang ditetapkan sistem untuk pengguna ini saat dibuat dan pilih Berikutnya.
5. Jika organisasi Anda memerlukan otentikasi multi-faktor (MFA), Anda perlu mengaturnya sekarang. Jika tidak, lompat ke langkah 6.
 - a. Anda disajikan dengan layar untuk mendaftarkan perangkat MFA Anda. Pilih salah satu opsi yang tersedia dan pilih Berikutnya.

- b. Lakukan langkah-langkah yang diperlukan untuk mengonfigurasi MFA untuk pengguna ini: langkah-langkahnya tergantung pada opsi MFA yang Anda pilih.
- c. Anda mungkin harus menetapkan kata sandi baru untuk pengguna Anda: jika diperlukan, lakukan sekarang. Sistem mungkin juga mengharuskan Anda masuk lagi, menggunakan kredensial MFA baru yang Anda konfigurasi.

Penggunaan Anda akan melihat layar yang mirip dengan yang berikut ini. Perhatikan bahwa tampilan layar ini mencakup penyesuaian untuk favicon dan logo.



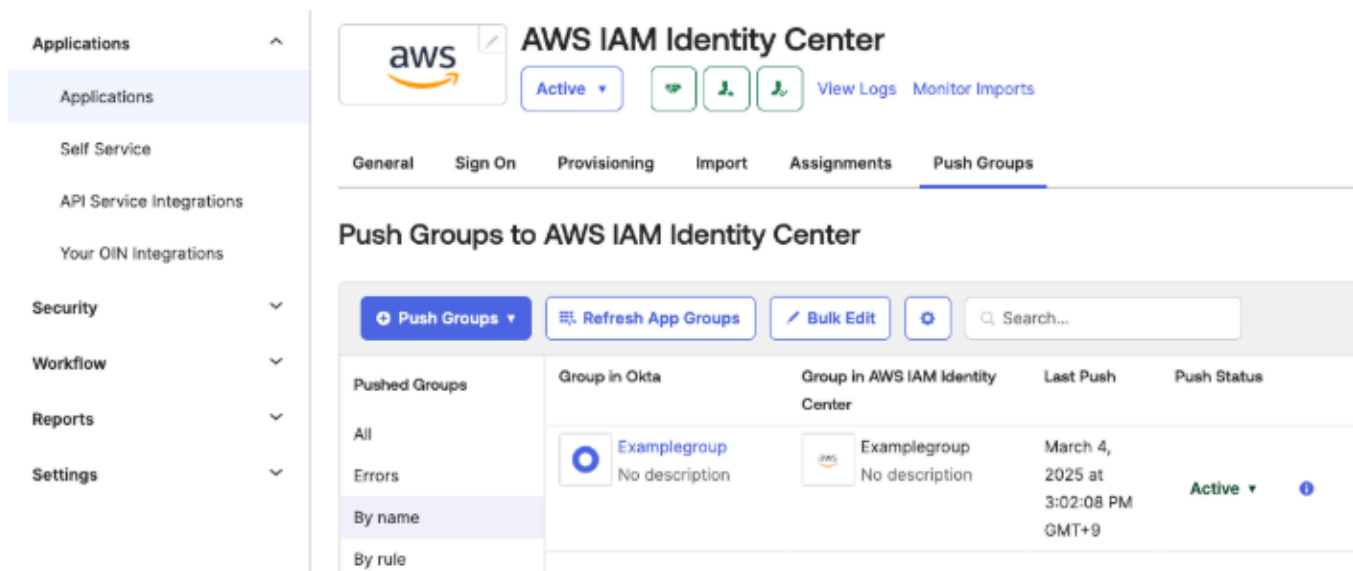
Langkah selanjutnya

Anda telah berhasil menyiapkan aplikasi web Transfer Family dasar dengan akses bucket S3 standar. Jika Anda memerlukan kontrol lebih terperinci atas izin bucket, seperti mengizinkan pengguna mengunduh dari satu bucket dan mengunggah ke bucket lainnya, lihat. [Tutorial: Menyiapkan aplikasi AWS Transfer Family web dengan akses multi-bucket selektif](#)

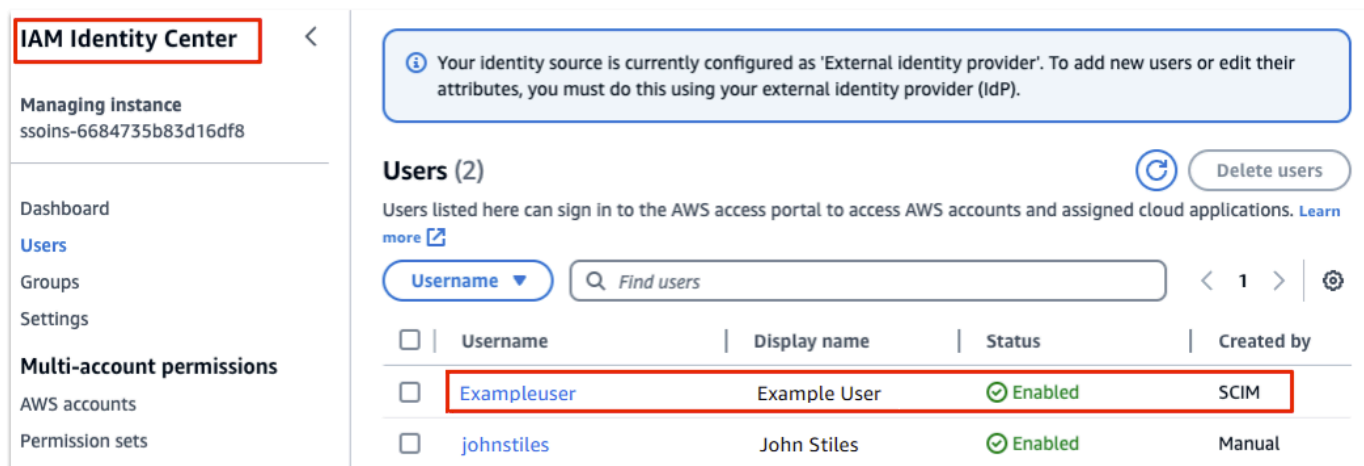
Integrasikan Okta sebagai penyedia identitas Anda untuk aplikasi web

Anda dapat mengintegrasikan penyedia identitas eksternal dengan aplikasi web Transfer Family. Bagian ini menjelaskan cara mengatur Okta sebagai penyedia identitas Anda.

1. Di Okta, buat pengguna, grup, dan aplikasi. Untuk detail tentang cara melakukannya, lihat [Mengonfigurasi SAFL dan SCIM dengan Okta dan Pusat Identitas IAM](#).



2. Connect Okta dan impor pengguna dan grup dari Okta ke. AWS IAM Identity Center Ikuti langkah 1—4 di [Konfigurasi SAFL dan SCIM dengan Okta dan IAM](#) Identity Center.



IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

[Dashboard](#)
[Users](#)
[Groups](#)
[Settings](#)

Multi-account permissions
[AWS accounts](#)
[Permission sets](#)

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

Groups (2)

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

< 1 > ⚙

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

3. Konfirmasikan bahwa sumber identitas di IAM Identity Center adalah SAFL 2.0.

Settings

Details

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

Instance name - [Edit](#)
[redacted]

Instance ID
ssoins-[redacted]

Organization ID
AWS Organizations not enabled

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

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

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

[Identity source](#) | [Authentication](#) | [Management](#) | [Tags](#)

Identity source

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

Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
SCIM

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

Identity store ID
[d-\[redacted\]](#)

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

Actions ▼

4. Tetapkan pengguna dan grup Anda, seperti yang dijelaskan dalam [Langkah 4: Tambahkan pengguna ke aplikasi web Transfer Family](#).
5. Untuk menghindari pengguna Anda perlu menggunakan MFA saat masuk ke aplikasi web Anda, lakukan langkah-langkah berikut di Okta.
 - a. Dari konsol admin Okta, akses [Aplikasi] - [Aplikasi], dan pilih AWS IAM Identity Center aplikasi.
 - b. Pada tab Masuk, pilih [Otentikasi pengguna] - Edit.
 - c. Pilih Kata Sandi saja.

Setelah Anda melakukan semua langkah lain untuk tutorial, pengguna Anda harus dapat mengakses aplikasi web Transfer Family Anda dengan menavigasi ke titik akhir akses aplikasi web di browser web.

Tutorial: Menyiapkan aplikasi AWS Transfer Family web dengan akses multi-bucket selektif

Tutorial ini memandu Anda dalam mengonfigurasi aplikasi web Transfer Family dengan izin bucket Amazon S3 khusus untuk satu pengguna. Anda akan belajar cara menyiapkan solusi yang memungkinkan pengguna mengunduh dari satu bucket dan mengunggah ke bucket lainnya sambil menjaga keamanan. Ini adalah tutorial lanjutan yang dibangun di atas konsep yang tercakup dalam tutorial dasar. Jika Anda baru mengenal aplikasi AWS Transfer Family web, pertimbangkan untuk memulai dengan [Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#).

Prasyarat

Sebelum Anda memulai tutorial ini, Anda perlu:

- Pusat Identitas IAM dikonfigurasi di wilayah yang sama dengan aplikasi AWS Transfer Family web Anda. Perhatikan bahwa hanya AWS mengizinkan satu instance Pusat Identitas IAM per AWS akun untuk semua Wilayah.
- Setidaknya satu pengguna dikonfigurasi di IAM Identity Center.
- Dua ember S3: satu untuk unduhan dan satu untuk unggahan.

Note

Tutorial ini berbagi banyak prasyarat dengan tutorial aplikasi web dasar. Untuk informasi selengkapnya tentang menyiapkan Pusat Identitas IAM dan membuat pengguna, lihat [Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#).

Langkah 1: Buat aplikasi web Transfer Family

Untuk membuat aplikasi web Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Aplikasi Web.
3. Pilih Buat aplikasi web.

Untuk akses otentikasi, perhatikan bahwa layanan secara otomatis menemukan AWS IAM Identity Center instance yang Anda atur sebagai prasyarat.

4. Di panel Jenis izin, pilih Buat dan gunakan peran layanan baru. Layanan ini menciptakan peran pembawa identitas untuk Anda. Peran pembawa identitas mencakup identitas pengguna yang diautentikasi dalam sesinya.
5. Di panel unit aplikasi Web, terima nilai default 1, atau sesuaikan ke nilai yang lebih tinggi jika diperlukan.
6. Tambahkan tag untuk membantu Anda mengatur aplikasi web Anda. Untuk tutorial, masukkan Nama untuk kunci dan aplikasi web Tutorial untuk nilainya.

Tip

Anda dapat mengedit nama aplikasi web langsung dari halaman daftar aplikasi Web setelah Anda membuatnya.

7. Pilih Berikutnya untuk membuka halaman aplikasi web Desain. Di layar ini, berikan informasi berikut.

Anda dapat memberikan judul untuk aplikasi web Anda secara opsional. Anda juga dapat mengunggah file gambar untuk logo dan favicon Anda.

- Untuk judul halaman, sesuaikan judul untuk tab browser yang dilihat pengguna Anda saat mereka terhubung ke aplikasi web. Jika Anda tidak memasukkan apa pun untuk judul halaman, defaultnya adalah Transfer Web App.
- Untuk logo, unggah file gambar. Ukuran file maksimum untuk gambar logo Anda adalah 50 KB.
- Untuk favicon, unggah file gambar. Ukuran file maksimum untuk favicon Anda adalah 20 KB.

8. Pilih Berikutnya, lalu pilih Buat aplikasi web.

Langkah 2: Konfigurasi peran IAM untuk akses S3

Anda perlu membuat dua peran IAM: satu dengan akses khusus unduhan ke bucket pertama dan satu lagi dengan akses khusus unggah ke bucket kedua.

Kebijakan kepercayaan untuk kedua peran

Gunakan kebijakan kepercayaan berikut untuk kedua peran IAM:

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

Kebijakan IAM untuk bucket unduhan

Buat peran IAM dengan kebijakan berikut untuk akses hanya-baca ke bucket unduhan Anda:

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

Important

Ganti amzn-s3-demo-bucket1 dengan nama sebenarnya dari bucket unduhan Anda.

Kebijakan IAM untuk upload bucket

Buat peran IAM lain dengan kebijakan berikut untuk akses tulis ke bucket upload Anda:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelWritePermissions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",

```

```
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket2/*",
        "arn:aws:s3:::amzn-s3-demo-bucket2"
    ]
}
]
```

Important

Ganti amzn-s3-demo-bucket2 dengan nama sebenarnya dari bucket upload Anda.

Langkah 3: Siapkan Hibah Akses S3

1. Buka konsol S3 di <https://console.aws.amazon.com/s3/>.
2. Di panel navigasi, pilih Access Grants.
3. Klik Buat contoh Hibah Akses S3.
4. Pilih opsi Add IAM Identity Center instance dan masukkan instance pusat identitas ARN.
5. Klik Berikutnya, lalu klik Batal untuk menyelesaikan pembuatan instance S3 Access Grants tanpa melanjutkan dengan langkah tambahan.

Langkah ini membuat instance S3 Access Grants. Anda sekarang akan mendaftarkan lokasi dan membuat hibah akses.

Langkah 4: Daftarkan lokasi bucket S3

Daftarkan kedua bucket S3 sebagai lokasi dengan Hibah Akses S3:

1. Di konsol S3 Access Grants, navigasikan ke Lokasi dan klik Daftar lokasi.
2. Di bawah Cakupan lokasi, pilih bucket S3 spesifik untuk unduhan (amzn-s3-demo-bucket1).

3. Saat diminta untuk memilih peran IAM, pilih peran IAM unduhan yang Anda buat sebelumnya.
4. Selesaikan proses pendaftaran.
5. Ulangi proses untuk mendaftarkan bucket upload (amzn-s3-demo-bucket2), pilih peran IAM upload saat diminta.

Langkah 5: Buat Hibah Akses

Buat dua hibah, satu untuk setiap lokasi terdaftar:

1. Di konsol S3 Access Grants, navigasikan ke Grants dan klik Create grant.
2. Di Lokasi, klik Jelajahi lokasi dan pilih lokasi bucket unduhan (amzn-s3-demo-bucket1).
3. Di Subprefix (opsional), enter * untuk mengizinkan akses ke seluruh bucket, atau tentukan jalur seperti membatasi akses folder1/folder2/* ke awalan tertentu.

Menggunakan * akan mengatur cakupan hibah kes3://bucket-name/*, memungkinkan akses ke seluruh bucket. Untuk mengizinkan akses ke hanya awalan tertentu, masukkan jalur seperti folder1/folder2/*, yang akan mengatur cakupan hibah kes3://bucket-name/folder1/folder2/*.

4. Di bawah Izin dan akses, pilih Baca untuk keranjang unduhan.
5. Dalam tipe Penerima hibah, pilih Identitas direktori dari Pusat Identitas IAM.
6. Untuk tipe utama IAM, pilih User dan masukkan User ID pengguna IAM Identity Center Anda.
7. Selesaikan proses pembuatan hibah.
8. Ulangi proses untuk membuat hibah untuk bucket upload (amzn-s3-demo-bucket2), tetapi pilih izin. Read-write

Langkah 6: Konfigurasikan kebijakan CORS untuk bucket S3

Konfigurasikan kebijakan CORS untuk kedua bucket S3 agar memungkinkan akses melalui: AWS Transfer Family WebApp

1. Buka konsol S3 dan arahkan ke bucket unduhan Anda (amzn-s3-demo-bucket1).
2. Pilih tab Izin.
3. Gulir ke bawah ke bagian berbagi Cross-origin sumber daya (CORS) dan klik Edit.
4. Tambahkan konfigurasi CORS berikut, ganti *WebAppEndpoint* dengan URL WebApp titik akhir Anda yang sebenarnya:

Anda dapat menemukan URL endpoint aplikasi web Anda di AWS Transfer Family konsol di bawah WebApps. Ini akan terlihat mirip dengan `https://webapp-*****.transfer-webapp.us-west-2.on.aws`.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

5. Klik Simpan perubahan.
6. Ulangi proses untuk bucket upload Anda (amzn-s3-demo-bucket2).

Langkah 7: Uji konfigurasi

1. Buka URL aplikasi AWS Transfer Family web Anda. Anda dapat menemukan URL ini di AWS Transfer Family konsol WebApps di bawah bidang titik akhir Access.
2. Masuk menggunakan kredensial pengguna IAM Identity Center yang Anda konfigurasi dengan hibah akses.
3. Setelah masuk, Anda akan melihat kedua lokasi S3 di beranda.
4. Arahkan ke keranjang unduhan (amzn-s3-demo-bucket1) dan verifikasi bahwa Anda dapat mengunduh file tetapi tidak mengunggah.
5. Arahkan ke bucket upload (amzn-s3-demo-bucket2) dan verifikasi bahwa Anda dapat mengunggah file.

Kesimpulan

Anda telah berhasil mengonfigurasi AWS Transfer Family WebApp dengan akses bucket S3 selektif untuk satu pengguna. Pengaturan ini memungkinkan pengguna untuk mengunduh dari satu bucket dan mengunggah ke bucket lainnya sambil menjaga keamanan melalui peran IAM dan S3 Access Grants.

Pendekatan ini dapat diperluas ke beberapa pengguna dengan membuat hibah tambahan di S3 Access Grants untuk setiap pengguna, memungkinkan kontrol granular atas izin akses bucket. Untuk informasi tentang penyiapan aplikasi web dasar, lihat [Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#).

Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP

Topik ini memberikan detail untuk membuat dan menggunakan titik akhir AWS Transfer Family server yang menggunakan satu atau lebih protokol SFTP, FTPS, dan FTP.

Topik

- [Opsi penyedia identitas](#)
- [AWS Transfer Family matriks tipe titik akhir](#)
- [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#)
- [Pertimbangan Load Balancer Jaringan FTP dan FTPS](#)
- [Mentransfer file melalui titik akhir server menggunakan klien](#)
- [Mengelola pengguna untuk titik akhir server](#)
- [Menggunakan direktori logis untuk menyederhanakan struktur direktori Transfer Family Anda](#)
- [Akses fsX Anda untuk sistem file NetApp ONTAP dengan Transfer Family](#)

Opsi penyedia identitas

AWS Transfer Family menyediakan beberapa metode untuk mengautentikasi dan mengelola pengguna. Tabel berikut membandingkan penyedia identitas yang tersedia yang dapat Anda gunakan dengan Transfer Family.

Tindakan	AWS Transfer Family layanan dikelola	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Protokol yang didukung	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based otentikasi	Ya	Tidak	Ya	Ya
Autentikasi kata sandi	Tidak	Ya	Ya	Ya

Tindakan	AWS Transfer Family layanan dikelola	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
AWS Identity and Access Management (IAM) dan POSIX	Ya	Ya	Ya	Ya
Direktori home logis	Ya	Ya	Ya	Ya
Akses parameter (berbasis nama pengguna)	Ya	Ya	Ya	Ya
Struktur akses ad hoc	Ya	Tidak	Ya	Ya
AWS WAF	Tidak	Tidak	Ya	Tidak

Catatan:

- IAM digunakan untuk mengontrol akses untuk penyimpanan dukungan Amazon S3, dan POSIX digunakan untuk Amazon EFS.
- Ad hoc mengacu pada kemampuan untuk mengirim profil pengguna saat runtime. Misalnya, Anda dapat mendaratkan pengguna di direktori home mereka dengan meneruskan nama pengguna sebagai variabel.
- Untuk detailnya AWS WAF, lihat [Tambahkan firewall aplikasi web](#).
- Ada posting blog yang menjelaskan penggunaan fungsi Lambda yang terintegrasi dengan Microsoft Entra ID (sebelumnya Azure AD) sebagai penyedia identitas Transfer Family Anda. Untuk detailnya, lihat [Mengautentikasi AWS Transfer Family dengan Azure Active Directory](#) dan AWS Lambda
- Kami menyediakan beberapa CloudFormation template untuk membantu Anda dengan cepat menyebarkan server Transfer Family yang menggunakan penyedia identitas khusus. Lihat perinciannya di [Template fungsi Lambda](#).

Dalam prosedur berikut, Anda dapat membuat SFTP-enabled server, FTPS-enabled server, FTP-enabled server, atau AS2-enabled server.

Langkah selanjutnya

- [Buat SFTP-enabled server](#)
- [Buat FTPS-enabled server](#)
- [Buat FTP-enabled server](#)
- [Mengkonfigurasi AS2](#)

AWS Transfer Family matriks tipe titik akhir

Saat membuat server Transfer Family, Anda memilih jenis endpoint yang akan digunakan. Tabel berikut menjelaskan karakteristik untuk setiap jenis titik akhir.

Matriks tipe titik akhir

Karakteristik	Publik	VPC - Internet	VPC - Internal	VPC_Endpoint (tidak digunakan lagi)
Protokol yang didukung	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
Akses	Dari internet. Jenis titik akhir ini tidak memerlukan konfigurasi khusus apa pun di VPC Anda.	Melalui internet dan dari dalam VPC dan VPC-connected lingkungan, seperti pusat data lokal di atas Direct Connect atau VPN.	Dari dalam VPC dan VPC-connected lingkungan, seperti pusat data lokal di atas Direct Connect atau VPN.	Dari dalam VPC dan VPC-connected lingkungan, seperti pusat data lokal di atas Direct Connect atau VPN.
Alamat IP statis	Anda tidak dapat melampirkan alamat IP statis. AWS menyediakan	Anda dapat melampirkan alamat IP Elastis ke titik akhir.	Alamat IP pribadi yang dilampirkan ke titik akhir tidak berubah.	Alamat IP pribadi yang dilampirkan ke titik akhir tidak berubah.

Karakteristik	Publik	VPC - Internet	VPC - Internal	VPC_Endpoint (tidak digunakan lagi)
	an alamat IP yang dapat berubah.	Ini bisa berupa alamat AWS IP milik atau alamat IP Anda sendiri (Bawa alamat IP Anda sendiri). Alamat IP elastis yang dilampirkan ke titik akhir tidak berubah. Alamat IP pribadi yang dilampirkan ke server juga tidak berubah.		

Karakteristik	Publik	VPC - Internet	VPC - Internal	VPC_Endpoint (tidak digunakan lagi)
Daftar izin IP sumber	Jenis titik akhir ini tidak mendukung daftar izin berdasarkan alamat IP sumber. Titik akhir dapat diakses publik dan mendengarkan lalu lintas melalui port 22.  Note Untuk VPC-hosted endpoint, server SFTP Transfer Family dapat beroperasi melalui port 22 (default), 2222, 2223,	Untuk mengizinkan akses berdasarkan alamat IP sumber, Anda dapat menggunakan grup keamanan yang dilampirkan ke titik akhir server dan ACL jaringan yang dilampirkan ke subnet tempat titik akhir berada.	Untuk mengizinkan akses berdasarkan alamat IP sumber, Anda dapat menggunakan grup keamanan yang dilampirkan ke titik akhir server dan daftar kontrol akses jaringan (ACL jaringan) yang dilampirkan ke subnet tempat titik akhir berada.	Untuk mengizinkan akses berdasarkan alamat IP sumber, Anda dapat menggunakan grup keamanan yang dilampirkan ke titik akhir server dan ACL jaringan yang dilampirkan ke subnet tempat titik akhir berada.

Karakteristik	Publik	VPC - Internet	VPC - Internal	VPC_Endpoint (tidak digunakan lagi)
	atau 22000.			
Daftar izin firewall klien	Anda harus mengizinkan nama DNS server. Karena alamat IP dapat berubah, hindari menggunakan alamat IP untuk daftar izin firewall klien Anda.	Anda dapat mengizinkan nama DNS server atau alamat IP Elastis yang dilampirkan ke server.	Anda dapat mengizinkan alamat IP pribadi atau nama DNS dari titik akhir.	Anda dapat mengizinkan alamat IP pribadi atau nama DNS dari titik akhir.
Jenis alamat IP	IPv4 (default) atau dual-stack (IPv4 dan IPv6)	Hanya IPv4 (tumpukan ganda tidak didukung)	IPv4 (default) atau dual-stack (IPv4 dan IPv6)	Hanya IPv4 (tumpukan ganda tidak didukung)

Note

Jenis VPC_ENDPOINT endpoint sekarang sudah usang dan tidak dapat digunakan untuk membuat server baru. Alih-alih menggunakan `EndpointType=VPC_ENDPOINT`, gunakan tipe titik akhir VPC (`EndpointType=VPC`), yang dapat Anda gunakan sebagai Internal atau Internet Facing, seperti yang dijelaskan dalam tabel sebelumnya.

- Untuk detail tentang penghentian, lihat. [Menghentikan penggunaan VPC_ENDPOINT](#)
- Untuk informasi tentang mengelola izin titik akhir VPC, lihat. [Membatasi akses endpoint VPC untuk server Transfer Family](#)

Pertimbangkan opsi berikut untuk meningkatkan postur keamanan AWS Transfer Family server Anda:

- Gunakan titik akhir VPC dengan akses internal, sehingga server hanya dapat diakses oleh klien dalam VPC atau VPC-connected lingkungan Anda seperti pusat data lokal di atas atau VPN. Direct Connect
- Untuk memungkinkan klien mengakses titik akhir melalui internet dan melindungi server Anda, gunakan titik akhir VPC dengan akses yang menghadap ke internet. Kemudian, ubah grup keamanan VPC untuk mengizinkan lalu lintas hanya dari alamat IP tertentu yang meng-host klien pengguna Anda.
- Jika Anda memerlukan otentikasi berbasis kata sandi dan Anda menggunakan penyedia identitas khusus dengan server Anda, itu adalah praktik terbaik bahwa kebijakan kata sandi Anda mencegah pengguna membuat kata sandi yang lemah dan membatasi jumlah upaya login yang gagal.
- AWS Transfer Family adalah layanan terkelola, sehingga tidak menyediakan akses shell. Anda tidak dapat langsung mengakses server SFTP yang mendasarinya untuk menjalankan perintah asli OS di server Transfer Family.
- Gunakan Network Load Balancer di depan titik akhir VPC dengan akses internal. Ubah port listener pada penyeimbang beban dari port 22 ke port yang berbeda. Ini dapat mengurangi, tetapi tidak menghilangkan, risiko pemindai port dan bot yang menyelidiki server Anda, karena port 22 paling sering digunakan untuk pemindaian. Untuk detailnya, lihat posting blog [Network Load Balancers sekarang mendukung grup Keamanan](#).

 Note

Jika Anda menggunakan Network Load Balancer, AWS Transfer Family CloudWatch log menampilkan alamat IP untuk NLB, bukan alamat IP klien yang sebenarnya.

Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP

Anda dapat membuat server transfer file dengan menggunakan AWS Transfer Family layanan ini. Protokol transfer file berikut tersedia:

- Secure Shell (SSH) File Transfer Protocol (SFTP) — Transfer file melalui SSH. Lihat perinciannya di [the section called “Buat SFTP-enabled server”](#).

 Note

Kami memberikan AWS CDK contoh untuk membuat server SFTP Transfer Family. Contoh menggunakan TypeScript, dan tersedia di GitHub [sini](#).

- File Transfer Protocol Secure (FTPS) — Transfer file dengan enkripsi TLS. Lihat perinciannya di [the section called “Buat FTPS-enabled server”](#).
- Protokol Transfer File (FTP) — Transfer file tidak terenkripsi. Lihat perinciannya di [the section called “Buat FTP-enabled server”](#).
- Pernyataan Penerapan 2 (AS2) — Transfer file untuk mengangkut data bisnis-ke-bisnis terstruktur. Lihat perinciannya di [the section called “Konfigurasi AS2”](#). Untuk AS2, Anda dapat dengan cepat membuat CloudFormation tumpukan untuk tujuan demonstrasi. Prosedur ini dijelaskan dalam [Gunakan template untuk membuat demo Transfer Family AS2 stack](#).

Anda dapat membuat server dengan beberapa protokol.

 Note

Jika Anda memiliki beberapa protokol yang diaktifkan untuk titik akhir server yang sama dan Anda ingin memberikan akses dengan menggunakan nama pengguna yang sama melalui beberapa protokol, Anda dapat melakukannya selama kredensial khusus untuk protokol telah diatur di penyedia identitas Anda. Untuk FTP, kami sarankan untuk mempertahankan kredensial terpisah dari SFTP dan FTPS. Ini karena, tidak seperti SFTP dan FTPS, FTP mentransmisikan kredensial dalam teks yang jelas. Dengan mengisolasi kredensial FTP dari SFTP atau FTPS, jika kredensial FTP dibagikan atau diekspos, beban kerja Anda menggunakan SFTP atau FTPS tetap aman.

Saat Anda membuat server, Anda memilih spesifik Wilayah AWS untuk melakukan permintaan operasi file pengguna yang ditugaskan ke server tersebut. Seiring dengan menetapkan server satu atau beberapa protokol, Anda juga menetapkan salah satu jenis penyedia identitas berikut:

- Layanan dikelola dengan menggunakan kunci SSH. Lihat perinciannya di [Bekerja dengan pengguna yang dikelola layanan](#).
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Metode ini memungkinkan Anda mengintegrasikan grup Microsoft Active Directory untuk menyediakan akses

ke server Transfer Family Anda. Lihat perinciannya di [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

- Penyedia identitas khusus. Transfer Family menawarkan beberapa opsi untuk menggunakan penyedia identitas khusus, seperti yang dijelaskan dalam [Bekerja dengan penyedia identitas khusus](#) topik.

Anda juga menetapkan server jenis titik akhir (dapat diakses publik atau dihosting VPC) dan nama host dengan menggunakan titik akhir server default, atau nama host khusus dengan menggunakan layanan Amazon Route 53 atau dengan menggunakan layanan Sistem Nama Domain (DNS) pilihan Anda. Nama host server harus unik di Wilayah AWS tempat pembuatannya.

Selain itu, Anda dapat menetapkan peran CloudWatch pencatatan Amazon untuk mendorong peristiwa ke CloudWatch log Anda, memilih kebijakan keamanan yang berisi algoritme kriptografi yang diaktifkan untuk digunakan oleh server Anda, dan menambahkan metadata ke server dalam bentuk tag yang merupakan pasangan nilai kunci.

Important

Anda dikenakan biaya untuk server instantiated dan untuk transfer data. Untuk informasi tentang harga dan penggunaan AWS Kalkulator Harga untuk mendapatkan perkiraan biaya penggunaan Transfer Family, lihat [AWS Transfer Family harga](#).

Buat SFTP-enabled server

Secure Shell (SSH) File Transfer Protocol (SFTP) adalah protokol jaringan yang digunakan untuk transfer data yang aman melalui internet. Protokol ini mendukung fungsionalitas keamanan dan otentikasi penuh SSH. Ini banyak digunakan untuk bertukar data, termasuk informasi sensitif antara mitra bisnis di berbagai industri seperti layanan keuangan, perawatan kesehatan, ritel, dan periklanan.

Perhatikan hal berikut

- Server SFTP untuk Transfer Family beroperasi melalui port 22. Untuk VPC-hosted endpoint, server SFTP Transfer Family juga dapat beroperasi melalui port 2222, 2223 atau 22000. Lihat perinciannya di [Buat server di cloud pribadi virtual](#).

- Titik akhir publik tidak dapat membatasi lalu lintas melalui grup keamanan. Untuk menggunakan grup keamanan dengan server Transfer Family, Anda harus meng-host endpoint server Anda di dalam virtual private cloud (VPC) seperti yang dijelaskan dalam. [Buat server di cloud pribadi virtual](#)

Lihat juga

- Kami memberikan AWS CDK contoh untuk membuat server SFTP Transfer Family. Contoh menggunakan TypeScript, dan tersedia di GitHub [sini](#).
- Untuk panduan tentang cara menerapkan server Transfer Family di dalam VPC, lihat [Gunakan daftar izin IP untuk mengamankan server Anda](#). AWS Transfer Family

Untuk membuat SFTP-enabled server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/> dan pilih Server dari panel navigasi, lalu pilih Buat server.
2. Di Pilih protokol, pilih SFTP, lalu pilih Berikutnya.
3. Di Pilih penyedia identitas, pilih penyedia identitas yang ingin Anda gunakan untuk mengelola akses pengguna. Anda memiliki opsi berikut:
 - Layanan dikelola - Anda menyimpan identitas dan kunci pengguna. AWS Transfer Family
 - AWS Directory Service for Microsoft Active Directory— Anda menyediakan Directory Service direktori untuk mengakses titik akhir. Dengan demikian, Anda dapat menggunakan kredensial yang disimpan di Active Directory untuk mengautentikasi pengguna Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan penyedia AWS Managed Microsoft AD identitas, lihat [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

 Note

- Cross-Account dan Direktori bersama tidak didukung untuk AWS Managed Microsoft AD.
- Untuk menyiapkan server dengan Directory Service sebagai penyedia identitas Anda, Anda perlu menambahkan beberapa Directory Service izin. Lihat perinciannya di [Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory](#).

- Penyedia identitas khusus - Pilih salah satu opsi berikut:

- Gunakan AWS Lambda untuk menghubungkan penyedia identitas Anda — Anda dapat menggunakan penyedia identitas yang ada, didukung oleh fungsi Lambda. Anda memberikan nama fungsi Lambda. Untuk informasi selengkapnya, lihat [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#).
- Gunakan Amazon API Gateway untuk menghubungkan penyedia identitas Anda — Anda dapat membuat metode API Gateway yang didukung oleh fungsi Lambda untuk digunakan sebagai penyedia identitas. Anda menyediakan URL Amazon API Gateway dan peran pemanggilan. Untuk informasi selengkapnya, lihat [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

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

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

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

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

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

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

AWS Lambda function





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

☒ **Password OR public key**
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

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

Cancel Previous Next

4. Pilih Berikutnya.

5. Di Pilih titik akhir, lakukan hal berikut:

- a. Untuk tipe Endpoint, pilih tipe titik akhir yang dapat diakses publik. Untuk titik akhir yang dihosting VPC, lihat. [Buat server di cloud pribadi virtual](#)
- b. Untuk jenis alamat IP, pilih IPv4 (default) untuk kompatibilitas mundur atau untuk mengaktifkan koneksi IPv4 dan IPv6 Dual-stack titik akhir Anda.

 Note

Dual-stack mode memungkinkan endpoint Transfer Family Anda untuk berkomunikasi dengan klien berkemampuan IPv4 dan IPv6. Ini memungkinkan Anda untuk secara bertahap beralih dari sistem berbasis IPv4 ke IPv6 tanpa perlu beralih sekaligus.

- c. (Opsional) Untuk nama host Kustom, pilih Tidak Ada.

Anda mendapatkan nama host server yang disediakan oleh AWS Transfer Family. Nama host server mengambil formulir `serverId.server.transfer.regionId.amazonaws.com`.

Untuk nama host kustom, Anda menentukan alias kustom untuk endpoint server Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan nama host kustom, lihat [Bekerja dengan nama host khusus](#).

- d. (Opsional) Untuk FIPS Diaktifkan, pilih kotak centang titik akhir Diaktifkan FIPS untuk memastikan bahwa titik akhir sesuai dengan Standar Pemrosesan Informasi Federal (FIPS).

 Note

FIPS-enabled titik akhir hanya tersedia di AWS Wilayah Amerika Utara. Untuk Wilayah yang tersedia, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS Untuk informasi lebih lanjut tentang FIPS, lihat [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- e. Pilih Berikutnya.

6. Pada halaman Pilih domain, pilih layanan AWS penyimpanan yang ingin Anda gunakan untuk menyimpan dan mengakses data Anda melalui protokol yang dipilih:

- Pilih Amazon S3 untuk menyimpan dan mengakses file Anda sebagai objek di atas protokol yang dipilih.
- Pilih Amazon EFS untuk menyimpan dan mengakses file Anda di sistem file Amazon EFS Anda melalui protokol yang dipilih.

Pilih Berikutnya.

7. Di Konfigurasi detail tambahan, lakukan hal berikut:

- a. Untuk logging, tentukan grup log yang ada atau buat yang baru (opsi default). Jika Anda memilih grup log yang ada, Anda harus memilih salah satu yang terkait dengan Akun AWS.

Jika Anda memilih Buat grup log, CloudWatch konsol (<https://console.aws.amazon.com/cloudwatch/>) terbuka ke halaman Buat grup log. Untuk detailnya, lihat [Membuat grup log di CloudWatch Log](#).

- b. (Opsional) Untuk alur kerja Terkelola, pilih ID alur kerja (dan peran terkait) yang harus diasumsikan oleh Transfer Family saat menjalankan alur kerja. Anda dapat memilih satu alur kerja untuk dieksekusi setelah unggahan lengkap, dan satu lagi untuk mengeksekusi pada unggahan sebagian. Untuk mempelajari lebih lanjut tentang memproses file Anda menggunakan alur kerja terkelola, lihat [AWS Transfer Family alur kerja terkelola](#).

The screenshot shows the 'Managed workflows' section in the AWS Transfer Family console. It includes three configuration areas:

- Workflow for complete file uploads:** A dropdown menu with 'w-' selected, a refresh button, and a 'Create a new Workflow' button with an external link icon.
- Workflow for partial file uploads:** A dropdown menu with 'w-' selected, a refresh button, and a 'Create a new Workflow' button with an external link icon.
- Managed workflows execution role:** A dropdown menu with a role name selected, a refresh button, and an 'Info' link.

- c. Untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritma kriptografi yang diaktifkan untuk digunakan oleh server Anda. Kebijakan keamanan terbaru kami adalah default: untuk detailnya, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).
- d. (Opsional) Untuk Server Host Key, masukkan kunci pribadi RSA, ED25519, atau ECDSA yang akan digunakan untuk mengidentifikasi server Anda ketika klien terhubung ke sana melalui SFTP. Anda juga dapat menambahkan deskripsi untuk membedakan antara beberapa kunci host.

Setelah Anda membuat server Anda, Anda dapat menambahkan kunci host tambahan. Memiliki beberapa kunci host berguna jika Anda ingin memutar tombol atau jika Anda ingin memiliki berbagai jenis kunci, seperti kunci RSA dan juga kunci ECDSA.

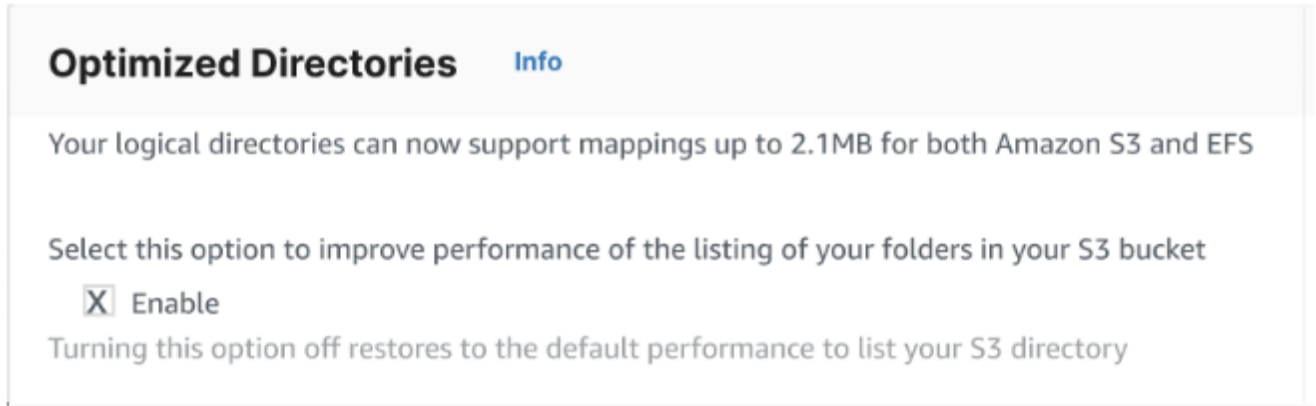
Note

Bagian Server Host Key hanya digunakan untuk memigrasikan pengguna dari SFTP-enabled server yang ada.

- e. (Opsional) Untuk Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, lalu pilih Tambahkan tag.
- f. Pilih Berikutnya.
- g. Anda dapat mengoptimalkan kinerja untuk direktori Amazon S3 Anda. Misalnya, Anda masuk ke direktori home Anda, dan Anda memiliki 10.000 subdirektori. Dengan kata lain, bucket Amazon S3 Anda memiliki 10.000 folder. Dalam skenario ini, jika Anda menjalankan perintah `ls` (daftar), operasi daftar memakan waktu antara enam dan delapan menit.

Namun, jika Anda mengoptimalkan direktori Anda, operasi ini hanya membutuhkan beberapa detik.

Saat Anda membuat server menggunakan konsol, direktori yang dioptimalkan diaktifkan secara default. Jika Anda membuat server menggunakan API, perilaku ini tidak diaktifkan secara default.



- h. (Opsional) Konfigurasi AWS Transfer Family server untuk menampilkan pesan yang disesuaikan seperti kebijakan organisasi atau syarat dan ketentuan kepada pengguna akhir Anda. Untuk Spanduk tampilan, di kotak teks spanduk Pre-authentication tampilan, masukkan pesan teks yang ingin ditampilkan kepada pengguna Anda sebelum mereka mengautentikasi.
- i. (Opsional) Anda dapat mengonfigurasi opsi tambahan berikut.
 - SetStat opsi: aktifkan opsi ini untuk mengabaikan kesalahan yang dihasilkan saat klien mencoba menggunakan SETSTAT pada file yang Anda unggah ke bucket Amazon S3. Untuk detail tambahan, lihat SetStatOption dokumentasi di [ProtocolDetails](#).
 - Dimulainya kembali sesi TLS: opsi ini hanya tersedia jika Anda telah mengaktifkan FTPS sebagai salah satu protokol untuk server ini.
 - IP Pasif: opsi ini hanya tersedia jika Anda telah mengaktifkan FTPS atau FTP sebagai salah satu protokol untuk server ini.

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. Di Tinjau dan buat, tinjau pilihan Anda.

- Jika Anda ingin mengedit salah satu dari mereka, pilih Edit di sebelah langkah.

Note

Anda harus meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Jika Anda tidak memiliki perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file, tetapi Anda harus membuat pengguna terlebih dahulu. Untuk detail tentang membuat pengguna, lihat [Mengelola pengguna untuk titik akhir server](#).

Buat FTPS-enabled server

File Transfer Protocol over SSL (FTPS) adalah ekstensi ke FTP. Ini menggunakan protokol kriptografi Transport Layer Security (TLS) dan Secure Sockets Layer (SSL) untuk mengenkripsi lalu lintas. FTPS memungkinkan enkripsi koneksi kontrol dan saluran data baik secara bersamaan maupun independen.

Note

Untuk pertimbangan penting tentang Network Load Balancers, lihat [Hindari menempatkan NLB dan NAT di depan AWS Transfer Family server](#)

Untuk membuat FTPS-enabled server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/> dan pilih Server dari panel navigasi, lalu pilih Buat server.
2. Di Pilih protokol, pilih FTPS.

Untuk sertifikat Server, pilih sertifikat yang disimpan di AWS Certificate Manager (ACM) yang akan digunakan untuk mengidentifikasi server Anda ketika klien terhubung ke sana melalui FTPS dan kemudian pilih Berikutnya.

Untuk meminta sertifikat publik baru, lihat [Meminta sertifikat publik](#) di Panduan AWS Certificate Manager Pengguna.

Untuk mengimpor sertifikat yang ada ke ACM, lihat [Mengimpor sertifikat ke ACM di Panduan Pengguna](#). AWS Certificate Manager

Untuk meminta sertifikat pribadi untuk menggunakan FTPS melalui alamat IP pribadi, lihat [Meminta Sertifikat Pribadi](#) di AWS Certificate Manager Panduan Pengguna.

Sertifikat dengan algoritme kriptografi dan ukuran kunci berikut didukung:

- 2048-bit RSA (RSA_2048)
- 4096-bit RSA (RSA_4096)

- Elliptic Prime Curve 256 bit (EC_prime256v1)
- Elliptic Prime Curve 384 bit (EC_secp384r1)
- Elliptic Prime Curve 521 bit (EC_secp521r1)

 Note

Sertifikat harus berupa sertifikat SSL/TLS X.509 versi 3 yang valid dengan FQDN atau alamat IP yang ditentukan dan berisi informasi tentang penerbit.

3. Di Pilih penyedia identitas, pilih penyedia identitas yang ingin Anda gunakan untuk mengelola akses pengguna. Anda memiliki opsi berikut:

- AWS Directory Service for Microsoft Active Directory— Anda menyediakan Directory Service direktori untuk mengakses titik akhir. Dengan demikian, Anda dapat menggunakan kredensial yang disimpan di Active Directory untuk mengautentikasi pengguna Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan penyedia AWS Managed Microsoft AD identitas, lihat [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

 Note

- Cross-Account dan Direktori bersama tidak didukung untuk AWS Managed Microsoft AD.
- Untuk menyiapkan server dengan Directory Service sebagai penyedia identitas Anda, Anda perlu menambahkan beberapa Directory Service izin. Lihat perinciannya di [Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory](#).

- Penyedia identitas khusus - Pilih salah satu opsi berikut:
 - Gunakan AWS Lambda untuk menghubungkan penyedia identitas Anda — Anda dapat menggunakan penyedia identitas yang ada, didukung oleh fungsi Lambda. Anda memberikan nama fungsi Lambda. Untuk informasi selengkapnya, lihat [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#).
 - Gunakan Amazon API Gateway untuk menghubungkan penyedia identitas Anda — Anda dapat membuat metode API Gateway yang didukung oleh fungsi Lambda untuk digunakan sebagai penyedia identitas. Anda menyediakan URL Amazon API Gateway dan peran

pemanggilan. Untuk informasi selengkapnya, lihat [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Pilih Berikutnya.
5. Di Pilih titik akhir, lakukan hal berikut:

[i](#) Note

Server FTPS untuk Transfer Family beroperasi melalui Port 21 (Saluran Kontrol) dan Rentang Port 8192-8200 (Saluran Data).

- a. Untuk tipe Endpoint, pilih tipe endpoint yang dihosting VPC untuk meng-host endpoint server Anda. Untuk informasi tentang menyiapkan titik akhir yang dihosting VPC Anda, lihat [Buat server di cloud pribadi virtual](#)

 Note

Titik akhir yang dapat diakses publik tidak didukung.

- b. (Opsional) Untuk FIPS Diaktifkan, pilih kotak centang titik akhir Diaktifkan FIPS untuk memastikan bahwa titik akhir sesuai dengan Standar Pemrosesan Informasi Federal (FIPS).

 Note

FIPS-enabled titik akhir hanya tersedia di AWS Wilayah Amerika Utara. Untuk Wilayah yang tersedia, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS Untuk informasi lebih lanjut tentang FIPS, lihat [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- c. Pilih Berikutnya.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

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

☐ FIPS Enabled endpoint

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

6. Pada halaman Pilih domain, pilih layanan AWS penyimpanan yang ingin Anda gunakan untuk menyimpan dan mengakses data Anda melalui protokol yang dipilih:

- Pilih Amazon S3 untuk menyimpan dan mengakses file Anda sebagai objek di atas protokol yang dipilih.
- Pilih Amazon EFS untuk menyimpan dan mengakses file Anda di sistem file Amazon EFS Anda melalui protokol yang dipilih.

Pilih Berikutnya.

7. Di Konfigurasi detail tambahan, lakukan hal berikut:

- a. Untuk logging, tentukan grup log yang ada atau buat yang baru (opsi default).

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

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

Jika Anda memilih Buat grup log, CloudWatch konsol (<https://console.aws.amazon.com/cloudwatch/>) terbuka ke halaman Buat grup log. Untuk detailnya, lihat [Membuat grup log di CloudWatch Log](#).

- b. (Opsional) Untuk alur kerja Terkelola, pilih ID alur kerja (dan peran terkait) yang harus diasumsikan oleh Transfer Family saat menjalankan alur kerja. Anda dapat memilih satu alur kerja untuk dieksekusi setelah unggahan lengkap, dan satu lagi untuk mengeksekusi pada unggahan sebagian. Untuk mempelajari lebih lanjut tentang memproses file Anda menggunakan alur kerja terkelola, lihat [AWS Transfer Family alur kerja terkelola](#).

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

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

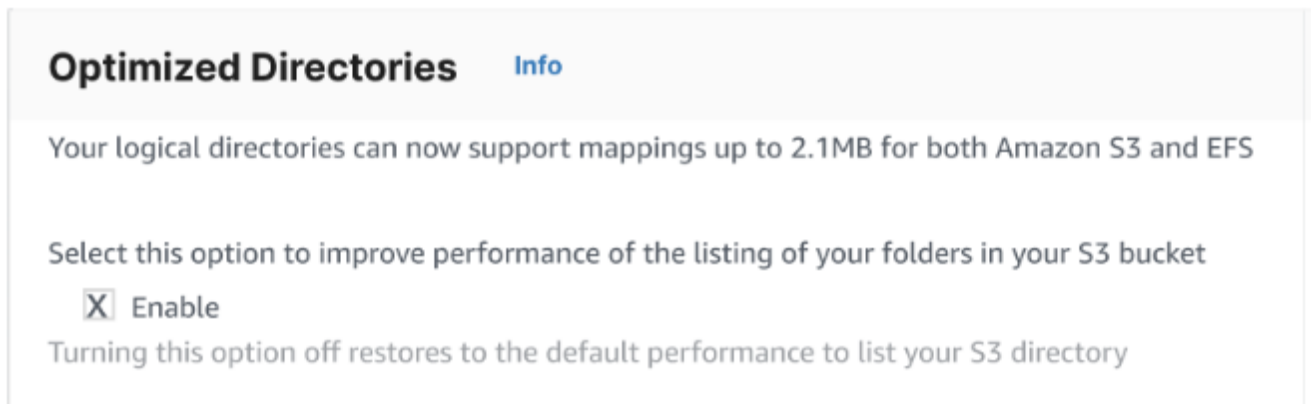
Managed workflows execution role Info
Select the role that AWS Transfer Family should assume when executing a workflow

- c. Untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritma kriptografi yang diaktifkan untuk digunakan oleh server Anda. Kebijakan keamanan terbaru kami

adalah default: untuk detailnya, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

- d. Untuk Server Host Key, biarkan kosong.
- e. (Opsional) Untuk Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, lalu pilih Tambahkan tag.
- f. Anda dapat mengoptimalkan kinerja untuk direktori Amazon S3 Anda. Misalnya, Anda masuk ke direktori home Anda, dan Anda memiliki 10.000 subdirektori. Dengan kata lain, bucket Amazon S3 Anda memiliki 10.000 folder. Dalam skenario ini, jika Anda menjalankan perintah `ls` (daftar), operasi daftar memakan waktu antara enam dan delapan menit. Namun, jika Anda mengoptimalkan direktori Anda, operasi ini hanya membutuhkan beberapa detik.

Saat Anda membuat server menggunakan konsol, direktori yang dioptimalkan diaktifkan secara default. Jika Anda membuat server menggunakan API, perilaku ini tidak diaktifkan secara default.



- g. Pilih Berikutnya.
- h. (Opsional) Anda dapat mengonfigurasi AWS Transfer Family server untuk menampilkan pesan yang disesuaikan seperti kebijakan organisasi atau syarat dan ketentuan kepada pengguna akhir Anda. Anda juga dapat menampilkan Message of The Day (MOTD) yang disesuaikan kepada pengguna yang telah berhasil diautentikasi.

Untuk Spanduk tampilan, di kotak teks spanduk Pre-authentication tampilan, masukkan pesan teks yang ingin ditampilkan kepada pengguna Anda sebelum mereka mengautentikasi, dan di kotak teks spanduk Post-authentication tampilan, masukkan teks yang ingin Anda tampilkan kepada pengguna Anda setelah mereka berhasil mengautentikasi.

- i. (Opsional) Anda dapat mengonfigurasi opsi tambahan berikut.

- SetStat opsi: aktifkan opsi ini untuk mengabaikan kesalahan yang dihasilkan saat klien mencoba menggunakan SETSTAT pada file yang Anda unggah ke bucket Amazon S3. Untuk detail tambahan, lihat SetStatOption dokumentasi dalam [ProtocolDetails](#) topik.
- Dimulainya kembali sesi TLS: menyediakan mekanisme untuk melanjutkan atau berbagi kunci rahasia yang dinegosiasikan antara kontrol dan koneksi data untuk sesi FTPS. Untuk detail tambahan, lihat TlsSessionResumptionMode dokumentasi dalam [ProtocolDetails](#) topik.
- IP pasif: menunjukkan mode pasif, untuk protokol FTP dan FTPS. Masukkan satu alamat IPv4, seperti alamat IP publik firewall, router, atau penyeimbang beban. Untuk detail tambahan, lihat PassiveIp dokumentasi dalam [ProtocolDetails](#) topik.

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. Di Tinjau dan buat, tinjau pilihan Anda.

- Jika Anda ingin mengedit salah satu dari mereka, pilih Edit di sebelah langkah.

 Note

Anda harus meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Jika Anda tidak memiliki perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file untuk pengguna Anda.

Langkah selanjutnya: Untuk langkah selanjutnya, lanjutkan [Bekerja dengan penyedia identitas khusus](#) untuk mengatur pengguna.

Buat FTP-enabled server

File Transfer Protocol (FTP) adalah protokol jaringan yang digunakan untuk transfer data. FTP menggunakan saluran terpisah untuk kontrol dan transfer data. Saluran kontrol terbuka hingga batas waktu dihentikan atau tidak aktif. Saluran data aktif selama transfer. FTP menggunakan teks yang jelas dan tidak mendukung enkripsi lalu lintas.

 Note

Saat Anda mengaktifkan FTP, Anda harus memilih opsi akses internal untuk titik VPC-hosted akhir. Jika Anda membutuhkan server Anda untuk memiliki data melintasi jaringan publik, Anda harus menggunakan protokol aman, seperti SFTP atau FTPS.

 Note

Untuk pertimbangan penting tentang Network Load Balancers, lihat. [Hindari menempatkan NLB dan NAT di depan AWS Transfer Family server](#)

Untuk membuat FTP-enabled server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/> dan pilih Server dari panel navigasi, lalu pilih Buat server.

2. Di Pilih protokol, pilih FTP, lalu pilih Berikutnya.
3. Di Pilih penyedia identitas, pilih penyedia identitas yang ingin Anda gunakan untuk mengelola akses pengguna. Anda memiliki opsi berikut:
 - AWS Directory Service for Microsoft Active Directory— Anda menyediakan Directory Service direktori untuk mengakses titik akhir. Dengan demikian, Anda dapat menggunakan kredensial yang disimpan di Active Directory untuk mengautentikasi pengguna Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan penyedia AWS Managed Microsoft AD identitas, lihat [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

 Note

- Cross-Account dan Direktori bersama tidak didukung untuk AWS Managed Microsoft AD.
 - Untuk menyiapkan server dengan Directory Service sebagai penyedia identitas Anda, Anda perlu menambahkan beberapa Directory Service izin. Lihat perinciannya di [Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory](#).
- Penyedia identitas khusus - Pilih salah satu opsi berikut:
 - Gunakan AWS Lambda untuk menghubungkan penyedia identitas Anda — Anda dapat menggunakan penyedia identitas yang ada, didukung oleh fungsi Lambda. Anda memberikan nama fungsi Lambda. Untuk informasi selengkapnya, lihat [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#).
 - Gunakan Amazon API Gateway untuk menghubungkan penyedia identitas Anda — Anda dapat membuat metode API Gateway yang didukung oleh fungsi Lambda untuk digunakan sebagai penyedia identitas. Anda menyediakan URL Amazon API Gateway dan peran pemanggilan. Untuk informasi selengkapnya, lihat [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#).

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

To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Pilih Berikutnya.
5. Di Pilih titik akhir, lakukan hal berikut:

Note

Server FTP untuk Transfer Family beroperasi melalui Port 21 (Saluran Kontrol) dan Rentang Port 8192-8200 (Saluran Data).

- a. Untuk jenis Endpoint, pilih VPC yang dihosting untuk meng-host endpoint server Anda. Untuk informasi tentang menyiapkan titik akhir yang dihosting VPC Anda, lihat. [Buat server di cloud pribadi virtual](#)

 Note

Titik akhir yang dapat diakses publik tidak didukung.

- b. Untuk FIPS Diaktifkan, biarkan kotak centang titik akhir FIPS Enabled tetap bersih.

 Note

FIPS-enabled endpoint tidak didukung untuk server FTP.

- c. Pilih Berikutnya.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

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

☐ FIPS Enabled endpoint

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

6. Pada halaman Pilih domain, pilih layanan AWS penyimpanan yang ingin Anda gunakan untuk menyimpan dan mengakses data Anda melalui protokol yang dipilih.

- Pilih Amazon S3 untuk menyimpan dan mengakses file Anda sebagai objek di atas protokol yang dipilih.
- Pilih Amazon EFS untuk menyimpan dan mengakses file Anda di sistem file Amazon EFS Anda melalui protokol yang dipilih.

Pilih Berikutnya.

7. Di Konfigurasi detail tambahan, lakukan hal berikut:

- a. Untuk logging, tentukan grup log yang ada atau buat yang baru (opsi default).

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

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

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

Jika Anda memilih Buat grup log, CloudWatch konsol (<https://console.aws.amazon.com/cloudwatch/>) terbuka ke halaman Buat grup log. Untuk detailnya, lihat [Membuat grup log di CloudWatch Log](#).

- b. (Opsional) Untuk alur kerja Terkelola, pilih ID alur kerja (dan peran terkait) yang harus diasumsikan oleh Transfer Family saat menjalankan alur kerja. Anda dapat memilih satu alur kerja untuk dieksekusi setelah unggahan lengkap, dan satu lagi untuk mengeksekusi pada unggahan sebagian. Untuk mempelajari lebih lanjut tentang memproses file Anda menggunakan alur kerja terkelola, lihat [AWS Transfer Family alur kerja terkelola](#).

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

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

Managed workflows execution role Info
Select the role that AWS Transfer Family should assume when executing a workflow

- c. Untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritma kriptografi yang diaktifkan untuk digunakan oleh server Anda.

 Note

Transfer Family menetapkan kebijakan keamanan terbaru ke server FTP Anda. Namun, karena protokol FTP tidak menggunakan enkripsi apa pun, server FTP tidak menggunakan algoritma kebijakan keamanan apa pun. Kecuali server Anda juga menggunakan protokol FTPS atau SFTP, kebijakan keamanan tetap tidak digunakan.

- d. Untuk Server Host Key, biarkan kosong.
- e. (Opsional) Untuk Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, lalu pilih Tambahkan tag.
- f. Anda dapat mengoptimalkan kinerja untuk direktori Amazon S3 Anda. Misalnya, Anda masuk ke direktori home Anda, dan Anda memiliki 10.000 subdirektori. Dengan kata lain, bucket Amazon S3 Anda memiliki 10.000 folder. Dalam skenario ini, jika Anda menjalankan perintah `ls` (daftar), operasi daftar memakan waktu antara enam dan delapan menit. Namun, jika Anda mengoptimalkan direktori Anda, operasi ini hanya membutuhkan beberapa detik.

Saat Anda membuat server menggunakan konsol, direktori yang dioptimalkan diaktifkan secara default. Jika Anda membuat server menggunakan API, perilaku ini tidak diaktifkan secara default.

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. Pilih Berikutnya.
- h. (Opsional) Anda dapat mengonfigurasi AWS Transfer Family server untuk menampilkan pesan yang disesuaikan seperti kebijakan organisasi atau syarat dan ketentuan kepada pengguna akhir Anda. Anda juga dapat menampilkan Message of The Day (MOTD) yang disesuaikan kepada pengguna yang telah berhasil diautentikasi.

Untuk Spanduk tampilan, di kotak teks spanduk Pre-authentication tampilan, masukkan pesan teks yang ingin ditampilkan kepada pengguna Anda sebelum mereka mengautentikasi, dan di kotak teks spanduk Post-authentication tampilan, masukkan teks yang ingin Anda tampilkan kepada pengguna Anda setelah mereka berhasil mengautentikasi.

- i. (Opsional) Anda dapat mengonfigurasi opsi tambahan berikut.
 - SetStat opsi: aktifkan opsi ini untuk mengabaikan kesalahan yang dihasilkan saat klien mencoba menggunakan SETSTAT pada file yang Anda unggah ke bucket Amazon S3. Untuk detail tambahan, lihat SetStatOption dokumentasi dalam [ProtocolDetails](#) topik.
 - Dimulainya kembali sesi TLS: menyediakan mekanisme untuk melanjutkan atau berbagi kunci rahasia yang dinegosiasikan antara kontrol dan koneksi data untuk sesi FTPS. Untuk detail tambahan, lihat TlsSessionResumptionMode dokumentasi dalam [ProtocolDetails](#) topik.
 - IP pasif: menunjukkan mode pasif, untuk protokol FTP dan FTPS. Masukkan satu alamat IPv4, seperti alamat IP publik firewall, router, atau penyeimbang beban. Untuk detail tambahan, lihat PassiveIp dokumentasi dalam [ProtocolDetails](#) topik.

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. Di Tinjau dan buat, tinjau pilihan Anda.

- Jika Anda ingin mengedit salah satu dari mereka, pilih Edit di sebelah langkah.

 Note

Anda harus meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Jika Anda tidak memiliki perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file untuk pengguna Anda.

Langkah selanjutnya — Untuk langkah selanjutnya, lanjutkan [Bekerja dengan penyedia identitas khusus](#) untuk mengatur pengguna.

Buat server di cloud pribadi virtual

Anda dapat meng-host endpoint server Anda di dalam virtual private cloud (VPC) untuk digunakan untuk mentransfer data ke dan dari bucket Amazon S3 atau sistem file Amazon EFS tanpa melalui internet publik.

Note

Setelah 19 Mei 2021, Anda tidak akan dapat membuat server menggunakan `EndpointType=VPC_ENDPOINT` di AWS akun Anda jika akun Anda belum melakukannya sebelum 19 Mei 2021. Jika Anda telah membuat server dengan `EndpointType=VPC_ENDPOINT` di AWS akun Anda pada atau sebelum 21 Februari 2021, Anda tidak akan terpengaruh. Setelah tanggal ini, gunakan `EndpointType =VPC`. Untuk informasi selengkapnya, lihat [the section called “Menghentikan penggunaan VPC_ENDPOINT”](#).

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi pribadi antara VPC dan server. Anda kemudian dapat menggunakan server ini untuk mentransfer data melalui klien Anda ke dan dari bucket Amazon S3 Anda tanpa menggunakan alamat IP publik atau memerlukan gateway internet.

Menggunakan Amazon VPC, Anda dapat meluncurkan AWS sumber daya di jaringan virtual khusus. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi selengkapnya tentang VPC, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.

Di bagian selanjutnya, temukan petunjuk tentang cara membuat dan menghubungkan VPC Anda ke server. Sebagai ikhtisar, Anda melakukan ini sebagai berikut:

1. Siapkan server menggunakan titik akhir VPC.
2. Connect ke server Anda menggunakan klien yang ada di dalam VPC Anda melalui titik akhir VPC. Melakukan hal ini memungkinkan Anda untuk mentransfer data yang disimpan di bucket Amazon S3 Anda melalui klien Anda menggunakan AWS Transfer Family Anda dapat melakukan transfer ini meskipun jaringan terputus dari internet publik.
3. Selain itu, jika Anda memilih untuk membuat titik akhir server Anda menghadap ke internet, Anda dapat mengaitkan alamat IP Elastic dengan titik akhir Anda. Melakukan hal ini memungkinkan klien di luar VPC Anda terhubung ke server Anda. Anda dapat menggunakan grup keamanan VPC

untuk mengontrol akses ke pengguna yang diautentikasi yang permintaannya hanya berasal dari alamat yang diizinkan.

 Note

AWS Transfer Family mendukung dual-stack endpoint, memungkinkan server Anda untuk berkomunikasi melalui IPv4 dan IPv6. Untuk mengaktifkan dukungan dual-stack, pilih opsi Enable DNS dual-stack endpoint saat membuat endpoint VPC Anda. Perhatikan bahwa VPC dan subnet Anda harus dikonfigurasi untuk mendukung IPv6 sebelum Anda dapat menggunakan fitur ini. Dual-stack dukungan sangat berguna ketika Anda memiliki klien yang perlu terhubung menggunakan salah satu protokol.

Untuk informasi tentang titik akhir server dual-stack (IPv4 dan IPv6), lihat. [Dukungan IPv6 untuk server Transfer Family](#)

Topik

- [Buat endpoint server yang hanya dapat diakses dalam VPC Anda](#)
- [Buat titik akhir yang menghadap ke internet untuk server Anda](#)
- [Ubah tipe endpoint untuk server Anda](#)
- [Menghentikan penggunaan VPC_ENDPOINT](#)
- [Membatasi akses endpoint VPC untuk server Transfer Family](#)
- [Fitur jaringan tambahan](#)
- [Memperbarui tipe endpoint AWS Transfer Family server dari VPC_ENDPOINT ke VPC](#)

Buat endpoint server yang hanya dapat diakses dalam VPC Anda

Dalam prosedur berikut, Anda membuat endpoint server yang hanya dapat diakses oleh sumber daya dalam VPC Anda.

Untuk membuat endpoint server di dalam VPC

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Dari panel navigasi, pilih Server, lalu pilih Buat server.
3. Di Pilih protokol, pilih satu atau beberapa protokol, lalu pilih Berikutnya. Untuk informasi lebih lanjut tentang protokol, lihat. [Langkah 2: Buat SFTP-enabled server](#)

4. Di Pilih penyedia identitas, pilih Layanan yang dikelola untuk menyimpan identitas dan kunci pengguna AWS Transfer Family, lalu pilih Berikutnya.

Prosedur ini menggunakan opsi yang dikelola layanan. Jika Anda memilih Kustom, Anda menyediakan titik akhir Amazon API Gateway dan peran AWS Identity and Access Management (IAM) untuk mengakses titik akhir. Dengan demikian, Anda dapat mengintegrasikan layanan direktori Anda untuk mengautentikasi dan mengotorisasi pengguna Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan penyedia identitas kustom, lihat [Bekerja dengan penyedia identitas khusus](#).

5. Di Pilih titik akhir, lakukan hal berikut:
 - a. Untuk tipe Endpoint, pilih tipe endpoint yang dihosting VPC untuk meng-host endpoint server Anda.
 - b. Untuk Access, pilih Internal untuk membuat endpoint Anda hanya dapat diakses oleh klien menggunakan alamat IP pribadi endpoint.

Untuk detail tentang opsi Menghadapi Internet, lihat [Buat titik akhir yang menghadap ke internet untuk server Anda](#). Server yang dibuat dalam VPC untuk akses internal saja tidak mendukung nama host khusus.

- c. Untuk VPC, pilih ID VPC yang ada atau pilih Buat VPC untuk membuat VPC baru.
 - d. Di bagian Availability Zones, pilih hingga tiga Availability Zones dan subnet terkait.
 - e. Di bagian Grup Keamanan, pilih ID atau ID grup keamanan yang ada atau pilih Buat grup keamanan untuk membuat grup keamanan baru. Untuk informasi selengkapnya tentang grup keamanan, lihat [Grup keamanan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud. Untuk membuat grup keamanan, lihat [Membuat grup keamanan](#) di Panduan Pengguna Amazon Virtual Private Cloud.

 Note

VPC Anda secara otomatis dilengkapi dengan grup keamanan default. Jika Anda tidak menentukan grup atau grup keamanan yang berbeda saat meluncurkan server, kami mengaitkan grup keamanan default dengan server Anda.

- Untuk aturan masuk untuk grup keamanan, Anda dapat mengonfigurasi lalu lintas SSH untuk menggunakan port 22, 2222, 22000, atau kombinasi apa pun. Port 22 dikonfigurasi secara default. Untuk menggunakan port 2222 atau port 22000, Anda menambahkan

aturan masuk ke grup keamanan Anda. Untuk jenisnya, pilih TCP Kustom, lalu masukkan salah satu **2222** atau **22000** untuk rentang Port, dan untuk sumbernya, masukkan rentang CIDR yang sama dengan yang Anda miliki untuk aturan port SSH 22 Anda.

- Untuk aturan masuk untuk grup keamanan, konfigurasi lalu lintas FTP dan FTPS untuk menggunakan rentang Port **21** untuk saluran kontrol dan **8192-8200** untuk saluran data.

 Note

Anda juga dapat menggunakan port 2223 untuk klien yang membutuhkan ACK “piggy-back” TCP, atau kemampuan untuk ack akhir dari jabat tangan 3 arah TCP untuk juga berisi data.

Beberapa perangkat lunak klien mungkin tidak kompatibel dengan port 2223: misalnya, klien yang memerlukan server untuk mengirim String Identifikasi SFTP sebelum klien melakukannya.

VPC > Security Groups > sg-[redacted]-default > Edit inbound rules

Edit inbound rules [Info](#)

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

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- f. (Optional) Untuk FIPS Diaktifkan, pilih kotak centang titik akhir Diaktifkan FIPS untuk memastikan titik akhir sesuai dengan Standar Pemrosesan Informasi Federal (FIPS).

Note

FIPS-enabled titik akhir hanya tersedia di AWS Wilayah Amerika Utara. Untuk Wilayah yang tersedia, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi

Umum AWS Untuk informasi lebih lanjut tentang FIPS, lihat [Federal Information Processing Standard \(FIPS\) 140-2](#).

- g. Pilih Berikutnya.
6. Di Konfigurasikan detail tambahan, lakukan hal berikut:
- a. Untuk CloudWatch logging, pilih salah satu dari berikut ini untuk mengaktifkan CloudWatch pencatatan Amazon dari aktivitas pengguna Anda:
 - Buat peran baru untuk memungkinkan Transfer Family membuat peran IAM secara otomatis, selama Anda memiliki izin yang tepat untuk membuat peran baru. Peran IAM yang dibuat disebut `AWSTransferLoggingAccess`.
 - Pilih peran yang ada untuk memilih peran IAM yang ada dari akun Anda. Di bawah Peran logging, pilih peran. Peran IAM ini harus menyertakan kebijakan kepercayaan dengan Layanan yang disetel ke `transfer.amazonaws.com`.

Untuk informasi selengkapnya tentang CloudWatch pencatatan, lihat [Konfigurasikan peran CloudWatch logging](#).

 Note

- Anda tidak dapat melihat aktivitas pengguna akhir CloudWatch jika Anda tidak menentukan peran logging.
- Jika Anda tidak ingin menyiapkan peran CloudWatch logging, pilih Pilih peran yang ada, tetapi jangan pilih peran logging.

- b. Untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritma kriptografi yang diaktifkan untuk digunakan oleh server Anda.

 Note

Secara default, kebijakan `TransferSecurityPolicy-2024-01` keamanan dilampirkan ke server Anda kecuali Anda memilih yang berbeda.

Untuk informasi selengkapnya tentang kebijakan keamanan, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

- c. (Opsional: bagian ini hanya untuk memigrasi pengguna dari SFTP-enabled server yang ada.) Untuk Server Host Key, masukkan kunci pribadi RSA, ED25519, atau ECDSA yang akan digunakan untuk mengidentifikasi server Anda ketika klien terhubung dengannya melalui SFTP.
 - d. (Opsional) Untuk Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, lalu pilih Tambahkan tag.
 - e. Pilih Berikutnya.
7. Di Tinjau dan buat, tinjau pilihan Anda. Jika Anda:
- Ingin mengedit salah satu dari mereka, pilih Edit di sebelah langkah.

 Note

Anda perlu meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Tidak ada perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file, tetapi Anda harus membuat pengguna terlebih dahulu. Untuk detail tentang membuat pengguna, lihat [Mengelola pengguna untuk titik akhir server](#).

Buat titik akhir yang menghadap ke internet untuk server Anda

Dalam prosedur berikut, Anda membuat endpoint server. Titik akhir ini dapat diakses melalui internet hanya untuk klien yang alamat IP sumbernya diizinkan di grup keamanan default VPC Anda. Selain itu, dengan menggunakan alamat IP Elastic untuk membuat titik akhir Anda menghadap ke internet, klien Anda dapat menggunakan alamat IP Elastic untuk memungkinkan akses ke titik akhir Anda di firewall mereka.

 Note

Hanya SFTP dan FTPS yang dapat digunakan pada titik akhir yang dihosting VPC yang menghadap ke internet.

Untuk membuat titik akhir yang menghadap ke internet

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Dari panel navigasi, pilih Server, lalu pilih Buat server.
3. Di Pilih protokol, pilih satu atau beberapa protokol, lalu pilih Berikutnya. Untuk informasi lebih lanjut tentang protokol, lihat. [Langkah 2: Buat SFTP-enabled server](#)
4. Di Pilih penyedia identitas, pilih Layanan yang dikelola untuk menyimpan identitas dan kunci pengguna AWS Transfer Family, lalu pilih Berikutnya.

Prosedur ini menggunakan opsi yang dikelola layanan. Jika Anda memilih Kustom, Anda menyediakan titik akhir Amazon API Gateway dan peran AWS Identity and Access Management (IAM) untuk mengakses titik akhir. Dengan demikian, Anda dapat mengintegrasikan layanan direktori Anda untuk mengautentikasi dan mengotorisasi pengguna Anda. Untuk mempelajari lebih lanjut tentang bekerja dengan penyedia identitas kustom, lihat [Bekerja dengan penyedia identitas khusus](#).

5. Di Pilih titik akhir, lakukan hal berikut:
 - a. Untuk tipe Endpoint, pilih tipe endpoint yang dihosting VPC untuk meng-host endpoint server Anda.
 - b. Untuk Akses, pilih Internet Facing untuk membuat titik akhir Anda dapat diakses oleh klien melalui internet.

 Note

Ketika Anda memilih Internet Facing, Anda dapat memilih alamat IP Elastis yang ada di setiap subnet atau subnet. Atau Anda dapat pergi ke konsol VPC (<https://console.aws.amazon.com/vpc/>) untuk mengalokasikan satu atau lebih alamat IP Elastis baru. Alamat ini dapat dimiliki oleh AWS atau oleh Anda. Anda tidak dapat mengaitkan alamat IP Elastis yang sudah digunakan dengan titik akhir Anda.

- c. (Opsional) Untuk nama host Kustom, pilih salah satu dari berikut ini:

 Note

Pelanggan AWS GovCloud (US) perlu terhubung melalui alamat IP Elastic secara langsung, atau membuat catatan nama host dalam Commercial Route 53 yang mengarah ke EIP mereka. Untuk informasi selengkapnya tentang menggunakan

Route 53 untuk GovCloud titik akhir, lihat [Menyiapkan Amazon Route 53 dengan AWS GovCloud \(US\) sumber daya Anda](#) di Panduan AWS GovCloud (US) Pengguna.

- Amazon Route 53 Alias DNS — jika nama host yang ingin Anda gunakan terdaftar di Route 53. Anda kemudian dapat memasukkan nama host.
- DNS lainnya — jika nama host yang ingin Anda gunakan terdaftar dengan penyedia DNS lain. Anda kemudian dapat memasukkan nama host.
- Tidak ada - untuk menggunakan titik akhir server dan tidak menggunakan nama host khusus. Nama host server mengambil formulir `server-id.server.transfer.region.amazonaws.com`.

 Note

Untuk pelanggan di AWS GovCloud (US), memilih None tidak membuat nama host dalam format ini.

Untuk mempelajari lebih lanjut tentang bekerja dengan nama host kustom, lihat [Bekerja dengan nama host khusus](#).

- d. Untuk VPC, pilih ID VPC yang ada atau pilih Buat VPC untuk membuat VPC baru.
- e. Di bagian Availability Zones, pilih hingga tiga Availability Zones dan subnet terkait. Untuk Alamat IPv4, pilih alamat IP Elastis untuk setiap subnet. Ini adalah alamat IP yang dapat digunakan klien Anda untuk memungkinkan akses ke titik akhir Anda di firewall mereka.

Tip: Anda harus menggunakan subnet publik untuk Availability Zones Anda, atau terlebih dahulu menyiapkan gateway internet jika Anda ingin menggunakan subnet pribadi.

- f. Di bagian Grup Keamanan, pilih ID atau ID grup keamanan yang ada atau pilih Buat grup keamanan untuk membuat grup keamanan baru. Untuk informasi selengkapnya tentang grup keamanan, lihat [Grup keamanan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud. Untuk membuat grup keamanan, lihat [Membuat grup keamanan](#) di Panduan Pengguna Amazon Virtual Private Cloud.

 Note

VPC Anda secara otomatis dilengkapi dengan grup keamanan default. Jika Anda tidak menentukan grup atau grup keamanan yang berbeda saat meluncurkan server, kami mengaitkan grup keamanan default dengan server Anda.

- Untuk aturan masuk untuk grup keamanan, Anda dapat mengonfigurasi lalu lintas SSH untuk menggunakan port 22, 2222, 22000, atau kombinasi apa pun. Port 22 dikonfigurasi secara default. Untuk menggunakan port 2222 atau port 22000, Anda menambahkan aturan masuk ke grup keamanan Anda. Untuk jenisnya, pilih TCP Kustom, lalu masukkan salah satu **2222** atau **22000** untuk rentang Port, dan untuk sumbernya, masukkan rentang CIDR yang sama dengan yang Anda miliki untuk aturan port SSH 22 Anda.
- Untuk aturan masuk untuk grup keamanan, konfigurasi lalu lintas FTPS untuk menggunakan rentang Port **21** untuk saluran kontrol dan **8192-8200** untuk saluran data.

 Note

Anda juga dapat menggunakan port 2223 untuk klien yang membutuhkan ACK “piggy-back” TCP, atau kemampuan untuk ack akhir dari jabat tangan 3 arah TCP untuk juga berisi data.

Beberapa perangkat lunak klien mungkin tidak kompatibel dengan port 2223: misalnya, klien yang memerlukan server untuk mengirim String Identifikasi SFTP sebelum klien melakukannya.

VPC > Security Groups > sg-[redacted]-default > Edit inbound rules

Edit inbound rules Info

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

Inbound rules Info

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- g. (Optional) Untuk FIPS Diaktifkan, pilih kotak centang titik akhir Diaktifkan FIPS untuk memastikan titik akhir sesuai dengan Standar Pemrosesan Informasi Federal (FIPS).

Note

FIPS-enabled titik akhir hanya tersedia di AWS Wilayah Amerika Utara. Untuk Wilayah yang tersedia, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi

Umum AWS Untuk informasi lebih lanjut tentang FIPS, lihat [Federal Information Processing Standard \(FIPS\) 140-2](#).

- h. Pilih Berikutnya.
6. Di Konfigurasikan detail tambahan, lakukan hal berikut:
- a. Untuk CloudWatch logging, pilih salah satu dari berikut ini untuk mengaktifkan CloudWatch pencatatan Amazon dari aktivitas pengguna Anda:
- Buat peran baru untuk memungkinkan Transfer Family membuat peran IAM secara otomatis, selama Anda memiliki izin yang tepat untuk membuat peran baru. Peran IAM yang dibuat disebut `AWSTransferLoggingAccess`.
 - Pilih peran yang ada untuk memilih peran IAM yang ada dari akun Anda. Di bawah Peran logging, pilih peran. Peran IAM ini harus menyertakan kebijakan kepercayaan dengan Layanan yang disetel ke `transfer.amazonaws.com`.

Untuk informasi selengkapnya tentang CloudWatch pencatatan, lihat [Konfigurasikan peran CloudWatch logging](#).

 Note

- Anda tidak dapat melihat aktivitas pengguna akhir CloudWatch jika Anda tidak menentukan peran logging.
- Jika Anda tidak ingin menyiapkan peran CloudWatch logging, pilih Pilih peran yang ada, tetapi jangan pilih peran logging.

- b. Untuk opsi algoritma kriptografi, pilih kebijakan keamanan yang berisi algoritma kriptografi yang diaktifkan untuk digunakan oleh server Anda.

 Note

Secara default, kebijakan `TransferSecurityPolicy-2024-01` keamanan dilampirkan ke server Anda kecuali Anda memilih yang berbeda.

Untuk informasi selengkapnya tentang kebijakan keamanan, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

- c. (Opsional: bagian ini hanya untuk memigrasi pengguna dari SFTP-enabled server yang ada.) Untuk Server Host Key, masukkan kunci pribadi RSA, ED25519, atau ECDSA yang akan digunakan untuk mengidentifikasi server Anda ketika klien terhubung dengannya melalui SFTP.
- d. (Opsional) Untuk Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, lalu pilih Tambahkan tag.
- e. Pilih Berikutnya.
- f. (Opsional) Untuk alur kerja Terkelola, pilih ID alur kerja (dan peran terkait) yang harus diasumsikan oleh Transfer Family saat menjalankan alur kerja. Anda dapat memilih satu alur kerja untuk dieksekusi setelah unggahan lengkap, dan satu lagi untuk mengeksekusi pada unggahan sebagian. Untuk mempelajari lebih lanjut tentang memproses file Anda menggunakan alur kerja terkelola, lihat [AWS Transfer Family alur kerja terkelola](#).

The screenshot shows the 'Managed workflows' section in the AWS Transfer Family console. It has a title 'Managed workflows' with an 'Info' link. Below the title, there are two sections for selecting workflows. The first section is 'Workflow for complete file uploads' with the instruction 'Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server'. It contains a dropdown menu with 'w-' followed by a redacted ID, a refresh button, and a 'Create a new Workflow' button with an external link icon. The second section is 'Workflow for partial file uploads' with the instruction 'Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server'. It also contains a dropdown menu with 'w-' followed by a redacted ID, a refresh button, and a 'Create a new Workflow' button with an external link icon. At the bottom, there is a section for 'Managed workflows execution role' with the instruction 'Select the role that AWS Transfer Family should assume when executing a workflow'. It features a dropdown menu with a redacted role name and a refresh button.

7. Di Tinjau dan buat, tinjau pilihan Anda. Jika Anda:

- Ingin mengedit salah satu dari mereka, pilih Edit di sebelah langkah.

Note

Anda perlu meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Tidak ada perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Anda dapat memilih ID server untuk melihat pengaturan rinci dari server yang baru saja Anda buat. Setelah kolom alamat IPv4 Publik diisi, alamat IP Elastis yang Anda berikan berhasil dikaitkan dengan titik akhir server Anda.

 Note

Ketika server Anda di VPC sedang online, hanya subnet yang dapat dimodifikasi dan hanya melalui API. [UpdateServer](#) Anda harus [menghentikan server](#) untuk menambah atau mengubah alamat IP Elastis titik akhir server.

Ubah tipe endpoint untuk server Anda

Jika Anda memiliki server yang sudah ada yang dapat diakses melalui internet (yaitu, memiliki tipe titik akhir publik), Anda dapat mengubah titik akhir ke titik akhir VPC.

 Note

Jika Anda memiliki server yang ada di VPC yang ditampilkan sebagai `VPC_ENDPOINT`, kami sarankan Anda memodifikasinya ke jenis titik akhir VPC yang baru. Dengan tipe endpoint baru ini, Anda tidak perlu lagi menggunakan Network Load Balancer (NLB) untuk mengaitkan alamat IP Elastis dengan endpoint server Anda. Selain itu, Anda dapat menggunakan grup keamanan VPC untuk membatasi akses ke titik akhir server Anda. Namun, Anda dapat terus menggunakan tipe `VPC_ENDPOINT` endpoint sesuai kebutuhan.

Prosedur berikut mengasumsikan bahwa Anda memiliki server yang menggunakan tipe endpoint publik saat ini atau tipe yang lebih lama `VPC_ENDPOINT`.

Untuk mengubah tipe endpoint untuk server Anda

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih kotak centang server yang ingin Anda ubah tipe endpoint.

 Important

Anda harus menghentikan server sebelum Anda dapat mengubah titik akhirnya.

4. Untuk Tindakan, pilih Berhenti.
5. Di kotak dialog konfirmasi yang muncul, pilih Berhenti untuk mengonfirmasi bahwa Anda ingin menghentikan server.

 Note

Sebelum melanjutkan ke langkah berikutnya, di detail Endpoint, tunggu Status server berubah menjadi Offline; ini bisa memakan waktu beberapa menit. Anda mungkin harus memilih Refresh di halaman Server untuk melihat perubahan status. Anda tidak akan dapat melakukan pengeditan apa pun sampai server Offline.

6. Di detail Endpoint, pilih Edit.
7. Dalam konfigurasi Edit titik akhir, lakukan hal berikut:
 - a. Untuk jenis Edit titik akhir, pilih VPC yang dihosting.
 - b. Untuk Access, pilih salah satu dari berikut ini:
 - Internal untuk membuat titik akhir Anda hanya dapat diakses oleh klien menggunakan alamat IP pribadi titik akhir.
 - Menghadapi Internet untuk membuat titik akhir Anda dapat diakses oleh klien melalui internet publik.

 Note

Ketika Anda memilih Internet Facing, Anda dapat memilih alamat IP Elastis yang ada di setiap subnet atau subnet. Atau, Anda dapat pergi ke konsol VPC (<https://console.aws.amazon.com/vpc/>) untuk mengalokasikan satu atau lebih alamat IP Elastis baru. Alamat ini dapat dimiliki oleh AWS atau oleh Anda. Anda tidak dapat mengaitkan alamat IP Elastis yang sudah digunakan dengan titik akhir Anda.

- c. (Opsional untuk akses yang menghadap internet saja) Untuk nama host Kustom, pilih salah satu dari berikut ini:
 - Amazon Route 53 Alias DNS — jika nama host yang ingin Anda gunakan terdaftar di Route 53. Anda kemudian dapat memasukkan nama host.
 - DNS lainnya — jika nama host yang ingin Anda gunakan terdaftar dengan penyedia DNS lain. Anda kemudian dapat memasukkan nama host.

- Tidak ada - untuk menggunakan titik akhir server dan tidak menggunakan nama host khusus. Nama host server mengambil formulir `serverId.server.transfer.regionId.amazonaws.com`.

Untuk mempelajari lebih lanjut tentang bekerja dengan nama host kustom, lihat [Bekerja dengan nama host khusus](#).

- d. Untuk VPC, pilih ID VPC yang ada, atau pilih Buat VPC untuk membuat VPC baru.
- e. Di bagian Availability Zones, pilih hingga tiga Availability Zones dan subnet terkait. Jika Internet Facing dipilih, pilih juga alamat IP Elastis untuk setiap subnet.

 Note

Jika Anda menginginkan maksimum tiga Availability Zone, tetapi tidak cukup tersedia, buat di konsol VPC () <https://console.aws.amazon.com/vpc/>.

Jika Anda memodifikasi subnet atau alamat IP Elastis, server membutuhkan beberapa menit untuk memperbarui. Anda tidak dapat menyimpan perubahan Anda sampai pembaruan server selesai.

- f. Pilih Simpan.
8. Untuk Tindakan, pilih Mulai dan tunggu status server berubah menjadi Online; ini bisa memakan waktu beberapa menit.

 Note

Jika Anda mengubah tipe titik akhir publik menjadi tipe titik akhir VPC, perhatikan bahwa tipe Endpoint untuk server Anda telah berubah menjadi VPC.

Grup keamanan default dilampirkan ke titik akhir. Untuk mengubah atau menambahkan grup keamanan tambahan, lihat [Membuat Grup Keamanan](#).

Menghentikan penggunaan VPC_ENDPOINT

AWS Transfer Family telah menghentikan kemampuan untuk membuat server dengan `EndpointType=VPC_ENDPOINT` untuk AWS akun baru. Per 19 Mei 2021, AWS akun yang tidak memiliki AWS Transfer Family server dengan tipe titik akhir tidak `VPC_ENDPOINT` akan dapat membuat server baru. `EndpointType=VPC_ENDPOINT` Jika Anda sudah memiliki server yang menggunakan tipe `VPC_ENDPOINT` endpoint, kami sarankan Anda mulai menggunakan

EndpointType=VPC sesegera mungkin. Untuk detailnya, lihat [Memperbarui jenis titik akhir AWS Transfer Family server Anda dari VPC_ENDPOINT ke VPC](#).

Kami meluncurkan tipe VPC endpoint baru di awal tahun 2020. Untuk informasi selengkapnya, lihat [AWS Transfer Family untuk SFTP mendukung Grup Keamanan VPC dan](#) alamat IP Elastis. Titik akhir baru ini lebih kaya fitur dan hemat biaya dan tidak ada PrivateLink biaya. Untuk informasi selengkapnya, lihat [harga AWS PrivateLink](#).

Tipe endpoint ini secara fungsional setara dengan tipe endpoint sebelumnya (). VPC_ENDPOINT Anda dapat melampirkan alamat IP Elastis langsung ke titik akhir untuk membuatnya menghadap internet dan menggunakan grup keamanan untuk penyaringan IP sumber. Untuk informasi selengkapnya, lihat [daftar Use IP allow untuk mengamankan postingan blog server SFTP Anda AWS Transfer Family](#).

Anda juga dapat meng-host titik akhir ini di lingkungan VPC bersama. Untuk informasi selengkapnya, lihat [AWS Transfer Family sekarang mendukung lingkungan VPC layanan bersama](#).

Selain SFTP, Anda dapat menggunakan VPC EndpointType untuk mengaktifkan FTPS dan FTP. Kami tidak berencana untuk menambahkan fitur dan FTPS/FTP dukungan ini EndpointType=VPC_ENDPOINT. Kami juga telah menghapus jenis titik akhir ini sebagai opsi dari AWS Transfer Family konsol.

Anda dapat mengubah jenis endpoint untuk server menggunakan konsol Transfer Family, API AWS CLI, SDK, atau CloudFormation Untuk mengubah jenis endpoint server Anda, lihat [Memperbarui tipe endpoint AWS Transfer Family server dari VPC_ENDPOINT ke VPC](#).

Jika Anda memiliki pertanyaan, hubungi AWS Dukungan atau tim AWS akun Anda.

Note

Kami tidak berencana untuk menambahkan fitur ini dan dukungan FTPS atau FTP ke = VPC_ENDPOINT. EndpointType Kami tidak lagi menawarkannya sebagai opsi di AWS Transfer Family Konsol.

Jika Anda memiliki pertanyaan tambahan, Anda dapat menghubungi kami melalui AWS Dukungan atau tim akun Anda.

Membatasi akses endpoint VPC untuk server Transfer Family

Saat membuat AWS Transfer Family server dengan tipe titik akhir VPC, pengguna dan kepala sekolah IAM Anda memerlukan izin untuk membuat dan menghapus titik akhir VPC. Namun, kebijakan keamanan organisasi Anda dapat membatasi izin ini. Anda dapat menggunakan kebijakan IAM untuk mengizinkan pembuatan dan penghapusan titik akhir VPC secara khusus untuk Transfer Family sambil mempertahankan batasan untuk layanan lain.

Important

Kebijakan IAM berikut memungkinkan pengguna untuk membuat dan menghapus titik akhir VPC hanya untuk server Transfer Family sementara menolak operasi ini untuk layanan lain:

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource": ["*"],
  "Condition": {
    "ForAnyValue:StringNotLike": {
      "ec2:VpceServiceName": [
        "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
      ]
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
      ]
    }
  }
}
```

Ganti *INPUT-YOUR-REGION* dengan AWS Wilayah Anda (misalnya, **us-east-1**) dan *INPUT-YOUR-ROLE* dengan peran IAM yang ingin Anda berikan izin ini.

Fitur jaringan tambahan

AWS Transfer Family menyediakan beberapa fitur jaringan canggih yang meningkatkan keamanan dan fleksibilitas saat menggunakan konfigurasi VPC:

- Dukungan lingkungan VPC bersama - Anda dapat meng-host endpoint server Transfer Family Anda di lingkungan VPC bersama. Untuk informasi selengkapnya, lihat [Menggunakan titik akhir yang dihosting VPC di VPC bersama](#). AWS Transfer Family
- Otentikasi dan keamanan - Anda dapat menggunakan Firewall Aplikasi AWS Web untuk melindungi titik akhir Amazon API Gateway Anda. Untuk informasi selengkapnya, lihat [Mengamankan AWS Transfer Family dengan Firewall Aplikasi AWS Web dan Amazon API Gateway](#).

Memperbarui tipe endpoint AWS Transfer Family server dari VPC_ENDPOINT ke VPC

Anda dapat menggunakan Konsol Manajemen AWS, CloudFormation, atau Transfer Family API untuk memperbarui server EndpointType dari VPC_ENDPOINT ke VPC. Prosedur dan contoh terperinci untuk menggunakan masing-masing metode ini untuk memperbarui jenis endpoint server disediakan di bagian berikut. Jika Anda memiliki server di beberapa AWS wilayah dan di beberapa AWS akun, Anda dapat menggunakan contoh skrip yang disediakan di bagian berikut, dengan modifikasi, untuk mengidentifikasi server menggunakan VPC_ENDPOINT jenis yang perlu Anda perbarui.

Topik

- [Mengidentifikasi server menggunakan tipe VPC_ENDPOINT endpoint](#)
- [Memperbarui tipe endpoint server menggunakan Konsol Manajemen AWS](#)
- [Memperbarui tipe endpoint server menggunakan CloudFormation](#)
- [Memperbarui server EndpointType menggunakan API](#)

Mengidentifikasi server menggunakan tipe **VPC_ENDPOINT** endpoint

Anda dapat mengidentifikasi server mana yang VPC_ENDPOINT menggunakan Konsol Manajemen AWS.

Untuk mengidentifikasi server menggunakan tipe **VPC_ENDPOINT** endpoint menggunakan konsol

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.

2. Pilih Server di panel navigasi untuk menampilkan daftar server di akun Anda di wilayah tersebut.
3. Urutkan daftar server berdasarkan jenis Endpoint untuk melihat semua server yang menggunakan VPC_ENDPOINT.

Untuk mengidentifikasi server yang menggunakan **VPC_ENDPOINT** berbagai AWS Wilayah dan akun

Jika Anda memiliki server di beberapa AWS wilayah dan di beberapa AWS akun, Anda dapat menggunakan contoh skrip berikut, dengan modifikasi, untuk mengidentifikasi server menggunakan tipe VPC_ENDPOINT endpoint. Contoh skrip menggunakan Amazon EC2 [DescribeRegions](#) dan operasi Transfer Family [ListServers](#) API. Jika Anda memiliki banyak AWS akun, Anda dapat melakukan loop melalui akun Anda menggunakan Peran IAM dengan akses auditor hanya baca jika Anda mengautentikasi menggunakan profil sesi ke penyedia identitas Anda.

1. Berikut ini adalah contoh sederhana.

```
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. Setelah Anda memiliki daftar server untuk diperbarui, Anda dapat menggunakan salah satu metode yang dijelaskan di bagian berikut untuk memperbarui EndpointType keVPC.

Memperbarui tipe endpoint server menggunakan Konsol Manajemen AWS

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.

2. Di panel navigasi, pilih Server.
3. Pilih kotak centang server yang ingin Anda ubah tipe endpoint.

 Important

Anda harus menghentikan server sebelum Anda dapat mengubah titik akhirnya.

4. Untuk Tindakan, pilih Berhenti.
5. Di kotak dialog konfirmasi yang muncul, pilih Berhenti untuk mengonfirmasi bahwa Anda ingin menghentikan server.

 Note

Sebelum melanjutkan ke langkah berikutnya, tunggu Status server berubah menjadi Offline; ini bisa memakan waktu beberapa menit. Anda mungkin harus memilih Refresh di halaman Server untuk melihat perubahan status.

6. Setelah status berubah menjadi Offline, pilih server untuk menampilkan halaman detail server.
7. Di bagian Detail titik akhir, pilih Edit.
8. Pilih VPC yang dihosting untuk tipe Endpoint.
9. Pilih Simpan.
10. Untuk Tindakan, pilih Mulai dan tunggu status server berubah menjadi Online; ini bisa memakan waktu beberapa menit.

Memperbarui tipe endpoint server menggunakan CloudFormation

Bagian ini menjelaskan cara menggunakan CloudFormation untuk memperbarui server EndpointType keVPC. Gunakan prosedur ini untuk server Transfer Family yang telah Anda gunakan CloudFormation. Dalam contoh ini, CloudFormation template asli yang digunakan untuk menyebarkan server Transfer Family ditampilkan sebagai berikut:

```
AWS::TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
```



```

VpcId:
  Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
        - !Select [2, !Ref SubnetIds]
      VpcEndpointType: Interface
      VpcId: !Ref VpcId

```

Template diperbarui dengan perubahan berikut:

- EndpointType diubah menjadi VPC.
- AWS::EC2::VPCEndpoint Sumber daya dihapus.
- Itu SecurityGroupIdSubnetIds,, dan VpcId dipindahkan ke EndpointDetails bagian AWS::Transfer::Server sumber daya,
- VpcEndpointId Properti EndpointDetails telah dihapus.

Template yang diperbarui terlihat sebagai berikut:

```

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
```

Untuk memperbarui jenis endpoint dari server Transfer Family yang digunakan CloudFormation

1. Hentikan server yang ingin Anda perbarui menggunakan langkah-langkah berikut.
 - a. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
 - b. Di panel navigasi, pilih Server.
 - c. Pilih kotak centang server yang ingin Anda ubah tipe endpoint.

 Important

Anda harus menghentikan server sebelum Anda dapat mengubah titik akhirnya.

- d. Untuk Tindakan, pilih Berhenti.
- e. Di kotak dialog konfirmasi yang muncul, pilih Berhenti untuk mengonfirmasi bahwa Anda ingin menghentikan server.

Note

Sebelum melanjutkan ke langkah berikutnya, tunggu Status server berubah menjadi Offline; ini bisa memakan waktu beberapa menit. Anda mungkin harus memilih Refresh di halaman Server untuk melihat perubahan status.

2. Perbarui CloudFormation tumpukan

- a. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
- b. Pilih tumpukan yang digunakan untuk membuat server Transfer Family.
- c. Pilih Perbarui.
- d. Pilih Ganti template saat ini
- e. Unggah template baru. CloudFormation Ubah Set membantu Anda memahami bagaimana perubahan template akan memengaruhi sumber daya yang berjalan sebelum Anda menerapkannya. Dalam contoh ini, sumber daya server Transfer akan dimodifikasi, dan sumber daya VPcendPoint akan dihapus. Server tipe titik akhir VPC membuat titik akhir VPC atas nama Anda, menggantikan sumber daya asli. VPCEndpoint

Setelah mengunggah template baru, set perubahan akan terlihat mirip dengan yang berikut ini:

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. Perbarui tumpukan.
- ## 3. Setelah pembaruan tumpukan selesai, navigasikan ke konsol manajemen Transfer Family di <https://console.aws.amazon.com/transfer/>.

4. Mulai ulang server. Pilih server yang Anda perbarui CloudFormation, lalu pilih Mulai dari menu Tindakan.

Memperbarui server EndpointType menggunakan API

Anda dapat menggunakan [perintah deskripsi-server](#), atau AWS CLI perintah API. [UpdateServer](#) Contoh skrip berikut menghentikan server Transfer Family, memperbarui EndpointType, menghapus VPC_ENDPOINT, dan memulai server.

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
            group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
```

```
print(transfer_update)
time.sleep(10)
transfer_start = transfer.start_server(ServerId=server_id)
print(transfer_start)
delete_vpc_endpoint =
ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
```

Bekerja dengan nama host khusus

Nama host server Anda adalah nama host yang pengguna Anda masukkan di klien mereka ketika mereka terhubung ke server Anda. Anda dapat menggunakan domain khusus yang telah Anda daftarkan untuk nama host server Anda saat Anda bekerja dengannya AWS Transfer Family. Misalnya, Anda mungkin menggunakan nama host khusus seperti `mysftpserver.mysubdomain.domain.com`.

Untuk mengarahkan lalu lintas dari domain kustom terdaftar ke titik akhir server, Anda dapat menggunakan Amazon Route 53 atau penyedia Sistem Nama Domain (DNS) apa pun. Route 53 adalah layanan DNS yang mendukung AWS Transfer Family secara native.

Topik

- [Gunakan Amazon Route 53 sebagai penyedia DNS Anda](#)
- [Gunakan penyedia DNS lainnya](#)
- [Nama host khusus untuk server yang dibuat non-konsol](#)

Di konsol, Anda dapat memilih salah satu opsi ini untuk menyiapkan nama host khusus:

- Amazon Route 53 Alias DNS — jika nama host yang ingin Anda gunakan terdaftar di Route 53. Anda kemudian dapat memasukkan nama host.
- DNS lainnya — jika nama host yang ingin Anda gunakan terdaftar dengan penyedia DNS lain. Anda kemudian dapat memasukkan nama host.
- Tidak ada - untuk menggunakan titik akhir server dan tidak menggunakan nama host khusus.

Anda mengatur opsi ini ketika Anda membuat server baru atau mengedit konfigurasi server yang ada. Untuk informasi selengkapnya tentang membuat server baru, lihat [Langkah 2: Buat SFTP-enabled server](#). Untuk informasi selengkapnya tentang mengedit konfigurasi server yang ada, lihat [Edit detail server](#).

Untuk detail selengkapnya tentang penggunaan domain Anda sendiri untuk nama host server dan cara AWS Transfer Family menggunakan Route 53, lihat bagian berikut.

Gunakan Amazon Route 53 sebagai penyedia DNS Anda

Saat membuat server, Anda dapat menggunakan Amazon Route 53 sebagai penyedia DNS Anda. Sebelum Anda menggunakan domain dengan Route 53, Anda mendaftarkan domain. Untuk informasi selengkapnya, lihat [Cara kerja pendaftaran Domain](#) di Panduan Pengembang Amazon Route 53.

Saat Anda menggunakan Route 53 untuk menyediakan perutean DNS ke server Anda, AWS Transfer Family gunakan nama host khusus yang Anda masukkan untuk mengekstrak zona hostingnya. Saat AWS Transfer Family mengekstrak zona yang dihosting, tiga hal dapat terjadi:

1. Jika Anda baru mengenal Route 53 dan tidak memiliki zona yang dihosting, AWS Transfer Family tambahkan zona host baru dan CNAME catatan. Nilai CNAME catatan ini adalah nama host endpoint untuk server Anda. CNAME adalah nama domain alternatif.
2. Jika Anda memiliki zona yang dihosting di Route 53 tanpa CNAME catatan apa pun, AWS Transfer Family tambahkan CNAME catatan ke zona yang dihosting.
3. Jika layanan mendeteksi bahwa CNAME rekaman sudah ada di zona yang dihosting, Anda akan melihat kesalahan yang menunjukkan bahwa CNAME rekaman sudah ada. Dalam hal ini, ubah nilai CNAME catatan ke nama host server Anda.

Untuk informasi selengkapnya tentang zona yang dihosting di Route 53, lihat [Zona yang dihosting](#) di Panduan Pengembang Amazon Route 53.

Gunakan penyedia DNS lainnya

Saat membuat server, Anda juga dapat menggunakan penyedia DNS selain Amazon Route 53. Jika Anda menggunakan penyedia DNS alternatif, pastikan lalu lintas dari domain Anda diarahkan ke titik akhir server Anda.

Untuk melakukannya, atur domain Anda ke nama host endpoint untuk server.

- Untuk titik akhir IPv4, nama host terlihat seperti ini di konsol:

`serverid.server.transfer.region.amazonaws.com`

- Untuk titik akhir tumpukan ganda, nama host terlihat seperti ini di konsol:

`serverid.transfer-server.region.on.aws`

Note

Jika server Anda memiliki titik akhir VPC, maka format untuk nama host berbeda dari yang dijelaskan di atas. Untuk menemukan titik akhir VPC Anda, pilih VPC di halaman detail server, lalu pilih ID titik akhir VPC di dasbor VPC. Endpoint adalah nama DNS pertama dari yang terdaftar.

Nama host khusus untuk server yang dibuat non-konsol

Saat Anda membuat server menggunakan AWS Cloud Development Kit (AWS CDK), CloudFormation, atau melalui CLI, Anda harus menambahkan tag jika Anda ingin server tersebut memiliki nama host khusus. Saat Anda membuat server Transfer Family menggunakan konsol, penandaan dilakukan secara otomatis.

Note

Anda juga perlu membuat catatan DNS untuk mengarahkan lalu lintas dari domain Anda ke titik akhir server Anda. Untuk detailnya, lihat [Bekerja dengan catatan](#) di Panduan Pengembang Amazon Route 53.

Gunakan kunci berikut untuk nama host kustom Anda:

- Tambahkan `transfer:customHostname` untuk menampilkan nama host khusus di konsol.
- Jika Anda menggunakan Route 53 sebagai penyedia DNS Anda, tambahkan `transfer:route53HostedZoneId`. Tag ini menautkan nama host kustom ke Route 53 Hosted Zone ID Anda.

Untuk menambahkan nama host khusus, keluarkan perintah CLI berikut.

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

Contoh:

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

Jika Anda menggunakan Route 53, keluarkan perintah berikut untuk menautkan nama host kustom Anda ke Route 53 Hosted Zone ID.

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

Contoh:

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

Dengan asumsi nilai sampel dari perintah sebelumnya, jalankan perintah berikut untuk melihat tag Anda:

```
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

Zona publik Anda yang dihosting, dan ID mereka tersedia di Amazon Route 53. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.

Pertimbangan Load Balancer Jaringan FTP dan FTPS

Meskipun kami menyarankan untuk menghindari Network Load Balancer di depan AWS Transfer Family server, jika implementasi FTP atau FTPS Anda memerlukan NLB atau NAT dalam rute komunikasi dari klien, ikuti rekomendasi ini:

- Untuk NLB, gunakan port 21 untuk pemeriksaan kesehatan, bukan port 8192-8200.
- Untuk AWS Transfer Family server, aktifkan dimulainya kembali sesi TLS dengan pengaturan. `TlsSessionResumptionMode = ENFORCED`

Note

Ini adalah mode yang disarankan, karena memberikan keamanan yang ditingkatkan:

- Membutuhkan klien untuk menggunakan dimulainya kembali sesi TLS untuk koneksi berikutnya.
 - Memberikan jaminan keamanan yang lebih kuat dengan memastikan parameter enkripsi yang konsisten.
 - Membantu mencegah potensi serangan downgrade.
 - Menjaga kepatuhan terhadap standar keamanan sambil mengoptimalkan kinerja.
- Jika memungkinkan, bermigrasi dari menggunakan NLB untuk memanfaatkan batas AWS Transfer Family kinerja dan koneksi sepenuhnya.

Untuk panduan tambahan tentang alternatif NLB, hubungi tim Manajemen AWS Transfer Family Produk melalui Support AWS . Untuk informasi lebih lanjut tentang meningkatkan postur keamanan Anda, lihat posting blog [Enam tips untuk meningkatkan keamanan AWS Transfer Family server Anda](#).

Panduan keamanan untuk NLB disediakan di [Hindari menempatkan NLB dan NAT di depan AWS Transfer Family server](#)

Mentransfer file melalui titik akhir server menggunakan klien

Anda mentransfer file melalui AWS Transfer Family layanan dengan menentukan operasi transfer di klien. AWS Transfer Family mendukung klien berikut:

- Kami mendukung versi 3 dari protokol SFTP.
- OpenSSH (macOS dan Linux)

 Note

Klien ini hanya berfungsi dengan server yang diaktifkan untuk Secure Shell (SSH) File Transfer Protocol (SFTP).

- WinSCP (hanya Microsoft Windows)
- Cyberduck (Windows, macOS, dan Linux)
- FileZilla (Windows, macOS, dan Linux)

Batasan berikut berlaku untuk setiap klien:

- Protokol SCP tidak didukung, karena dianggap tidak aman. Anda dapat menggunakan perintah scp OpenSSH seperti yang dijelaskan dalam [Menggunakan scp perintah](#)
- Jumlah maksimum sesi SFTP bersamaan, multipleks, per koneksi adalah 10.
- Untuk koneksi idle, nilai batas waktu adalah 1800 detik (30 menit) untuk semua protokol (). SFTP/FTP/FTPS Jika tidak ada aktivitas setelah periode ini, klien mungkin terputus. Untuk koneksi yang tidak responsif:
 - SFTP memiliki batas waktu 300 detik (5 menit) ketika klien benar-benar tidak responsif.
 - FTPS dan FTP memiliki batas waktu kurang lebih 10 menit yang tidak responsif yang ditangani oleh perpustakaan yang mendasarinya.
- Amazon S3 dan Amazon EFS (karena protokol NFSv4) memerlukan nama file untuk dikodekan. UTF-8 Menggunakan pengkodean yang berbeda dapat menyebabkan hasil yang tidak terduga. Untuk Amazon S3, lihat Pedoman [penamaan kunci objek](#).
- Untuk Protokol Transfer File melalui SSL (FTPS), hanya mode Eksplisit yang didukung. Mode implisit tidak didukung.
- Untuk File Transfer Protocol (FTP) dan FTPS, hanya mode Pasif yang didukung.
- Untuk FTP dan FTPS, hanya mode STREAM yang didukung.
- Untuk FTP dan FTPS, hanya Image/Binary mode yang didukung.
- Untuk FTP dan FTPS, TLS - PROT C (tidak dilindungi) TLS untuk koneksi data adalah default tetapi PROT C tidak didukung dalam protokol FTPS. AWS Transfer Family Jadi untuk FTPS, Anda perlu mengeluarkan PROT P agar operasi data Anda dapat diterima.
- Jika Anda menggunakan Amazon S3 untuk penyimpanan server Anda, dan jika klien Anda berisi opsi untuk menggunakan beberapa koneksi untuk satu transfer, pastikan untuk menonaktifkan opsi

tersebut. Jika tidak, unggahan file besar dapat gagal dengan cara yang tidak terduga. Perhatikan bahwa jika Anda menggunakan Amazon EFS sebagai backend penyimpanan, EFS mendukung beberapa koneksi untuk satu transfer.

Berikut ini adalah daftar perintah yang tersedia untuk FTP dan FTPS:

Perintah yang tersedia					
ABOR	PRESTASI	MLST	LULUS	RETR	BESAR
AUTENTIKASI	LANG	MKD	PASV	RMD	STOU
CDUP	DAFTAR	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	UKURAN	TIPE
EPSV	MLSD	MEMILIH	QUIT (BERHENTI)	STAT	USER

 Note

APPE tidak didukung.

Untuk SFTP, operasi berikut saat ini tidak didukung untuk pengguna yang menggunakan direktori home logis pada server yang menggunakan Amazon Elastic File System (Amazon EFS).

Perintah SFTP yang tidak didukung			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT ketika file yang diminta adalah symlink	SSH_FXP_R EALPATH ketika jalur yang diminta berisi komponen symlink

Hasilkan key pair publik-pribadi

Sebelum Anda dapat mentransfer file, Anda harus memiliki key pair publik-pribadi yang tersedia. Jika sebelumnya Anda belum membuat key pair, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

Topik

- [SFTP/FTPS/FTP Perintah yang Tersedia](#)
- [Temukan titik akhir Amazon VPC Anda](#)
- [Hindari setstat kesalahan](#)
- [Gunakan OpenSSH](#)
- [Gunakan WinSCP](#)
- [Gunakan Cyberduck](#)
- [Gunakan FileZilla](#)
- [Gunakan klien Perl](#)
- [Gunakan LFTP](#)
- [Pemrosesan unggahan pasca](#)
- [Pesan SFTP](#)

SFTP/FTPS/FTP Perintah yang Tersedia

Tabel berikut menjelaskan perintah yang tersedia untuk AWS Transfer Family, untuk protokol SFTP, FTPS, dan FTP.

Note

Tabel menyebutkan file dan direktori untuk Amazon S3, yang hanya mendukung bucket dan objek: tidak ada hierarki. Namun, Anda dapat menggunakan awalan dalam nama kunci objek untuk menyiratkan hierarki dan mengatur data Anda dengan cara yang mirip dengan folder. Perilaku ini dijelaskan dalam [Bekerja dengan metadata objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

SFTP/FTPS/FTP Perintah

Perintah	Amazon S3	Amazon EFS
cd	Didukung	Didukung
chgrp	Tidak Support	Didukung (root atau owner hanya)
chmod	Tidak didukung	Didukung (root hanya)
chmtime	Tidak didukung	Didukung
chown	Tidak Support	Didukung (root hanya)
get	Didukung	Didukung (termasuk menyelesaikan tautan simbolik)
ln -s	Tidak didukung	Didukung
ls/dir	Didukung	Didukung
mkdir	Didukung	Didukung
put	Didukung	Didukung
pwd	Didukung	Didukung
rename	Didukung hanya untuk file  Note Mengganti nama yang akan menimpa file yang ada tidak didukung.	Didukung  Note Mengganti nama yang akan menimpa file atau direktori yang ada tidak didukung.
rm	Didukung	Didukung

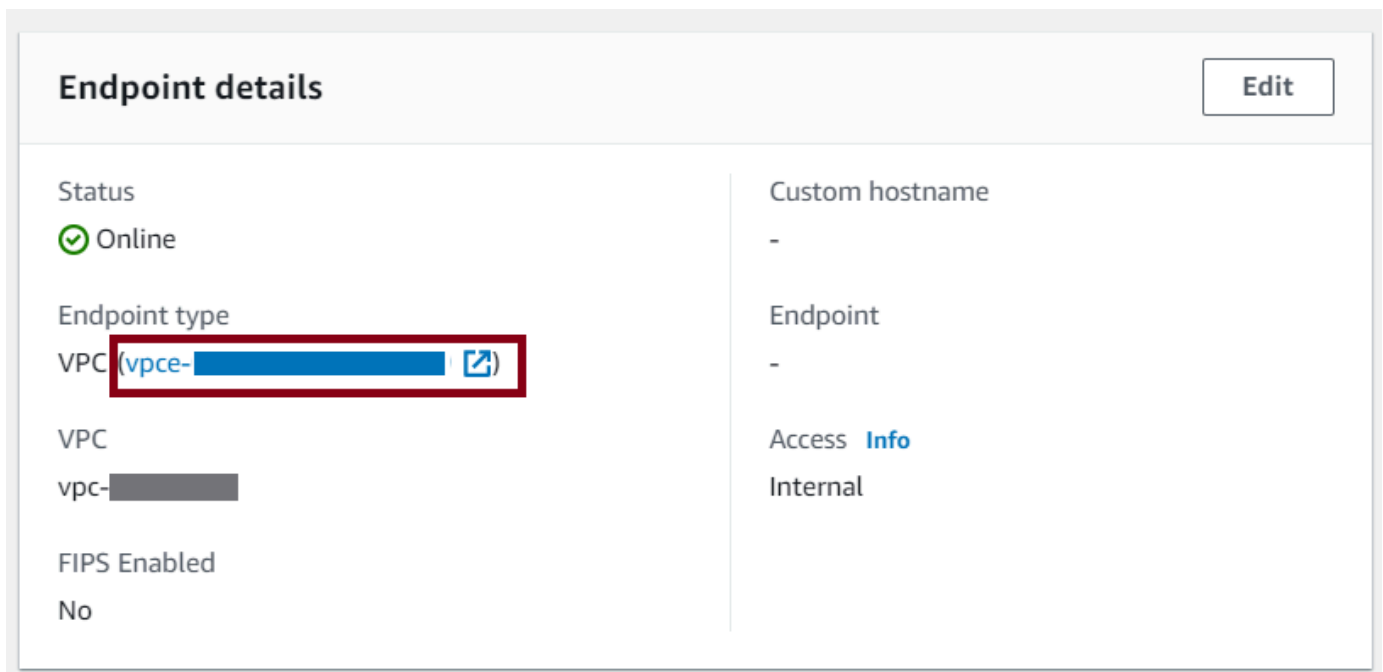
Perintah	Amazon S3	Amazon EFS
<code>rmdir</code>	Didukung (hanya direktori kosong)	Didukung
<code>version</code>	Didukung	Didukung

Temukan titik akhir Amazon VPC Anda

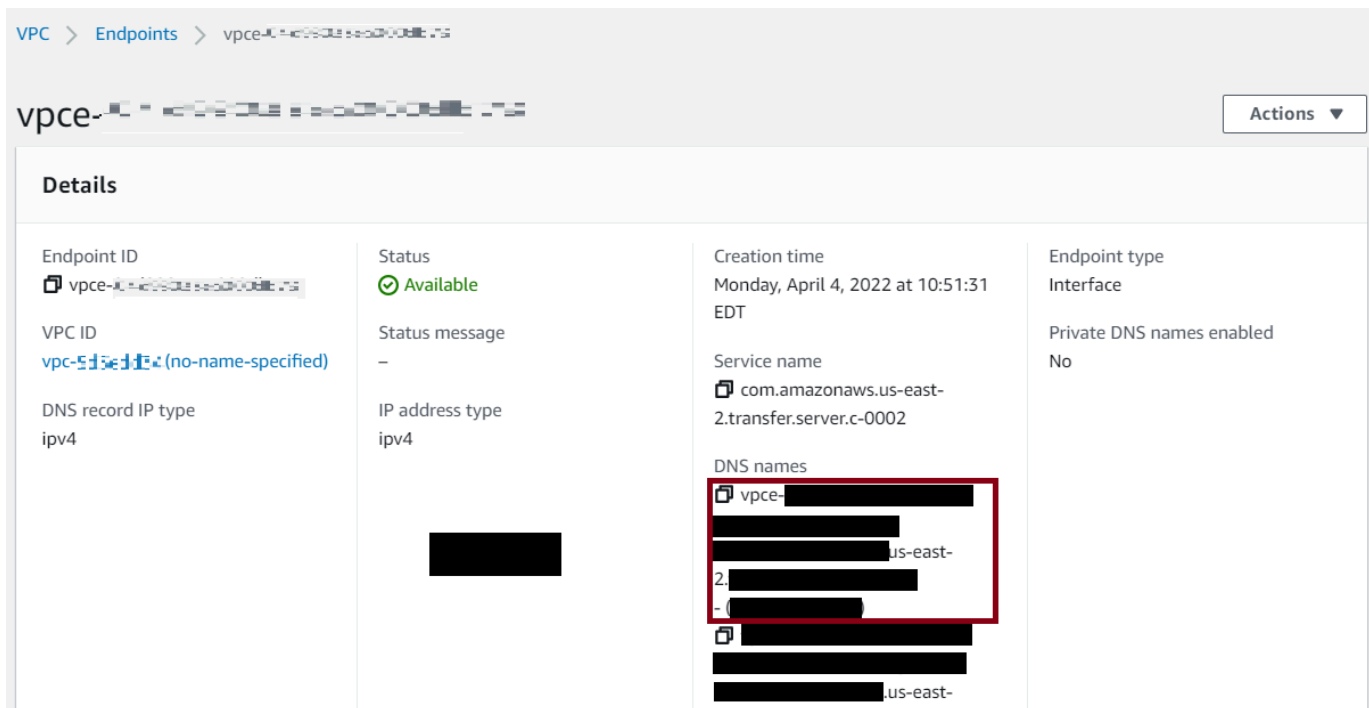
Jika tipe endpoint untuk server Transfer Family Anda adalah VPC, mengidentifikasi titik akhir yang akan digunakan untuk mentransfer file tidaklah mudah. Dalam hal ini, gunakan prosedur berikut untuk menemukan titik akhir VPC Amazon Anda.

Untuk menemukan titik akhir VPC Amazon Anda

1. Arahkan ke halaman detail server Anda.
2. Di panel Detail titik akhir, pilih VPC.



3. Di dasbor Amazon VPC, pilih ID titik akhir VPC.
4. Dalam daftar nama DNS, titik akhir server Anda adalah yang pertama terdaftar.



Hindari **setstat** kesalahan

Beberapa klien transfer file SFTP dapat mencoba mengubah atribut file jarak jauh, termasuk stempel waktu dan izin, menggunakan perintah, seperti SETSTAT saat mengunggah file. Namun, perintah ini tidak kompatibel dengan sistem penyimpanan objek, seperti Amazon S3. Karena ketidakcocokan ini, unggahan file dari klien ini dapat mengakibatkan kesalahan bahkan ketika file tersebut berhasil diunggah.

- Saat Anda memanggil UpdateServer API CreateServer atau, gunakan ProtocolDetails opsi SetStatOption untuk mengabaikan kesalahan yang dihasilkan saat klien mencoba menggunakan SETSTAT pada file yang Anda unggah ke bucket S3.
- Tetapkan nilainya ENABLE_NO_OP agar server Transfer Family mengabaikan perintah SETSTAT, dan unggah file tanpa perlu membuat perubahan apa pun pada klien SFTP Anda.
- Perhatikan bahwa meskipun SetStatOption ENABLE_NO_OP pengaturan mengabaikan kesalahan, itu menghasilkan entri CloudWatch log di Log, sehingga Anda dapat menentukan kapan klien melakukan panggilan SETSTAT.

Untuk detail API untuk opsi ini, lihat [ProtocolDetails](#).

Gunakan OpenSSH

Bagian ini berisi instruksi untuk mentransfer file dari baris perintah menggunakan OpenSSH.

Note

Klien ini hanya berfungsi dengan SFTP-enabled server.

Topik

- [Menggunakan OpenSSH](#)
- [Menggunakan scp perintah](#)

Menggunakan OpenSSH

Untuk mentransfer file AWS Transfer Family menggunakan utilitas baris perintah OpenSSH

1. Di Linux, macOS, atau Windows, buka terminal perintah.
2. Pada prompt, masukkan perintah berikut:

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

Pada perintah sebelumnya, *sftp_user* adalah nama pengguna dan *transfer-key* merupakan kunci pribadi SSH. Di sini, *service_endpoint* adalah titik akhir server seperti yang ditunjukkan di AWS Transfer Family konsol untuk server yang dipilih.

Note

Perintah ini menggunakan pengaturan yang ada di `ssh_config` file default. Kecuali Anda sebelumnya telah mengedit file ini, SFTP menggunakan port 22. Anda dapat menentukan port yang berbeda (misalnya 2222) dengan menambahkan **-P** bendera ke perintah, sebagai berikut.

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

Atau, jika Anda selalu ingin menggunakan port 2222 atau port 22000, Anda dapat memperbarui port default di file `Andassh_config`.

sftpPrompt akan muncul.

3. (Opsional) Untuk melihat direktori home pengguna, masukkan perintah berikut pada sftp prompt:

```
pwd
```

4. Untuk mengunggah file dari sistem file Anda ke server Transfer Family, gunakan put perintah. Misalnya, untuk mengunggah hello.txt (dengan asumsi bahwa file ada di direktori Anda saat ini di sistem file Anda), jalankan perintah berikut pada sftp prompt:

```
put hello.txt
```

Pesan yang mirip dengan berikut ini muncul, menunjukkan bahwa transfer file sedang berlangsung, atau selesai.

```
Uploading hello.txt to /amzn-s3-demo-bucket/home/sftp_user/hello.txt  
hello.txt 100% 127 0.1KB/s 00:00
```

Note

Setelah server Anda dibuat, diperlukan beberapa menit agar nama host endpoint server dapat diselesaikan oleh layanan DNS di lingkungan Anda.

Menggunakan **scp** perintah

Transfer Family tidak mendukung protokol SCP. Namun, Anda dapat menggunakan perintah scp OpenSSH jika Anda membutuhkan fungsi ini.

Rekomendasi untuk menggunakan SCP melalui SFTP adalah menggunakan OpenSSH versi 9.0 atau yang lebih baru. Di OpenSSH versi 9 dan yang lebih baru, scp perintah default menggunakan protokol SFTP untuk transfer file, bukan protokol SCP lama.

Important

Pastikan server Transfer Family Anda telah dikonfigurasi untuk menggunakan akses direktori yang dioptimalkan S3.

Gunakan WinSCP

Gunakan instruksi yang mengikuti untuk mentransfer file dari baris perintah menggunakan WinSCP.

Note

Jika Anda menggunakan WinSCP 5.19, Anda dapat langsung terhubung ke Amazon S3 menggunakan kredensial dan file Anda. AWS upload/download Untuk detail selengkapnya, lihat [Menghubungkan ke layanan Amazon S3](#).

Untuk mentransfer file AWS Transfer Family menggunakan WinSCP

1. Buka klien WinSCP.
2. Di kotak dialog Login, untuk protokol File, pilih protokol: SFTP atau FTP.

Jika Anda memilih FTP, untuk Enkripsi, pilih salah satu dari berikut ini:

- Tidak ada enkripsi untuk FTP
 - TLS/SSL Enkripsi eksplisit untuk FTPS
3. Untuk nama Host, masukkan endpoint server Anda. Titik akhir server terletak di halaman detail Server. Untuk informasi selengkapnya, lihat [Lihat detail server SFTP, FTPS, dan FTP](#).

Jika server Anda menggunakan titik akhir VPC, lihat. [Temukan titik akhir Amazon VPC Anda](#)

4. Untuk nomor Port, masukkan yang berikut ini:
 - **22** untuk SFTP
 - **21** untuk FTP/FTPS
5. Untuk nama Pengguna, masukkan nama untuk pengguna yang Anda buat untuk penyedia identitas spesifik Anda.

Tip: Nama pengguna harus menjadi salah satu pengguna yang Anda buat atau konfigurasi untuk penyedia identitas Anda. AWS Transfer Family menyediakan penyedia identitas berikut:

- [Bekerja dengan pengguna yang dikelola layanan](#)
- [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#)
- [Bekerja dengan penyedia identitas khusus](#)

6. Pilih **Advanced** untuk membuka kotak dialog **Advanced Site Settings**. Di bagian **SSH**, pilih **Otentikasi**.
7. Untuk file kunci pribadi, telusuri dan pilih file kunci pribadi SSH dari sistem file Anda.

Jika WinSCP menawarkan untuk mengonversi kunci pribadi SSH Anda ke format PPK, pilih **OK**.

8. Pilih **OK** untuk kembali ke kotak dialog **Login**, lalu pilih **Simpan**.
9. Dalam kotak dialog **Simpan sesi sebagai situs**, pilih **OK** untuk menyelesaikan pengaturan koneksi Anda.
10. Di kotak dialog **Login**, pilih **Tools**, lalu pilih **Preferences**.
11. Di kotak dialog **Preferensi**, untuk **Transfer**, pilih **Endurance**.

Untuk opsi **Aktifkan transfer resume/transfer ke nama file sementara untuk opsi**, pilih **Nonaktifkan**.

 Important

Jika Anda membiarkan opsi ini diaktifkan, ini meningkatkan biaya unggahan, secara substansial mengurangi kinerja unggahan. Hal ini juga dapat menyebabkan kegagalan upload file besar.

12. Untuk **Transfer**, pilih **Latar Belakang**, dan kosongkan kotak centang **Gunakan beberapa koneksi untuk transfer tunggal**.

Tip: Jika Anda membiarkan opsi ini dipilih, unggahan file besar dapat gagal dengan cara yang tidak terduga. Misalnya, unggahan multipart yang dikenakan biaya Amazon S3 dapat dibuat. Korupsi data senyap juga dapat terjadi.

13. Lakukan transfer file Anda.

Anda dapat menggunakan metode **drag-and-drop** untuk menyalin file antara target dan jendela sumber. Anda dapat menggunakan ikon bilah alat untuk mengunggah, mengunduh, menghapus, mengedit, atau memodifikasi properti file di WinSCP.

 Note

Catatan ini tidak berlaku jika Anda menggunakan Amazon EFS untuk penyimpanan. Perintah yang mencoba mengubah atribut file jarak jauh, termasuk stempel waktu, tidak kompatibel dengan sistem penyimpanan objek seperti Amazon S3. Oleh karena itu, jika Anda

menggunakan Amazon S3 untuk penyimpanan, pastikan untuk menonaktifkan pengaturan stempel waktu WinSCP (atau gunakan `SetStatOption` seperti yang dijelaskan dalam) sebelum Anda melakukan transfer file. [Hindari setstat kesalahan](#) Untuk melakukannya, di kotak dialog WinSCP Transfer settings, nonaktifkan opsi Setel izin upload dan opsi Preserve timestamp common.

Gunakan Cyberduck

Gunakan instruksi yang mengikuti untuk mentransfer file dari baris perintah menggunakan Cyberduck.

Untuk mentransfer file AWS Transfer Family menggunakan Cyberduck

1. Buka klien [Cyberduck](#).
2. Pilih Buka Koneksi.
3. Dalam kotak dialog Open Connection, pilih protokol: SFTP (SSH File Transfer Protocol), FTP-SSL (Explicit AUTH TLS), atau FTP (File Transfer Protocol).
4. Untuk Server, masukkan endpoint server Anda. Titik akhir server terletak di halaman detail Server. Untuk informasi selengkapnya, lihat [Lihat detail server SFTP, FTPS, dan FTP](#).

Jika server Anda menggunakan titik akhir VPC, lihat. [Temukan titik akhir Amazon VPC Anda](#)

5. Untuk nomor Port, masukkan yang berikut ini:
 - **22** untuk SFTP
 - **21** untuk FTP/FTPS
6. Untuk Nama Pengguna, masukkan nama untuk pengguna yang Anda buat [Mengelola pengguna untuk titik akhir server](#).
7. Jika SFTP dipilih, untuk SSH Private Key, pilih atau masukkan kunci pribadi SSH.
8. Pilih Hubungkan.
9. Lakukan transfer file Anda.

Tergantung di mana file Anda berada, lakukan salah satu hal berikut:

- Di direktori lokal Anda (sumber), pilih file yang ingin Anda transfer, dan seret dan jatuhkan ke direktori Amazon S3 (target).

- Di direktori Amazon S3 (sumber), pilih file yang ingin Anda transfer, dan seret dan jatuhkan ke direktori lokal Anda (target).

Gunakan FileZilla

Gunakan instruksi yang mengikuti untuk mentransfer file menggunakan FileZilla.

FileZilla Untuk mengatur transfer file

1. Buka FileZilla klien.
2. Pilih File, lalu pilih Site Manager.
3. Di kotak dialog Pengelola Situs, pilih Situs baru.
4. Pada tab Umum, untuk Protokol, pilih protokol: SFTP atau FTP.

Jika Anda memilih FTP, untuk Enkripsi, pilih salah satu dari berikut ini:

- Hanya gunakan FTP biasa (tidak aman) — untuk FTP
 - Gunakan FTP eksplisit melalui TLS jika tersedia - untuk FTPS
5. Untuk nama Host, masukkan protokol yang Anda gunakan, diikuti oleh endpoint server Anda. Titik akhir server terletak di halaman detail Server. Untuk informasi selengkapnya, lihat [Lihat detail server SFTP, FTPS, dan FTP](#).
- Jika Anda menggunakan SFTP, masukkan: `sftp://hostname`
 - Jika Anda menggunakan FTPS, masukkan: `ftps://hostname`

Pastikan untuk mengganti *hostname* dengan endpoint server Anda yang sebenarnya.

Jika server Anda menggunakan titik akhir VPC, lihat. [Temukan titik akhir Amazon VPC Anda](#)

6. Untuk nomor Port, masukkan yang berikut ini:
 - **22** untuk SFTP
 - **21** untuk FTP/FTPS
7. Jika SFTP dipilih, untuk Jenis Logon, pilih File kunci.

Untuk file Kunci, pilih atau masukkan kunci pribadi SSH.

8. Untuk Pengguna, masukkan nama untuk pengguna yang Anda buat [Mengelola pengguna untuk titik akhir server](#).
9. Pilih Hubungkan.
10. Lakukan transfer file Anda.

Note

Jika Anda mengganggu transfer file yang sedang berlangsung, AWS Transfer Family mungkin menulis sebagian objek di bucket Amazon S3 Anda. Jika Anda mengganggu unggahan, periksa apakah ukuran file di bucket Amazon S3 cocok dengan ukuran file objek sumber sebelum melanjutkan.

Gunakan klien Perl

Jika Anda menggunakan klien `Net::SFTP::Foreign` perl, Anda harus mengatur `queue_size` ke 1. Contoh:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

Note

[Solusi ini diperlukan untuk revisi sebelum 1.92.02. Net::SFTP::Foreign](#)

Gunakan LFTP

LFTP adalah klien FTP gratis yang memungkinkan pengguna untuk melakukan transfer file melalui antarmuka baris perintah dari sebagian besar mesin Linux.

Untuk unduhan file besar, LFTP memiliki masalah yang diketahui dengan paket yang rusak, menyebabkan transfer file gagal.

Pemrosesan unggahan pasca

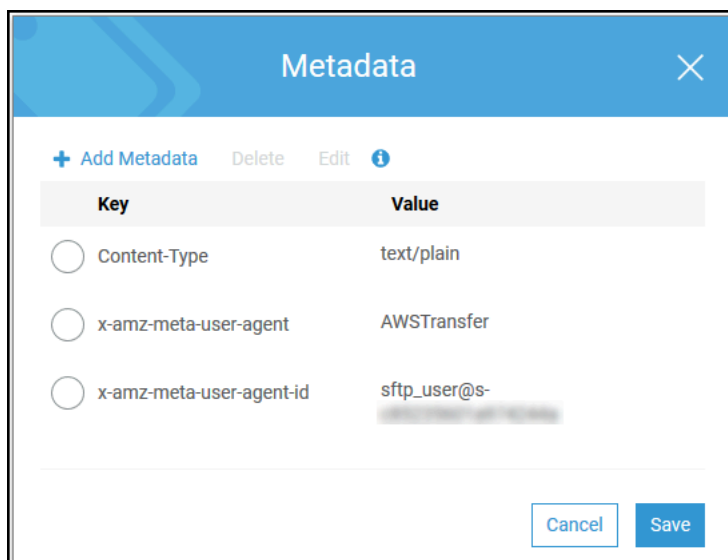
Anda dapat melihat informasi pemrosesan unggahan posting termasuk metadata objek Amazon S3 dan pemberitahuan acara.

Topik

- [Metadata objek Amazon S3](#)
- [Pemberitahuan acara Amazon S3](#)

Metadata objek Amazon S3

Sebagai bagian dari metadata objek Anda, Anda melihat kunci yang disebut `x-amz-meta-user-agent` yang nilainya `AWSTransfer` dan `x-amz-meta-user-agent-id` nilainya `username@server-id`. `username@server-id` adalah pengguna Transfer Family yang mengunggah file dan `server-id` merupakan server yang digunakan untuk mengunggah. Informasi ini dapat diakses menggunakan [HeadObject](#) operasi pada objek S3 di dalam fungsi Lambda Anda.



Pemberitahuan acara Amazon S3

Saat objek diunggah ke bucket S3 Anda menggunakan Transfer Family, `RoleSessionName` terdapat dalam bidang Peminta dalam struktur notifikasi [peristiwa S3](#) sebagai `[AWS:Role Unique Identifier]/username.sessionid@server-id`. Misalnya, berikut ini adalah konten untuk bidang Peminta sampel dari log akses S3 untuk file yang disalin ke bucket S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/  
username.sessionid@server-id
```

Di bidang Pemohon di atas, ini menunjukkan Peran IAM yang disebut `IamRoleName`. Untuk informasi selengkapnya tentang mengonfigurasi notifikasi peristiwa S3, lihat [Mengonfigurasi notifikasi peristiwa Amazon S3 di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon](#). Untuk

informasi selengkapnya tentang pengidentifikasi unik peran AWS Identity and Access Management (IAM), lihat [Pengidentifikasi unik di Panduan](#) Pengguna.AWS Identity and Access Management

Pesan SFTP

Bagian ini menjelaskan pesan sisi klien yang mungkin Anda terima selama atau setelah transfer file SFTP Anda saat menggunakan server Transfer Family. Untuk informasi lebih lanjut tentang acara SFTP apa pun, periksa log klien SFTP Anda. Anda dapat menggunakan informasi tersebut untuk memecahkan masalah kesalahan apa pun, atau meneruskan informasi tersebut ke tim jaringan Anda untuk bantuan mereka dalam mengidentifikasi masalah.

Pesan sisi klien SFTP

Aktifitas	Deskripsi
AUTH_FAILURE	Pengguna gagal otentikasi. Ini bisa berupa kegagalan apa pun dari penyedia identitas khusus atau pengguna yang dikelola layanan. Rincian dalam acara tersebut membantu memperjelas akar penyebab kegagalan.
TUTUP	Menunjukkan bahwa file atau direktori yang dibuka berhasil ditutup.
CONNECTED/DISCONNECTED	Menunjukkan keberhasilan koneksi normal dan pemutusan.
CREATE_SYMLINK	Tautan simbolis dibuat (berhasil atau tidak berhasil).
DELETE	Sebuah file telah dihapus (berhasil atau tidak berhasil).
ERROR	Kesalahan umum yang tidak terduga. Deskripsi terkait berisi informasi yang dapat membantu Anda atau administrator jaringan Anda untuk mengidentifikasi masalah tertentu.
EXIT_REASON	Dipancarkan ketika kesalahan tak terduga menyebabkan penghentian sesi SFTP Anda.

Aktifitas	Deskripsi
	Pesan yang terkait dengan peristiwa tersebut menjelaskan penyebabnya.
MKDIR	Direktori dibuat (berhasil atau tidak berhasil).
BUKA	File dibuka untuk dibaca atau ditulis (berhasil atau tidak berhasil)
PARSIAL_CLOSE	Klien terputus dari server saat file masih terbuka tanpa pesan CLOSE diterima. Transfer Family menyimpan bagian file yang diterima (yang sebenarnya bisa menjadi file lengkap) dan memancarkan acara PARTIAL_CLOSE untuk mengingatkan pelanggan tentang masalah tersebut. Integrasi alur kerja juga menerima onPartialClose acara untuk menangani file dengan tepat.
GANTI NAMA	File diganti namanya (berhasil atau tidak berhasil)
RMDIR	Direktori telah dihapus (berhasil atau tidak berhasil)

Aktifitas	Deskripsi
SETSTAT	Atribut file diubah (berhasil atau tidak berhasil).  Note Transfer Family tidak mendukung SETSTAT jika Anda menggunakan Amazon S3 untuk penyimpanan. Hindari setstat kesalahanBagian ini memberikan detail tentang cara menghindari SetStat kesalahan, dengan mematikan pengaturan. Ini menghindari Anda menerima <code>fail unsupported error</code> : sebagai gantinya, Anda menerima <code>success but do nothing</code> pesan.
TLS_RESUME_FAILURE	Server dikonfigurasi untuk menegakkan Dimulainya Kembali Sesi TLS dan klien tidak mendukungnya.

Mengelola pengguna untuk titik akhir server

Di bagian berikut, Anda dapat menemukan informasi tentang cara menambahkan pengguna yang menggunakan AWS Transfer Family, AWS Directory Service for Microsoft Active Directory atau penyedia identitas khusus.

Sebagai bagian dari properti setiap pengguna, Anda juga menyimpan kunci publik Secure Shell (SSH) pengguna tersebut. Melakukan hal itu diperlukan untuk otentikasi berbasis kunci. Kunci pribadi disimpan secara lokal di komputer pengguna Anda. Ketika pengguna Anda mengirim permintaan otentikasi ke server Anda dengan menggunakan klien, server Anda terlebih dahulu mengonfirmasi bahwa pengguna memiliki akses ke kunci pribadi SSH terkait. Server kemudian berhasil mengotentikasi pengguna.

 Note

Untuk penerapan otomatis dan pengelolaan pengguna dengan beberapa kunci SSH, lihat. [Modul Transfer Family Terraform](#)

Selain itu, Anda menentukan direktori home pengguna, atau direktori landing, dan menetapkan peran AWS Identity and Access Management (IAM) kepada pengguna. Secara opsional, Anda dapat memberikan kebijakan sesi untuk membatasi akses pengguna hanya ke direktori home bucket Amazon S3 Anda.

 Important

AWS Transfer Family memblokir nama pengguna yang panjangnya 1 atau 2 karakter dari otentikasi ke server SFTP. Selain itu, kami juga memblokir nama `root` pengguna. Alasan di balik ini adalah karena volume besar upaya login berbahaya oleh pemindai kata sandi.

Amazon EFS vs Amazon S3

Karakteristik masing-masing opsi penyimpanan:

- Untuk membatasi akses: Amazon S3 mendukung kebijakan sesi; Amazon EFS mendukung ID pengguna, grup, dan grup sekunder POSIX
- Kedua public/private kunci dukungan
- Keduanya mendukung direktori rumah
- Keduanya mendukung direktori logis

 Note

Untuk Amazon S3, sebagian besar dukungan untuk direktori logis adalah melalui API/CLI. Anda dapat menggunakan kotak centang Dibatasi di konsol untuk mengunci pengguna ke direktori home mereka, tetapi Anda tidak dapat menentukan struktur direktori virtual.

Direktori logis

Jika Anda menentukan nilai direktori logis untuk pengguna Anda, parameter yang Anda gunakan tergantung pada jenis pengguna.

- Untuk pengguna yang dikelola layanan, berikan nilai direktori logis di `HomeDirectoryMappings`
- Untuk pengguna penyedia identitas kustom, berikan nilai direktori logis di `HomeDirectoryDetails`.

AWS Transfer Family mendukung menentukan HomeDirectory nilai saat menggunakan LOGICAL HomeDirectoryType. Ini berlaku untuk pengguna yang Dikelola Layanan, akses Direktori Aktif, dan implementasi Penyedia Identitas Kustom HomeDirectoryDetails yang disediakan dalam respons.

Important

Saat menentukan HomeDirectory dengan LOGICAL HomeDirectoryType, nilainya harus dipetakan ke salah satu pemetaan direktori logis Anda. Layanan memvalidasi ini selama pembuatan dan pembaruan pengguna untuk mencegah konfigurasi yang tidak akan berfungsi.

Perilaku default

Secara default, jika dibiarkan tidak ditentukan, HomeDirectory diatur ke “/” untuk mode LOGICAL. Perilaku ini tidak berubah dan tetap kompatibel dengan definisi pengguna yang ada.

- Pastikan untuk memetakan Anda HomeDirectory ke Entri dan bukan Target. Untuk detail selengkapnya, lihat [Aturan untuk menggunakan direktori logis](#).
- Untuk detail tentang bagaimana direktori virtual terstruktur lihat [Struktur direktori virtual](#).

Pertimbangan Penyedia Identitas Kustom

Saat menggunakan Penyedia Identitas Kustom, Anda sekarang dapat menentukan respons saat menggunakan LOGICAL HomeDirectoryType. HomeDirectory Panggilan TestIdentityProvider API akan menghasilkan hasil yang benar ketika IDP Kustom menentukan mode LOGICAL. HomeDirectory

Contoh respon IDP kustom dengan HomeDirectory dan LOGICAL HomeDirectoryType:

```
{  
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",  
  "HomeDirectoryType": "LOGICAL",  
  "HomeDirectory": "/marketing",  
  "HomeDirectoryDetails": "[{\"Entry\":\"\\\\\"/\", \"Target\":\"\\\\\"bucket/home\"},{\"Entry\":\"\\\\\"/marketing\", \"Target\":\"\\\\\"marketing-bucket/campaigns\"}]"]"  
}
```

Kuota grup Direktori Aktif

AWS Transfer Family memiliki batas default 100 grup Active Directory per server. Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Batas ini berlaku untuk server yang menggunakan penyedia identitas berikut:

- AWS Directory Service untuk Microsoft Active Directory
- AWS Directory Service untuk Entra ID Domain Services

Jika Anda perlu meminta peningkatan batas layanan, lihat [Layanan AWS kuota](#) di. Referensi Umum AWS Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Untuk informasi pemecahan masalah yang terkait dengan batas grup Active Directory, lihat. [Batas grup Active Directory terlampaui](#)

Topik

- [Bekerja dengan pengguna yang dikelola layanan](#)
- [Bekerja dengan penyedia identitas khusus](#)
- [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#)
- [Menggunakan AWS Directory Service untuk Entra ID Domain Services](#)

Bekerja dengan pengguna yang dikelola layanan

Anda dapat menambahkan pengguna yang dikelola layanan Amazon S3 atau Amazon EFS ke server Anda, tergantung pada pengaturan Domain server. Untuk informasi selengkapnya, lihat [Mengonfigurasi titik akhir server SFTP, FTPS, atau FTP](#).

Jika Anda menggunakan tipe identitas yang dikelola layanan, Anda menambahkan pengguna ke server yang diaktifkan protokol transfer file Anda. Ketika Anda melakukannya, setiap nama pengguna harus unik di server Anda.

Untuk menambahkan pengguna yang dikelola layanan secara terprogram, lihat [contoh](#) untuk API. [CreateUser](#)

Note

Untuk pengguna yang dikelola layanan ada batas 2.000 entri direktori logis. Untuk informasi tentang menggunakan direktori logis, lihat [Menggunakan direktori logis untuk menyederhanakan struktur direktori Transfer Family Anda](#).

Topik

- [Menambahkan pengguna yang dikelola layanan Amazon S3](#)
- [Menambahkan pengguna yang dikelola layanan Amazon EFS](#)
- [Mengelola pengguna yang dikelola layanan](#)

Menambahkan pengguna yang dikelola layanan Amazon S3

Note

Jika Anda ingin mengonfigurasi bucket Amazon S3 lintas akun, ikuti langkah-langkah yang disebutkan dalam artikel Pusat Pengetahuan ini: [Bagaimana cara mengonfigurasi AWS Transfer Family server saya untuk menggunakan bucket Amazon Simple Storage Service yang ada di akun lain? AWS](#).

Untuk menambahkan pengguna yang dikelola layanan Amazon S3 ke server Anda

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>, lalu pilih Server dari panel navigasi.
2. Pada halaman Server, pilih kotak centang server yang ingin Anda tambahkan pengguna.
3. Pilih Tambahkan pengguna.
4. Di bagian Konfigurasi pengguna, untuk Nama Pengguna, masukkan nama pengguna. Nama pengguna ini harus minimal 3 dan maksimal 100 karakter. Anda dapat menggunakan karakter berikut dalam nama pengguna: a—z, 0—9 A-Z, garis bawah '_', tanda hubung '-', titik '.' dan di tanda '@'. Nama pengguna tidak dapat dimulai dengan tanda hubung '-', titik '.' atau di tanda '@'.
5. Untuk Access, pilih peran IAM yang sebelumnya Anda buat yang menyediakan akses ke bucket Amazon S3 Anda.

Anda membuat peran IAM ini menggunakan prosedur di [Buat peran dan kebijakan IAM](#). Peran IAM tersebut mencakup kebijakan IAM yang menyediakan akses ke bucket Amazon S3 Anda. Ini juga mencakup hubungan kepercayaan dengan AWS Transfer Family layanan, yang didefinisikan dalam kebijakan IAM lain. Jika Anda memerlukan kontrol akses berbutir halus untuk pengguna Anda, lihat [Tingkatkan kontrol akses data dengan dan posting blog Amazon AWS Transfer Family S3](#).

6. (Opsional) Untuk Kebijakan, pilih salah satu dari berikut ini:
 - Tidak ada
 - Kebijakan yang ada
 - Pilih kebijakan dari IAM: memungkinkan Anda memilih kebijakan sesi yang ada. Pilih Lihat untuk melihat objek JSON yang berisi detail kebijakan.
 - Auto-generate kebijakan berdasarkan folder beranda: menghasilkan kebijakan sesi untuk Anda. Pilih Lihat untuk melihat objek JSON yang berisi detail kebijakan.

 Note

Jika Anda memilih Auto-generate kebijakan berdasarkan folder beranda, jangan pilih Dibatasi untuk pengguna ini.

Untuk mempelajari lebih lanjut tentang kebijakan sesi, lihat [Buat peran dan kebijakan IAM](#), [Membuat kebijakan sesi untuk bucket Amazon S3](#), atau [Pendekatan manajemen izin dinamis](#).

7. Untuk direktori Home, pilih bucket Amazon S3 untuk menyimpan data yang akan ditransfer. AWS Transfer Family Masukkan jalur ke home direktori tempat pengguna Anda mendarat saat mereka masuk menggunakan klien mereka.

Jika parameter ini kosong, root direktori bucket Amazon S3 Anda akan digunakan. Dalam hal ini, pastikan bahwa peran IAM Anda menyediakan akses ke root direktori ini.

 Note

Sebaiknya pilih jalur direktori yang berisi nama pengguna pengguna, yang memungkinkan Anda menggunakan kebijakan sesi secara efektif. Kebijakan sesi membatasi akses pengguna di bucket Amazon S3 ke direktori pengguna tersebut. home

8. (Opsional) Untuk Dibatasi, pilih kotak centang sehingga pengguna Anda tidak dapat mengakses apa pun di luar folder itu dan tidak dapat melihat keranjang Amazon S3 atau nama folder.

 Note

Menugaskan pengguna direktori home dan membatasi pengguna ke direktori home itu harus cukup untuk mengunci akses pengguna ke folder yang ditunjuk. Jika Anda perlu menerapkan kontrol lebih lanjut, gunakan kebijakan sesi.

Jika Anda memilih Dibatasi untuk pengguna ini, Anda tidak dapat memilih Auto-generate kebijakan berdasarkan folder beranda, karena folder beranda bukan nilai yang ditentukan untuk pengguna Terbatas.

9. Untuk kunci publik SSH, masukkan bagian kunci SSH publik dari key pair SSH.

Kunci Anda divalidasi oleh layanan sebelum Anda dapat menambahkan pengguna baru Anda.

 Note

Untuk petunjuk tentang cara membuat key pair SSH, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

10. (Opsional) Untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, dan pilih Tambahkan tag.
11. Pilih Tambah untuk menambahkan pengguna baru Anda ke server yang Anda pilih.

Pengguna baru muncul di bagian Pengguna pada halaman detail Server.

Langkah selanjutnya — Untuk langkah selanjutnya, lanjutkan ke [Mentransfer file melalui titik akhir server menggunakan klien](#).

Menambahkan pengguna yang dikelola layanan Amazon EFS

Amazon EFS menggunakan model izin file Portable Operating System Interface (POSIX) untuk mewakili kepemilikan file.

- Untuk detail selengkapnya tentang kepemilikan file Amazon EFS, lihat [Kepemilikan file Amazon EFS](#).
- Untuk detail selengkapnya tentang menyiapkan direktori untuk pengguna EFS Anda, lihat [Menyiapkan pengguna Amazon EFS untuk Transfer Family](#).

Untuk menambahkan pengguna yang dikelola layanan Amazon EFS ke server Anda

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>, lalu pilih Server dari panel navigasi.
2. Pada halaman Server, pilih server Amazon EFS yang ingin Anda tambahkan pengguna.
3. Pilih Tambah pengguna untuk menampilkan halaman Tambah pengguna.
4. Di bagian Konfigurasi pengguna, gunakan pengaturan berikut.
 - a. Nama pengguna, harus minimal 3 dan maksimal 100 karakter. Anda dapat menggunakan karakter berikut dalam nama pengguna: a—z,, 0—9 A-Z, garis bawah '_', tanda hubung '-', periode '.', dan pada tanda "@". Nama pengguna tidak dapat dimulai dengan tanda hubung '-', titik '.', atau pada tanda "@".
 - b. Untuk User ID dan Group ID, perhatikan hal berikut:
 - Untuk pengguna pertama yang Anda buat, kami sarankan Anda memasukkan nilai 0 untuk ID Grup dan ID Pengguna. Ini memberikan hak administrator pengguna untuk Amazon EFS.

- Untuk pengguna tambahan, masukkan ID pengguna POSIX dan ID grup pengguna. ID ini digunakan untuk semua operasi Amazon Elastic File System yang dilakukan oleh pengguna.
 - Untuk ID Pengguna dan ID Grup, jangan gunakan angka nol di depan. Misalnya, dapat **12345** diterima, **012345** tidak.
- c. (Opsional) Untuk ID Grup Sekunder, masukkan satu atau lebih ID grup POSIX tambahan untuk setiap pengguna, dipisahkan dengan koma.
- d. Untuk Access, pilih peran IAM yang:
- Memberikan pengguna akses hanya ke sumber daya Amazon EFS (sistem file) yang Anda ingin mereka akses.
 - Mendefinisikan operasi sistem file mana yang dapat dan tidak dapat dilakukan oleh pengguna.

Kami menyarankan Anda menggunakan peran IAM untuk pemilihan sistem file Amazon EFS dengan akses mount dan read/write izin. Misalnya, kombinasi dari dua kebijakan AWS terkelola berikut, meskipun cukup permisif, memberikan izin yang diperlukan untuk pengguna Anda:

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

Untuk informasi selengkapnya, lihat [AWS Transfer Family dukungan posting blog untuk Amazon Elastic File System](#).

- e. Untuk direktori Home, lakukan hal berikut:
- Pilih sistem file Amazon EFS yang ingin Anda gunakan untuk menyimpan data yang akan ditransfer AWS Transfer Family.
 - Putuskan apakah akan mengatur direktori home ke Restricted. Menyetel direktori home ke Restricted memiliki efek berikut:
 - Pengguna Amazon EFS tidak dapat mengakses file atau direktori apa pun di luar folder itu.
 - Pengguna Amazon EFS tidak dapat melihat nama sistem file Amazon EFS (fs-xxxxxxx).

 Note

Saat Anda memilih opsi Dibatasi, symlink tidak dapat diselesaikan untuk pengguna Amazon EFS.

- (Opsional) Masukkan jalur ke direktori home yang Anda inginkan agar pengguna masuk saat mereka masuk menggunakan klien mereka.

Jika Anda tidak menentukan direktori home, direktori root sistem file Amazon EFS Anda akan digunakan. Dalam hal ini, pastikan bahwa peran IAM Anda menyediakan akses ke direktori root ini.

5. Untuk kunci publik SSH, masukkan bagian kunci SSH publik dari key pair SSH.

Kunci Anda divalidasi oleh layanan sebelum Anda dapat menambahkan pengguna baru Anda.

 Note

Untuk petunjuk tentang cara membuat key pair SSH, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

6. (Opsional) Masukkan tag apa pun untuk pengguna. Untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci, dan pilih Tambah tag.
7. Pilih Tambah untuk menambahkan pengguna baru Anda ke server yang Anda pilih.

Pengguna baru muncul di bagian Pengguna pada halaman detail Server.

Masalah yang mungkin Anda temui saat pertama kali SFTP ke server Transfer Family Anda:

- Jika Anda menjalankan `sftp` perintah dan prompt tidak muncul, Anda mungkin menemukan pesan berikut:

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

Dalam hal ini, Anda harus meningkatkan izin kebijakan untuk peran pengguna Anda. Anda dapat menambahkan kebijakan AWS terkelola, seperti `AmazonElasticFileSystemClientFullAccess`.

- Jika Anda memasukkan `pwd` pada `sftp` prompt untuk melihat direktori home pengguna, Anda mungkin melihat pesan berikut, di mana ***USER-HOME-DIRECTORY*** direktori home untuk pengguna SFTP:

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

Dalam hal ini, Anda harus dapat menavigasi ke direktori induk (`cd ..`), dan membuat direktori home pengguna (`mkdir username`).

Langkah selanjutnya — Untuk langkah selanjutnya, lanjutkan ke [Mentransfer file melalui titik akhir server menggunakan klien](#).

Mengelola pengguna yang dikelola layanan

Di bagian ini, Anda dapat menemukan informasi tentang cara melihat daftar pengguna, cara mengedit detail pengguna, dan cara menambahkan kunci publik SSH.

- [Melihat daftar pengguna](#)
- [Melihat atau mengedit detail pengguna](#)
- [Menghapus pengguna](#)
- [Tambahkan kunci publik SSH](#)
- [Hapus kunci publik SSH](#)

Untuk menemukan daftar pengguna Anda

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Pilih Server dari panel navigasi untuk menampilkan halaman Server.
3. Pilih pengenal di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, lihat daftar pengguna.

Untuk melihat atau mengedit detail pengguna

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Pilih Server dari panel navigasi untuk menampilkan halaman Server.
3. Pilih pengenal di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, pilih nama pengguna untuk melihat halaman Detail pengguna.

Anda dapat mengubah properti pengguna di halaman ini dengan memilih Edit.

5. Pada halaman Detail pengguna, pilih Edit di samping Konfigurasi pengguna.

Edit configuration

User configuration

Access [Info](#)
User's IAM role for Amazon S3 access

Admin ▼

Policy [Info](#)
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

[View](#)

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted [Info](#)

Cancel Save

6. Pada halaman Edit konfigurasi, untuk Access, pilih peran IAM yang sebelumnya Anda buat yang menyediakan akses ke bucket Amazon S3 Anda.

Anda membuat peran IAM ini menggunakan prosedur di [Buat peran dan kebijakan IAM](#). Peran IAM tersebut mencakup kebijakan IAM yang menyediakan akses ke bucket Amazon S3 Anda. Ini juga mencakup hubungan kepercayaan dengan AWS Transfer Family layanan, yang didefinisikan dalam kebijakan IAM lain.

7. (Opsional) Untuk Kebijakan, pilih salah satu dari berikut ini:

- Tidak ada
- Kebijakan yang ada
- Pilih kebijakan dari IAM untuk memilih kebijakan yang ada. Pilih Lihat untuk melihat objek JSON yang berisi detail kebijakan.

Untuk mempelajari lebih lanjut tentang kebijakan sesi, lihat [Buat peran dan kebijakan IAM](#). Untuk mempelajari selengkapnya tentang membuat kebijakan sesi, lihat [Membuat kebijakan sesi untuk bucket Amazon S3](#).

8. Untuk direktori Home, pilih bucket Amazon S3 untuk menyimpan data yang akan ditransfer. AWS Transfer Family Masukkan jalur ke home direktori tempat pengguna Anda mendarat saat mereka masuk menggunakan klien mereka.

Jika Anda membiarkan parameter ini kosong, root direktori bucket Amazon S3 Anda akan digunakan. Dalam hal ini, pastikan bahwa peran IAM Anda menyediakan akses ke root direktori ini.

 Note

Sebaiknya pilih jalur direktori yang berisi nama pengguna pengguna, yang memungkinkan Anda menggunakan kebijakan sesi secara efektif. Kebijakan sesi membatasi akses pengguna di bucket Amazon S3 ke direktori pengguna tersebut. home

9. (Opsional) Untuk Dibatasi, pilih kotak centang sehingga pengguna Anda tidak dapat mengakses apa pun di luar folder itu dan tidak dapat melihat keranjang Amazon S3 atau nama folder.

 Note

Saat menugaskan pengguna direktori home dan membatasi pengguna ke direktori home itu, ini harus cukup untuk mengunci akses pengguna ke folder yang ditunjuk. Gunakan kebijakan sesi saat Anda perlu menerapkan kontrol lebih lanjut.

10. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menghapus klaster

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Pilih Server dari panel navigasi untuk menampilkan halaman Server.
3. Pilih pengenalan di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, pilih nama pengguna untuk melihat halaman Detail pengguna.
5. Pada halaman Detail pengguna, pilih Hapus di sebelah kanan nama pengguna.

6. Di kotak dialog konfirmasi yang muncul, masukkan kata **delete**, lalu pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus pengguna.

Pengguna dihapus dari daftar pengguna.

Untuk menambahkan kunci publik SSH untuk pengguna

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih pengenalan di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, pilih nama pengguna untuk melihat halaman Detail pengguna.
5. Pilih Tambahkan kunci publik SSH untuk menambahkan kunci publik SSH baru ke pengguna.

 Note

Kunci SSH hanya digunakan oleh server yang diaktifkan untuk Secure Shell (SSH) File Transfer Protocol (SFTP). Untuk informasi tentang cara membuat key pair SSH, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

6. Untuk kunci publik SSH, masukkan bagian kunci publik SSH dari SSH key pair.

Kunci Anda divalidasi oleh layanan sebelum Anda dapat menambahkan pengguna baru Anda. Format kunci SSH adalah `ssh-rsa string`. Untuk menghasilkan key pair SSH, lihat [Buat kunci SSH untuk pengguna yang dikelola layanan](#).

7. Pilih Tambah kunci.

Untuk menghapus kunci publik SSH untuk pengguna

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih pengenalan di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, pilih nama pengguna untuk melihat halaman Detail pengguna.
5. Untuk menghapus kunci publik, pilih kotak centang kunci SSH dan pilih Hapus.

Bekerja dengan penyedia identitas khusus

AWS Transfer Family menawarkan beberapa opsi untuk penyedia identitas khusus untuk mengautentikasi dan mengotorisasi pengguna untuk transfer file yang aman. Berikut adalah pendekatan utama:

- [Solusi penyedia identitas khusus](#)—Topik ini menjelaskan solusi penyedia identitas kustom Transfer Family, menggunakan toolkit yang dihosting. GitHub

Note

Untuk sebagian besar kasus penggunaan, ini adalah opsi yang disarankan. Secara khusus, jika Anda perlu mendukung lebih dari 100 grup Active Directory, solusi penyedia identitas kustom menawarkan alternatif yang dapat diskalakan tanpa batasan grup. Solusi ini dijelaskan dalam posting blog, [Sederhanakan otentikasi Active Directory dengan penyedia identitas khusus](#) untuk AWS Transfer Family

- [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#)—Topik ini menjelaskan cara menggunakan AWS Lambda fungsi untuk mendukung metode Amazon API Gateway.

Anda dapat menyediakan antarmuka RESTful dengan satu metode Amazon API Gateway. Transfer Family memanggil metode ini untuk terhubung ke penyedia identitas Anda, yang mengautentikasi dan memberi wewenang kepada pengguna Anda untuk mengakses Amazon S3 atau Amazon EFS. Gunakan opsi ini jika Anda memerlukan RESTful API untuk mengintegrasikan penyedia identitas Anda atau jika Anda ingin menggunakannya untuk memanfaatkan kemampuannya AWS WAF untuk permintaan pemblokiran geografis atau pembatasan laju. Lihat perinciannya di [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#).

- [Pendekatan manajemen izin dinamis](#)—Topik ini menjelaskan pendekatan untuk mengelola izin pengguna secara dinamis menggunakan kebijakan sesi.

Untuk mengautentikasi pengguna, Anda dapat menggunakan penyedia identitas yang ada dengan AWS Transfer Family. Anda mengintegrasikan penyedia identitas Anda menggunakan AWS Lambda fungsi, yang mengautentikasi dan memberi wewenang kepada pengguna Anda untuk mengakses Amazon S3 atau Amazon Elastic File System (Amazon EFS). Lihat perinciannya di [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#). Anda juga dapat mengakses CloudWatch grafik untuk metrik seperti jumlah file dan byte yang ditransfer di AWS

Transfer Family Management Console, memberi Anda satu panel kaca untuk memantau transfer file menggunakan dasbor terpusat.

- Transfer Family menyediakan posting blog dan lokakarya yang memandu Anda membangun solusi transfer file. Solusi ini memanfaatkan AWS Transfer Family SFTP/FTPS endpoint terkelola dan Amazon Cognito dan DynamoDB untuk manajemen pengguna.

Posting blog tersedia di [Menggunakan Amazon Cognito sebagai penyedia identitas dengan AWS Transfer Family dan Amazon S3](#). Anda dapat melihat detail untuk lokakarya [di sini](#).

Note

Untuk penyedia identitas khusus, nama pengguna harus minimal 3 dan maksimal 100 karakter. Anda dapat menggunakan karakter berikut dalam nama pengguna: a—z,, 0—9 A-Z, garis bawah '_', tanda hubung '-', titik '.' dan di tanda '@'. Nama pengguna tidak dapat dimulai dengan tanda hubung '-', titik '.' atau di tanda '@'.

Saat menerapkan penyedia identitas khusus, pertimbangkan praktik terbaik berikut:

- Terapkan solusi di wilayah yang sama dengan Akun AWS server Transfer Family Anda.
- Menerapkan prinsip hak istimewa paling sedikit saat mengonfigurasi peran dan kebijakan IAM.
- Gunakan fitur seperti daftar izin IP dan pencatatan standar untuk keamanan yang ditingkatkan.
- Uji penyedia identitas kustom Anda secara menyeluruh di lingkungan non-produksi sebelum penerapan.

Topik

- [Solusi penyedia identitas khusus](#)
- [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#)
- [Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda](#)
- [Menggunakan beberapa metode otentikasi](#)
- [Dukungan IPv6 untuk penyedia identitas khusus](#)

Solusi penyedia identitas khusus

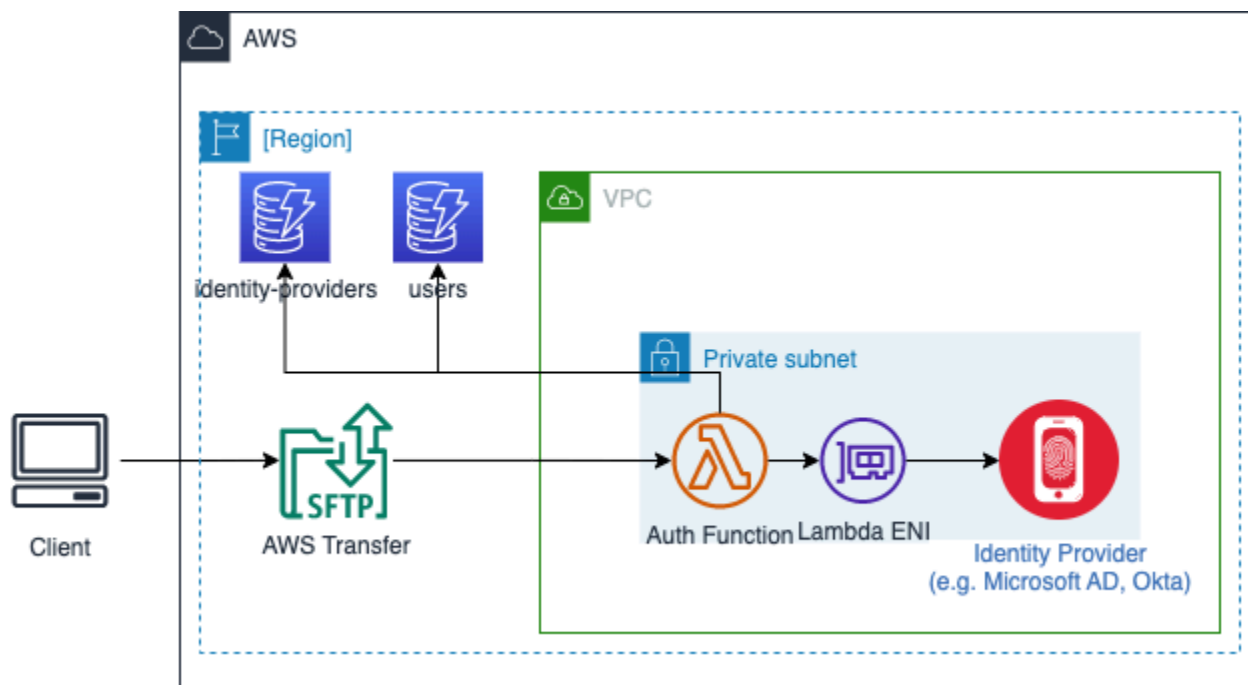
Solusi penyedia identitas AWS Transfer Family kustom adalah solusi penyedia identitas kustom modular yang memecahkan banyak kasus penggunaan otentikasi dan otorisasi umum yang dimiliki perusahaan saat menerapkan layanan. Solusi ini memberikan fondasi yang dapat digunakan kembali untuk menerapkan penyedia identitas khusus dengan konfigurasi sesi per pengguna terperinci dan memisahkan logika otentikasi dan otorisasi, menawarkan fondasi yang fleksibel dan mudah dirawat untuk berbagai kasus penggunaan.

Dengan solusi penyedia identitas AWS Transfer Family khusus, Anda dapat mengatasi kasus penggunaan otentikasi dan otorisasi perusahaan umum. Solusi modular ini menawarkan:

- Fondasi yang dapat digunakan kembali untuk menerapkan penyedia identitas khusus
- Konfigurasi sesi per pengguna granular
- Otentikasi terpisah dan logika otorisasi

Detail implementasi untuk toolkit identitas kustom

Solusinya menyediakan basis yang fleksibel dan dapat dipelihara untuk berbagai kasus penggunaan. Untuk memulai, tinjau toolkit di <https://github.com/aws-samples/toolkit-for-aws-transfer-family>, lalu ikuti petunjuk penerapan di bagian [Memulai](#).



 Note

Jika sebelumnya Anda telah menggunakan templat dan contoh penyedia identitas kustom, pertimbangkan untuk mengadopsi solusi ini sebagai gantinya. Ke depan, modul khusus penyedia akan menstandarisasi solusi ini. Pemeliharaan berkelanjutan dan peningkatan fitur akan diterapkan pada solusi ini.

Solusi ini berisi pola standar untuk menerapkan penyedia kustom yang memperhitungkan detail termasuk pencatatan dan tempat menyimpan metadata sesi tambahan yang diperlukan AWS Transfer Family, seperti parameter. `HomeDirectoryDetails` Solusi ini memberikan fondasi yang dapat digunakan kembali untuk menerapkan penyedia identitas kustom dengan konfigurasi sesi per pengguna granular, dan memisahkan logika otentikasi penyedia identitas dari logika yang dapat digunakan kembali yang membangun konfigurasi yang dikembalikan ke Transfer Family untuk menyelesaikan otentikasi dan menetapkan pengaturan untuk sesi tersebut.

Kode dan sumber daya pendukung untuk solusi ini tersedia di <https://github.com/aws-samples/toolkit-for-aws-transfer-family>.

Toolkit berisi fitur-fitur berikut:

- [AWS Serverless Application Model](#) Template yang menyediakan sumber daya yang dibutuhkan. Secara opsional, terapkan dan konfigurasi Amazon API Gateway untuk digabungkan AWS WAF, seperti yang dijelaskan dalam posting blog [Mengamankan AWS Transfer Family dengan Firewall Aplikasi AWS Web dan Amazon API Gateway](#).
- Skema [Amazon DynamoDB](#) untuk menyimpan metadata konfigurasi tentang penyedia identitas, termasuk setelan sesi pengguna seperti, dan. `HomeDirectoryDetails Role Policy`
- Pendekatan modular yang memungkinkan Anda menambahkan penyedia identitas baru ke solusi di masa depan, sebagai modul.
- Pengambilan atribut: Secara opsional mengambil peran IAM dan atribut Profil POSIX (UID dan GID) dari penyedia identitas yang didukung, termasuk AD, LDAP, dan Okta.
- Support untuk beberapa penyedia identitas yang terhubung ke satu server Transfer Family dan beberapa server Transfer Family menggunakan penerapan solusi yang sama.
- Built-in Pemeriksaan daftar ijin IP seperti IP mengizinkan daftar yang secara opsional dapat dikonfigurasi berdasarkan penyedia per-pengguna atau per-identitas.
- Pencatatan terperinci dengan tingkat log yang dapat dikonfigurasi dan dukungan penelusuran untuk membantu pemecahan masalah.

Sebelum Anda mulai menerapkan solusi penyedia identitas kustom, Anda harus memiliki AWS sumber daya berikut.

- Amazon Virtual Private Cloud (VPC) dengan subnet pribadi, dengan konektivitas internet melalui gateway NAT atau titik akhir gateway DynamoDB.
- Izin IAM yang sesuai untuk melakukan tugas-tugas berikut:
 - Menyebarkan `custom-idp.yaml` CloudFormation template,
 - Buat AWS CodePipeline proyek
 - Buat AWS CodeBuild proyek
 - Buat peran dan kebijakan IAM

Important

Anda harus menerapkan solusi yang sama Akun AWS dan Wilayah AWS yang berisi server Transfer Family target Anda.

Penyedia identitas yang didukung

Daftar berikut berisi detail untuk penyedia identitas yang didukung untuk solusi penyedia identitas kustom.

Penyedia	Alur kata sandi	Arus kunci publik	Multi-factor	Pengambilan atribut	Detail
Direktori Aktif dan LDAP	Ya	Ya	Tidak	Ya	Verifikasi pengguna dapat dilakukan sebagai bagian dari alur otentikasi kunci publik.
Argon2 (hash lokal)	Ya	Tidak	Tidak	Tidak	Hash Argon2 disimpan dalam

Penyedia	Alur kata sandi	Arus kunci publik	Multi-factor	Pengambilan atribut	Detail
					catatan pengguna untuk kasus penggunaan otentikasi berbasis kata sandi 'lokal'.
Amazon Cognito	Ya	Tidak	Ya*	Tidak	Time-based One-Time Hanya otentikasi multi-faktor berbasis kata sandi (TOTP). * SMS-based MFA tidak didukung.
Entra ID (sebelumnya Azure AD)	Ya	Tidak	Tidak	Tidak	
Okta	Ya	Ya	Ya*	Ya	TOTP-based Hanya MFA.
Kunci publik	Tidak	Ya	Tidak	Tidak	Kunci publik disimpan dalam catatan pengguna di DynamoDB.

Penyedia	Alur kata sandi	Arus kunci publik	Multi-factor	Pengambilan atribut	Detail
Secrets Manager	Ya	Ya	Tidak	Tidak	

Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda

Topik ini menjelaskan cara membuat AWS Lambda fungsi yang terhubung ke penyedia identitas kustom Anda. Anda dapat menggunakan penyedia identitas kustom apa pun, seperti Okta, Secrets Manager OneLogin, atau penyimpanan data khusus yang menyertakan logika otorisasi dan autentikasi.

Untuk sebagian besar kasus penggunaan, cara yang disarankan untuk mengonfigurasi penyedia identitas khusus adalah dengan menggunakan [Solusi penyedia identitas khusus](#).

Note

Sebelum membuat server Transfer Family yang menggunakan Lambda sebagai penyedia identitas, Anda harus membuat fungsinya. Untuk contoh fungsi Lambda, lihat [Contoh fungsi Lambda](#) Atau, Anda dapat menerapkan CloudFormation tumpukan yang menggunakan salah satu [Template fungsi Lambda](#) Selain itu, pastikan fungsi Lambda Anda menggunakan kebijakan berbasis sumber daya yang mempercayai Transfer Family. Untuk contoh kebijakan, lihat [Kebijakan berbasis sumber daya Lambda](#).

1. Buka [konsol AWS Transfer Family](#).
2. Pilih Buat server untuk membuka halaman Buat server. Untuk Pilih penyedia identitas, pilih Penyedia Identitas Kustom, seperti yang ditunjukkan pada gambar berikut.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel

Previous

Next

Note

Pilihan metode otentikasi hanya tersedia jika Anda mengaktifkan SFTP sebagai salah satu protokol untuk server Transfer Family Anda.

3. Pastikan nilai default, Gunakan AWS Lambda untuk menghubungkan penyedia identitas Anda, dipilih.
4. Untuk AWS Lambda fungsi, pilih nama fungsi Lambda Anda.

5. Isi kotak yang tersisa, lalu pilih Buat server. Untuk detail tentang langkah-langkah yang tersisa untuk membuat server, lihat [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#).

Kebijakan berbasis sumber daya Lambda

Anda harus memiliki kebijakan yang mereferensikan server Transfer Family dan Lambda ARN. Misalnya, Anda dapat menggunakan kebijakan berikut dengan fungsi Lambda yang terhubung ke penyedia identitas Anda. Kebijakan ini lolos dari JSON sebagai string.

```
"Policy":
{"Version\":\"2012-10-17\",
\Id\":\"default\",
\Statement\":[
  {\Sid\":\"AllowTransferInvocation\",
   \Effect\":\"Allow\",
   \Principal\":{\"Service\":\"transfer.amazonaws.com\"},
   \Action\":\"lambda:InvokeFunction\",
   \Resource\":\"arn:aws:lambda:region:123456789012:function:my-lambda-auth-function\",
   \Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
\"arn:aws:transfer:region:123456789012:server/server-id\"}}}
]}
```

Note

Dalam contoh kebijakan di atas, ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

Struktur pesan peristiwa

Struktur pesan acara dari server SFTP yang dikirim ke fungsi Lambda otorisasi untuk IDP kustom adalah sebagai berikut.

```
{
  "username": "value",
  "password": "value",
  "protocol": "SFTP",
  "serverId": "s-abcd123456",
```



```
"sourceIp": "192.168.0.100"
}
```

Di mana username dan password merupakan nilai untuk kredensial masuk yang dikirim ke server.

Misalnya, Anda memasukkan perintah berikut untuk menghubungkan:

```
sftp bobusa@server_hostname
```

Anda kemudian diminta untuk memasukkan kata sandi Anda:

```
Enter password:
mysecretpassword
```

Anda dapat memeriksa ini dari fungsi Lambda Anda dengan mencetak peristiwa yang diteruskan dari dalam fungsi Lambda. Seharusnya terlihat mirip dengan blok teks berikut.

```
{
  "username": "bobusa",
  "password": "mysecretpassword",
  "protocol": "SFTP",
  "serverId": "s-abcd123456",
  "sourceIp": "192.168.0.100"
}
```

Struktur acara serupa untuk FTP dan FTPS: satu-satunya perbedaan adalah nilai-nilai tersebut digunakan untuk `protocol` parameter, bukan SFTP.

Fungsi Lambda untuk otentikasi

Untuk menerapkan strategi otentikasi yang berbeda, edit fungsi Lambda. Untuk membantu Anda memenuhi kebutuhan aplikasi Anda, Anda dapat menerapkan CloudFormation tumpukan. Untuk informasi selengkapnya tentang Lambda, lihat [Panduan AWS Lambda Pengembang](#) atau Membangun fungsi [Lambda](#) dengan Node.js

Topik

- [Nilai Lambda yang valid](#)
- [Contoh fungsi Lambda](#)
- [Menguji konfigurasi Anda](#)
- [Template fungsi Lambda](#)

Nilai Lambda yang valid

Tabel berikut menjelaskan detail nilai yang diterima Transfer Family untuk fungsi Lambda yang digunakan untuk penyedia identitas kustom.

Nilai	Deskripsi	Diperlukan
Role	Menentukan Nama Sumber Daya Amazon (ARN) dari peran IAM yang mengontrol akses pengguna ke bucket Amazon S3 atau sistem file Amazon EFS. Kebijakan yang dilampirkan pada peran ini menentukan tingkat akses yang ingin Anda berikan kepada pengguna saat mentransfer file masuk dan keluar dari sistem file Amazon S3 atau Amazon EFS Anda. IAM role juga harus berisi hubungan kepercayaan yang mengizinkan server untuk mengakses sumber daya Anda saat melayani permintaan transfer pengguna. Untuk detail tentang membangun hubungan kepercayaan, lihat Untuk membangun hubungan kepercayaan.	Diperlukan
PosixProfile	Identitas POSIX lengkap, termasuk ID pengguna (Uid), ID grup (Gid), dan ID grup sekunder (SecondaryGids) apa pun, yang mengontrol	Diperlukan untuk penyimpanan dukungan Amazon EFS

Nilai	Deskripsi	Diperlukan
	akses pengguna ke sistem file Amazon EFS Anda. POSIX izin yang ditetapkan pada file dan direktori dalam sistem file Anda menentukan tingkat akses pengguna Anda mendapatkan ketika mentransfer file ke dalam dan keluar dari sistem file Amazon EFS Anda.	
PublicKeys	Daftar nilai kunci publik SSH yang valid untuk pengguna ini. Daftar kosong menyiratkan bahwa ini bukan login yang valid. Tidak boleh dikembalikan selama otentikasi kata sandi.	Opsional
Policy	Kebijakan sesi untuk pengguna Anda sehingga Anda dapat menggunakan peran IAM yang sama di beberapa pengguna. Kebijakan ini mencakup bawah akses pengguna ke bagian dari bucket Amazon S3 mereka. Untuk informasi selengkapnya tentang penggunaan kebijakan sesi dengan penyedia identitas kustom, lihat contoh kebijakan sesi dalam topik ini.	Opsional

Nilai	Deskripsi	Diperlukan
HomeDirectoryType	Jenis direktori pendaratan (folder) yang Anda inginkan direktori home pengguna Anda ketika mereka masuk ke server. • Jika Anda mengatur <code>yaPATH</code>, pengguna akan melihat bucket Amazon S3 absolut atau jalur Amazon EFS seperti pada klien protokol transfer file mereka. • Jika Anda menyetel <code>yaLOGICAL</code>, Anda harus menyediakan pemetaan dalam <code>HomeDirectoryDetails</code> parameter agar jalur Amazon S3 atau Amazon EFS terlihat oleh pengguna Anda.	Opsional

Nilai	Deskripsi	Diperlukan
HomeDirectoryDetails	Pemetaan direktori logis yang menentukan jalur dan kunci Amazon S3 atau Amazon EFS mana yang harus terlihat oleh pengguna Anda dan bagaimana Anda ingin membuatnya terlihat. Anda harus menentukan Entry dan Target memasangkan, di mana Entry menunjukkan bagaimana jalur dibuat terlihat dan Target merupakan jalur Amazon S3 atau Amazon EFS yang sebenarnya.	Diperlukan jika HomeDirectoryType memiliki nilai LOGICAL

Nilai	Deskripsi	Diperlukan
HomeDirectory	Direktori pendaratan untuk pengguna ketika mereka masuk ke server menggunakan klien. Formatnya tergantung pada backend penyimpanan Anda: • Untuk Amazon S3: / bucket-name/user-home-directory Contoh: /amzn-s3-demo-bucket/users/john • Untuk Amazon EFS: / fs-12345/user-home-directory Contoh: /fs-faa1a123/users/john  Important Nama bucket atau ID sistem file Amazon EFS harus disertakan dalam path. Menghilangkan informasi ini akan mengakibatkan kesalahan “File tidak ditemukan” selama transfer file.	Opsional

Note

`HomeDirectoryDetails` adalah representasi string dari peta JSON. Hal ini berbeda dengan `PosixProfile`, yang merupakan objek peta JSON yang sebenarnya, dan `PublicKeys` yang merupakan array JSON string. Lihat contoh kode untuk detail khusus bahasa.

⚠ HomeDirectory Persyaratan Format

Saat menggunakan `HomeDirectory` parameter, pastikan Anda menyertakan format jalur lengkap:

- Untuk penyimpanan Amazon S3: Selalu sertakan nama bucket dalam format `/bucket-name/path`
- Untuk penyimpanan Amazon EFS: Selalu sertakan ID sistem file dalam format `/fs-12345/path`

Penyebab umum kesalahan “File tidak ditemukan” adalah menghilangkan nama bucket atau ID sistem file EFS dari `HomeDirectory` jalur. Pengaturan `HomeDirectory` ke hanya `/` tanpa pengenal penyimpanan akan menyebabkan otentikasi berhasil tetapi operasi file gagal.

Contoh fungsi Lambda

Bagian ini menyajikan beberapa contoh fungsi Lambda, baik di NodeJS maupun Python.

Note

Dalam contoh ini, detail direktori pengguna, peran, profil POSIX, kata sandi, dan home directory adalah contoh, dan harus diganti dengan nilai aktual Anda.

Logical home directory, NodeJS

[Fungsi contoh NodeJS berikut memberikan rincian untuk pengguna yang memiliki direktori home logis.](#)

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
      not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
  }
  callback(null, response);
};
```


Path-based home directory, NodeJS

Fungsi contoh NodeJS berikut memberikan rincian untuk pengguna yang memiliki direktori home berbasis jalur.

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
  (e.g., "127.0.0.1") to further restrict logins.
  if (event.serverId !== "" && event.username == 'example-user') {
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      Policy: '', // Optional, JSON stringified blob to further restrict this user's
      permissions
      // HomeDirectory format depends on your storage backend:
      // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
      users/john')
      // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
      replace with your bucket name
      // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
      for EFS
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {};
    }
  } else {
```

```
// Return HTTP status 200 but with no role in the response to indicate
authentication failure
response = {};
}
callback(null, response);
};
```

Logical home directory, Python

Contoh fungsi Python berikut memberikan rincian untuk pengguna yang memiliki direktori [home logis](#).

```
# 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

Contoh fungsi Python berikut memberikan rincian untuk pengguna yang memiliki direktori home berbasis jalur.

```

# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    # (e.g., "127.0.0.1") to further restrict logins.
    if event['serverId'] != '' and event['username'] == 'example-user':
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'Policy': '', # Optional, JSON stringified blob to further restrict this
            # user's permissions
            # HomeDirectory format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            # users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
            # replace with your bucket name
            # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
            # uncomment for EFS
            'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH

```

```

    }

    # Check if password is provided
    if event.get('password', '') == '':
        # If no password provided, return the user's SSH public key
        response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
        # Check if password is correct
        elif event['password'] != 'Password1234':
            # Return HTTP status 200 but with no role in the response to indicate
            authentication failure
            response = {}
        else:
            # Return HTTP status 200 but with no role in the response to indicate
            authentication failure
            response = {}

    return response

```

Menguji konfigurasi Anda

Setelah Anda membuat penyedia identitas kustom Anda, Anda harus menguji konfigurasi Anda.

Console

Untuk menguji konfigurasi Anda dengan menggunakan AWS Transfer Family konsol

1. Buka [konsol AWS Transfer Family](#).
2. Pada halaman Server, pilih server baru Anda, pilih Tindakan, lalu pilih Uji.
3. Masukkan teks untuk Nama Pengguna dan Kata Sandi yang Anda atur saat Anda menerapkan CloudFormation tumpukan. Jika Anda menyimpan opsi default, nama pengguna adalah myuser dan kata sandinyaMySuperSecretPassword.
4. Pilih protokol Server dan masukkan alamat IP untuk IP Sumber, jika Anda mengaturnya saat Anda menerapkan CloudFormation tumpukan.

CLI

Untuk menguji konfigurasi Anda dengan menggunakan AWS CLI

1. Jalankan perintah [test-identity-provider](#). Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri, seperti yang dijelaskan dalam langkah-langkah selanjutnya.

```
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. Masukkan ID server.
3. Masukkan nama pengguna dan kata sandi yang Anda tetapkan saat Anda menerapkan CloudFormation tumpukan. Jika Anda menyimpan opsi default, nama pengguna adalah myuser dan kata sandinya MySuperSecretPassword.
4. Masukkan protokol server dan alamat IP sumber, jika Anda mengaturnya saat Anda menerapkan CloudFormation tumpukan.

Jika otentikasi pengguna berhasil, pengujian mengembalikan respons `Status Code: 200 HTTP`, string kosong `Message: ""` (yang akan berisi alasan kegagalan jika tidak), dan bidang `Response`

Note

Dalam contoh respons di bawah ini, `Response` bidang adalah objek JSON yang telah “dirangkai” (diubah menjadi string JSON datar yang dapat digunakan di dalam program), dan berisi rincian peran dan izin pengguna.

```
{
  "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\": \"\"
}
```

Template fungsi Lambda

Anda dapat menerapkan CloudFormation tumpukan yang menggunakan fungsi Lambda untuk otentikasi. Kami menyediakan beberapa templat yang mengautentikasi dan mengotorisasi pengguna Anda menggunakan kredensial masuk. Anda dapat memodifikasi template atau AWS Lambda kode ini untuk lebih menyesuaikan akses pengguna.

Note

Anda dapat membuat FIPS-enabled AWS Transfer Family server melalui CloudFormation dengan menentukan kebijakan FIPS-enabled keamanan di template Anda. Kebijakan keamanan yang tersedia dijelaskan dalam [Kebijakan keamanan untuk AWS Transfer Family server](#)

Untuk membuat CloudFormation tumpukan yang akan digunakan untuk otentikasi

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Ikuti petunjuk untuk menerapkan CloudFormation tumpukan dari template yang ada di [Memilih template tumpukan](#) di Panduan AWS CloudFormation Pengguna.
3. Gunakan salah satu templat berikut untuk membuat fungsi Lambda yang akan digunakan untuk otentikasi di Transfer Family.

- [Templat tumpukan klasik \(Amazon Cognito\)](#)

Template dasar untuk membuat AWS Lambda untuk digunakan sebagai penyedia identitas kustom di AWS Transfer Family. Ini mengautentikasi terhadap Amazon Cognito untuk otentikasi berbasis kata sandi dan kunci publik dikembalikan dari bucket Amazon S3 jika otentikasi berbasis kunci publik digunakan. Setelah penerapan, Anda dapat memodifikasi kode fungsi Lambda untuk melakukan sesuatu yang berbeda.

- [AWS Secrets Manager template tumpukan](#)

Template dasar yang digunakan AWS Lambda dengan AWS Transfer Family server untuk mengintegrasikan Secrets Manager sebagai penyedia identitas. Ini mengotentikasi terhadap entri dalam AWS Secrets Manager format `aws/transfer/server-id/username`. Selain itu, secret harus menyimpan pasangan kunci-nilai untuk semua properti pengguna yang dikembalikan ke Transfer Family. Setelah penerapan, Anda dapat memodifikasi kode fungsi Lambda untuk melakukan sesuatu yang berbeda.

- [Template tumpukan Okta](#): Template dasar yang digunakan AWS Lambda dengan AWS Transfer Family server untuk mengintegrasikan Okta sebagai penyedia identitas khusus.
- [Okta-mfa stack template: Template](#) dasar yang digunakan AWS Lambda dengan AWS Transfer Family server untuk mengintegrasikan Okta, dengan Multi Factor Authentication, sebagai penyedia identitas khusus.
- [Template Azure Active Directory](#): detail untuk tumpukan ini dijelaskan dalam posting blog [Mengautentikasi AWS Transfer Family dengan Azure Active Directory](#) dan. AWS Lambda

Setelah tumpukan dikerahkan, Anda dapat melihat detailnya di tab Output di CloudFormation konsol.

Menerapkan salah satu tumpukan ini adalah cara termudah untuk mengintegrasikan penyedia identitas kustom ke dalam alur kerja Transfer Family.

Menggunakan Amazon API Gateway untuk mengintegrasikan penyedia identitas Anda

Topik ini menjelaskan cara menggunakan AWS Lambda fungsi untuk mendukung metode API Gateway. Gunakan opsi ini jika Anda memerlukan RESTful API untuk mengintegrasikan penyedia identitas Anda atau jika Anda ingin menggunakannya untuk memanfaatkan kemampuannya AWS WAF untuk permintaan pemblokiran geografis atau pembatasan laju.

Untuk sebagian besar kasus penggunaan, cara yang disarankan untuk mengonfigurasi penyedia identitas khusus adalah dengan menggunakan [Solusi penyedia identitas khusus](#).

Batasan jika menggunakan API Gateway untuk mengintegrasikan penyedia identitas Anda

- Konfigurasi ini tidak mendukung domain kustom.
- Konfigurasi ini tidak mendukung URL API Gateway pribadi.

Jika Anda membutuhkan salah satu dari ini, Anda dapat menggunakan Lambda sebagai penyedia identitas, tanpa API Gateway. Lihat perinciannya di [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#).

Mengautentikasi menggunakan metode API Gateway

Anda dapat membuat metode API Gateway untuk digunakan sebagai penyedia identitas untuk Transfer Family. Pendekatan ini menyediakan cara yang sangat aman bagi Anda untuk membuat

dan menyediakan API. Dengan API Gateway, Anda dapat membuat titik akhir HTTPS sehingga semua operasi API yang masuk ditransmisikan dengan keamanan yang lebih besar. Untuk detail selengkapnya tentang layanan API Gateway, lihat [Panduan Pengembang API Gateway](#).

API Gateway menawarkan metode otorisasi bernama `AWS_IAM`, yang memberi Anda autentikasi yang sama berdasarkan AWS Identity and Access Management (IAM) yang AWS digunakan secara internal. Jika Anda mengaktifkan autentikasi `AWS_IAM`, hanya penelepon dengan izin eksplisit untuk memanggil API yang dapat mencapai metode API Gateway API tersebut.

Untuk menggunakan metode API Gateway Anda sebagai penyedia identitas khusus untuk Transfer Family, aktifkan IAM untuk metode API Gateway Anda. Sebagai bagian dari proses ini, Anda memberikan peran IAM dengan izin untuk Transfer Family untuk menggunakan gateway Anda.

 Note

Untuk meningkatkan keamanan, Anda dapat mengkonfigurasi firewall aplikasi web. AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke Amazon API Gateway. Lihat perinciannya di [Tambahkan firewall aplikasi web](#).

 Jangan aktifkan caching API Gateway

Jangan aktifkan caching untuk metode API Gateway Anda saat menggunakannya sebagai penyedia identitas khusus untuk Transfer Family. Caching tidak pantas dan tidak valid untuk permintaan otentikasi karena:

- Setiap permintaan otentikasi unik dan memerlukan respons langsung, bukan respons yang di-cache
- Caching tidak memberikan manfaat karena Transfer Family tidak pernah mengirimkan permintaan duplikat atau berulang ke API Gateway
- Mengaktifkan caching akan menyebabkan API Gateway merespons dengan data yang tidak cocok, sehingga respons yang tidak valid terhadap permintaan otentikasi

Untuk menggunakan metode API Gateway Anda untuk autentikasi kustom dengan Transfer Family

1. Buat CloudFormation tumpukan. Untuk melakukannya:

 Note

Templat tumpukan telah diperbarui untuk menggunakan BASE64-encoded kata sandi: untuk detailnya, lihat [Perbaikan CloudFormation template](#).

- a. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
- b. Ikuti petunjuk untuk menerapkan CloudFormation tumpukan dari template yang ada di [Memilih template tumpukan](#) di Panduan AWS CloudFormation Pengguna.
- c. Gunakan salah satu templat dasar berikut untuk membuat metode API Gateway yang AWS Lambda didukung untuk digunakan sebagai penyedia identitas kustom di Transfer Family.

- [Template tumpukan dasar](#)

Secara default, metode API Gateway Anda digunakan sebagai penyedia identitas khusus untuk mengautentikasi satu pengguna dalam satu server menggunakan kunci atau kata sandi SSH (Secure Shell) dengan kode keras. Setelah penerapan, Anda dapat memodifikasi kode fungsi Lambda untuk melakukan sesuatu yang berbeda.

- [AWS Secrets Manager template tumpukan](#)

Secara default, metode API Gateway Anda melakukan autentikasi terhadap entri di Secrets Manager format `aws/transfer/server-id/username`. Selain itu, secret harus menyimpan pasangan kunci-nilai untuk semua properti pengguna yang dikembalikan ke Transfer Family. Setelah penerapan, Anda dapat memodifikasi kode fungsi Lambda untuk melakukan sesuatu yang berbeda. Untuk informasi selengkapnya, lihat posting blog [Aktifkan otentikasi kata sandi untuk AWS Transfer Family digunakan AWS Secrets Manager](#).

- [Templat tumpukan Okta](#)

Metode API Gateway Anda terintegrasi dengan Okta sebagai penyedia identitas khusus di Transfer Family. Untuk informasi lebih lanjut, lihat posting blog [Menggunakan Okta sebagai penyedia identitas dengan AWS Transfer Family](#).

Menerapkan salah satu tumpukan ini adalah cara termudah untuk mengintegrasikan penyedia identitas kustom ke dalam alur kerja Transfer Family. Setiap tumpukan menggunakan fungsi Lambda untuk mendukung metode API Anda berdasarkan API Gateway. Anda kemudian dapat

menggunakan metode API Anda sebagai penyedia identitas kustom di Transfer Family. Secara default, fungsi Lambda mengautentikasi satu pengguna yang dipanggil `myuser` dengan kata sandi `MySuperSecretPassword`. Setelah penerapan, Anda dapat mengedit kredensial ini atau memperbarui kode fungsi Lambda untuk melakukan sesuatu yang berbeda.

 Important

Kami menyarankan Anda mengedit kredensi pengguna dan kata sandi default.

Setelah tumpukan dikerahkan, Anda dapat melihat detailnya di tab Output di CloudFormation konsol. Detail ini termasuk Amazon Resource Name (ARN) stack, ARN dari peran IAM yang dibuat stack, dan URL untuk gateway baru Anda.

 Note

Jika Anda menggunakan opsi penyedia identitas khusus untuk mengaktifkan autentikasi berbasis kata sandi bagi pengguna Anda, dan Anda mengaktifkan pencatatan permintaan dan respons yang disediakan oleh API Gateway, API Gateway mencatat kata sandi pengguna Anda ke Log Amazon Anda. CloudWatch Kami tidak menyarankan menggunakan log ini di lingkungan produksi Anda. Untuk informasi selengkapnya, lihat [Menyiapkan pencatatan CloudWatch API di API Gateway](#) di Panduan Pengembang API Gateway.

2. Periksa konfigurasi metode API Gateway untuk server Anda. Untuk melakukannya:
 - a. Buka konsol API Gateway di <https://console.aws.amazon.com/apigateway/>.
 - b. Pilih API template dasar Transfer Custom Identity Provider yang dihasilkan CloudFormation template. Anda mungkin perlu memilih wilayah Anda untuk melihat gateway Anda.
 - c. Di panel Resources, pilih GET. Tangkapan layar berikut menunjukkan konfigurasi metode yang benar.

The screenshot displays the AWS API Gateway console interface for configuring a new resource. On the left, a sidebar shows a hierarchical resource tree with paths: /, /servers, /serverId, /users, /username, and /config. The 'GET' method is selected for the /config path. The main panel shows the 'Method request' settings, which include:

- Method request settings:**
 - Authorization: AWS_IAM
 - Request validator: None
 - API key required: False
 - SDK operation name: Generated based on method and path
- Request paths (0):** No request paths defined.
- URL query string parameters (2):**

Name	Required	Caching
protocol	False	Inactive
sourceIp	False	Inactive
- HTTP request headers (1):**

Name	Required	Caching
PasswordBase64	False	Inactive
- Request body (0):** No request body defined.

Pada titik ini, gateway API Anda siap digunakan.

- Untuk Tindakan, pilih Deploy API. Untuk tahap Deployment, pilih prod, lalu pilih Deploy.

Setelah metode API Gateway berhasil diterapkan, lihat kinerjanya di Tahapan> Detail tahap, seperti yang ditunjukkan pada gambar berikut.

Note

Salin alamat URL Invoke yang muncul di bagian atas layar. Anda mungkin membutuhkannya untuk langkah selanjutnya.

4. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
5. Transfer Family seharusnya dibuat untuk Anda, saat Anda membuat tumpukan. Jika tidak, konfigurasi server Anda menggunakan langkah-langkah ini.
 - a. Pilih Buat server untuk membuka halaman Buat server. Untuk Pilih penyedia identitas, pilih Kustom, lalu pilih Gunakan Amazon API Gateway untuk terhubung ke penyedia identitas Anda, seperti yang ditunjukkan pada gambar berikut.

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. Di kotak teks Berikan URL Amazon API Gateway, tempelkan alamat URL Panggilan titik akhir API Gateway yang Anda buat di langkah 3 prosedur ini.
- c. Untuk Peran, pilih peran IAM yang dibuat oleh CloudFormation template. Peran ini memungkinkan Transfer Family untuk menjalankan metode gateway API Anda.

Peran pemanggilan berisi nama CloudFormation tumpukan yang Anda pilih untuk tumpukan yang Anda buat di langkah 1. Ini memiliki format berikut: *CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI*.

- d. Isi kotak yang tersisa, lalu pilih Buat server. Untuk detail tentang langkah-langkah yang tersisa untuk membuat server, lihat [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#).

Menerapkan metode API Gateway Anda

Untuk membuat penyedia identitas khusus untuk Transfer Family, metode API Gateway Anda harus mengimplementasikan satu metode yang memiliki jalur sumber daya `/servers/serverId/users/username/config`. Nilai *serverId* dan berasal dari jalur sumber daya RESTful. Juga, tambahkan `sourceIp` dan `protocol` sebagai Parameter String Kueri URL dalam Permintaan Metode, seperti yang ditunjukkan pada gambar berikut.

Resources

Create resource

/servers

/servers

/users

/users

/config

GET

/servers/{serverId}/users/{username}/config - GET - Method execution

ARN: `arn:aws:execute-api-east-1:...`

Resource ID: `aw4lhw`

Method request → Integration request → Lambda integration

Method response ← Integration response ←

Method request settings

Authorization: `AWS_IAM`

Request validator: `None`

API key required: `False`

SDK operation name: `Generated based on method and path`

Request paths (0)

No request paths defined

URL query string parameters (2)

Name	Required	Caching
protocol	False	Inactive
sourceIp	False	Inactive

Note

Nama pengguna harus minimal 3 dan maksimal 100 karakter. Anda dapat menggunakan karakter berikut dalam nama pengguna: `a—z`, `0—9` `A—Z`, garis bawah `'_'`, tanda hubung `'-'`, titik `'.'` dan di tanda `'@'`. Nama pengguna tidak dapat dimulai dengan tanda hubung `'-'`, titik `'.'` atau di tanda `'@'`.

Jika Transfer Family mencoba otentikasi kata sandi untuk pengguna Anda, layanan akan menyediakan bidang Password: header. Jika tidak ada Password: header, Transfer Family mencoba otentikasi kunci publik untuk mengautentikasi pengguna Anda.

Saat Anda menggunakan penyedia identitas untuk mengautentikasi dan mengotorisasi pengguna akhir, selain memvalidasi kredensialnya, Anda dapat mengizinkan atau menolak permintaan akses berdasarkan alamat IP klien yang digunakan oleh pengguna akhir Anda. Anda dapat menggunakan fitur ini untuk memastikan bahwa data yang disimpan di bucket S3 atau sistem file Amazon EFS Anda dapat diakses melalui protokol yang didukung hanya dari alamat IP yang telah Anda tentukan sebagai tepercaya. Untuk mengaktifkan fitur ini, Anda harus menyertakan sourceIp dalam string Query.

Jika Anda memiliki beberapa protokol yang diaktifkan untuk server Anda dan ingin memberikan akses menggunakan nama pengguna yang sama melalui beberapa protokol, Anda dapat melakukannya selama kredensial khusus untuk setiap protokol telah diatur di penyedia identitas Anda. Untuk mengaktifkan fitur ini, Anda harus menyertakan *protocol* nilai di jalur sumber daya RESTful.

Metode API Gateway Anda harus selalu menampilkan kode status HTTP200. Kode status HTTP lainnya berarti ada kesalahan saat mengakses API.

Contoh respons Amazon S3

Contoh badan respons adalah dokumen JSON dari formulir berikut untuk Amazon S3.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

Kebijakan ini lolos dari JSON sebagai string. Contoh:

```
"Policy":
"{
```

```

\"Version\": \"2012-10-17\",
\"Statement\":
[
  {\"Condition\":
    {\"StringLike\":
      {\"s3:prefix\":
        [\"user/*\", \"user/\"]}},
    \"Resource\": \"arn:aws:s3:::amzn-s3-demo-bucket\",
    \"Action\": \"s3:ListBucket\",
    \"Effect\": \"Allow\",
    \"Sid\": \"ListHomeDir\"},
  {\"Resource\": \"arn:aws:s3:::*\",
    \"Action\": [\"s3:PutObject\",
      \"s3:GetObject\",
      \"s3:DeleteObjectVersion\",
      \"s3:DeleteObject\",
      \"s3:GetObjectVersion\",
      \"s3:GetObjectACL\",
      \"s3:PutObjectACL\"],
    \"Effect\": \"Allow\",
    \"Sid\": \"HomeDirObjectAccess\"}]
}

```

Contoh respon berikut menunjukkan bahwa pengguna memiliki tipe direktori home logis.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\", \"Target\": \"/amzn-s3-demo-bucket1\"}]",
  "PublicKeys": [""],
}

```

Contoh respons Amazon EFS

Contoh badan respons adalah dokumen JSON dari formulir berikut untuk Amazon EFS.

```

{
  "Role": "IAM role with configured EFS permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ]
}

```



```

],
"PosixProfile": {
  "Uid": "POSIX user ID",
  "Gid": "POSIX group ID",
  "SecondaryGids": [Optional list of secondary Group IDs],
},
"HomeDirectory": "/fs-id/path/to/home/directory"
}

```

RoleBidang menunjukkan bahwa otentikasi berhasil terjadi. Saat melakukan otentikasi kata sandi (saat Anda menyediakan Password: header), Anda tidak perlu memberikan kunci publik SSH. Jika pengguna tidak dapat diautentikasi, misalnya, jika kata sandi salah, metode Anda harus mengembalikan respons tanpa Role disetel. Contoh respon tersebut adalah objek JSON kosong.

Contoh respon berikut menunjukkan pengguna yang memiliki tipe direktori home logis.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\"/\\\"\", \"Target\": \"\\\"/faa1a123\\\"}]\"",
  "PublicKeys": [""],
  "PosixProfile": {"Uid": 65534, "Gid": 65534}
}

```

Anda dapat menyertakan kebijakan pengguna dalam fungsi Lambda dalam format JSON. Untuk informasi selengkapnya tentang mengonfigurasi kebijakan pengguna di Transfer Family, lihat [Mengelola kontrol akses](#).

Fungsi Lambda default

Untuk menerapkan strategi otentikasi yang berbeda, edit fungsi Lambda yang digunakan gateway Anda. Untuk membantu Anda memenuhi kebutuhan aplikasi Anda, Anda dapat menggunakan contoh fungsi Lambda berikut di Node.js Untuk informasi selengkapnya tentang Lambda, lihat [Panduan AWS Lambda Pengembang](#) atau Membangun fungsi [Lambda](#) dengan Node.js

Contoh fungsi Lambda berikut mengambil nama pengguna, kata sandi (jika Anda melakukan otentikasi kata sandi), ID server, protokol, dan alamat IP klien. Anda dapat menggunakan kombinasi input ini untuk mencari penyedia identitas Anda dan menentukan apakah login harus diterima.

 Note

Jika Anda memiliki beberapa protokol yang diaktifkan untuk server Anda dan ingin memberikan akses menggunakan nama pengguna yang sama melalui beberapa protokol, Anda dapat melakukannya selama kredensial khusus untuk protokol telah diatur di penyedia identitas Anda.

Untuk File Transfer Protocol (FTP), kami sarankan untuk mempertahankan kredensial terpisah dari Secure Shell (SSH) File Transfer Protocol (SFTP) dan File Transfer Protocol melalui SSL (FTPS). Sebaiknya pertahankan kredensial terpisah untuk FTP karena, tidak seperti SFTP dan FTPS, FTP mentransmisikan kredensial dalam teks yang jelas. Dengan mengisolasi kredensial FTP dari SFTP atau FTPS, jika kredensial FTP dibagikan atau diekspos, beban kerja Anda menggunakan SFTP atau FTPS tetap aman.

Fungsi contoh ini mengembalikan peran dan rincian direktori home logis, bersama dengan kunci publik (jika melakukan otentikasi kunci publik).

Saat Anda membuat pengguna yang dikelola layanan, Anda mengatur direktori home mereka, baik logis maupun fisik. Demikian pula, kita membutuhkan hasil fungsi Lambda untuk menyampaikan struktur direktori fisik atau logis pengguna yang diinginkan. Parameter yang Anda tetapkan bergantung pada nilai untuk [HomeDirectoryType](#) bidang tersebut.

- `HomeDirectoryType` disetel ke `PATH` — `HomeDirectory` bidang tersebut kemudian harus berupa awalan bucket Amazon S3 absolut atau jalur absolut Amazon EFS yang dapat dilihat oleh pengguna Anda.
- `HomeDirectoryType` set ke `LOGICAL` - Jangan mengatur `HomeDirectory` bidang. Sebagai gantinya, kami menetapkan `HomeDirectoryDetails` bidang yang menyediakan Entry/Target pemetaan yang diinginkan, mirip dengan nilai yang dijelaskan dalam [HomeDirectoryDetails](#) parameter untuk pengguna yang dikelola layanan.

Contoh fungsi tercantum dalam [Contoh fungsi Lambda](#).

Fungsi Lambda untuk digunakan dengan AWS Secrets Manager

Untuk digunakan AWS Secrets Manager sebagai penyedia identitas Anda, Anda dapat bekerja dengan fungsi Lambda di template sampel CloudFormation . Fungsi Lambda menanyakan layanan Secrets Manager dengan kredensial Anda dan, jika berhasil, mengembalikan rahasia yang ditunjuk.

Untuk informasi selengkapnya tentang Secrets Manager, lihat [Panduan Pengguna AWS Secrets Manager](#).

Untuk mengunduh contoh CloudFormation template yang menggunakan fungsi Lambda ini, buka bucket [Amazon S3](#) yang disediakan oleh AWS Transfer Family

Perbaikan CloudFormation template

Perbaikan antarmuka API Gateway telah dilakukan pada CloudFormation template yang diterbitkan. Template sekarang menggunakan BASE64-encoded kata sandi dengan API Gateway. Penerapan Anda yang ada terus berfungsi tanpa peningkatan ini, tetapi jangan izinkan kata sandi dengan karakter di luar set karakter dasar US-ASCII .

Perubahan dalam template yang mengaktifkan kemampuan ini adalah sebagai berikut:

- `GetUserConfigRequest` `AWS::ApiGateway::Method` sumber daya harus memiliki `RequestTemplates` kode ini (baris miring adalah baris yang diperbarui)

```
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')",
    }
```

- `GetUserConfigSumber` daya harus diubah untuk menggunakan `PasswordBase64` header (baris miring adalah baris yang diperbarui): `RequestParameters`

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
  method.request.querystring.sourceIp: false
```

Untuk memeriksa apakah template untuk tumpukan Anda adalah yang terbaru

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.

2. Dari daftar tumpukan, pilih tumpukan Anda.
3. Dari panel detail, pilih tab Template.
4. Cari yang berikut ini:
 - `CariRequestTemplates`, dan pastikan Anda memiliki baris ini:

```
"password":  
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(  
    \',\'',\'"\')
```

- `CariRequestParameters`, dan pastikan Anda memiliki baris ini:

```
method.request.header.PasswordBase64: false
```

Jika Anda tidak melihat baris yang diperbarui, edit tumpukan Anda. Untuk detail tentang cara memperbarui CloudFormation tumpukan Anda, lihat [Memodifikasi template tumpukan](#) di AWS CloudFormation; Panduan Pengguna.

Menggunakan beberapa metode otentikasi

Server Transfer Family mengontrol logika AND saat Anda menggunakan beberapa metode otentikasi. Transfer Family memperlakukan ini sebagai dua permintaan terpisah ke penyedia identitas kustom Anda: namun, efeknya digabungkan.

Kedua permintaan harus berhasil dikembalikan dengan respons yang benar untuk memungkinkan otentikasi selesai. Transfer Family mengharuskan dua tanggapan lengkap, artinya berisi semua elemen yang diperlukan (peran, direktori beranda, kebijakan, dan profil POSIX jika Anda menggunakan Amazon EFS untuk penyimpanan). Transfer Family juga mensyaratkan bahwa respons kata sandi tidak boleh menyertakan kunci publik.

Permintaan kunci publik harus memiliki respons terpisah dari penyedia identitas. Perilaku itu tidak berubah saat menggunakan Kata Sandi ATAU Kunci atau Kata Sandi DAN Kunci.

SSH/SFTP Protokol menantang klien perangkat lunak terlebih dahulu dengan otentikasi kunci publik, kemudian meminta otentikasi kata sandi. Operasi ini mengamankan keduanya berhasil sebelum pengguna diizinkan untuk menyelesaikan otentikasi.

Untuk opsi penyedia identitas kustom, Anda dapat menentukan salah satu opsi berikut untuk cara mengautentikasi.

- Kata Sandi ATAU Kunci — pengguna dapat mengautentikasi dengan kata sandi atau kunci mereka. Ini adalah nilai default.
- Hanya kata sandi — pengguna harus memberikan kata sandi mereka untuk terhubung.
- Hanya kunci — pengguna harus menyediakan kunci pribadi mereka untuk terhubung.
- Kata Sandi dan Kunci — pengguna harus memberikan kunci pribadi dan kata sandi mereka untuk terhubung. Server memeriksa kunci terlebih dahulu, dan kemudian jika kuncinya valid, sistem meminta kata sandi. Jika kunci pribadi yang disediakan tidak cocok dengan kunci publik yang disimpan, otentikasi gagal.

Dukungan IPv6 untuk penyedia identitas khusus

AWS Transfer Family penyedia identitas khusus sepenuhnya mendukung koneksi IPv6. Saat menerapkan penyedia identitas khusus, fungsi Lambda Anda dapat menerima dan memproses permintaan otentikasi dari klien IPv4 dan IPv6 tanpa konfigurasi tambahan apa pun. Fungsi Lambda menerima alamat IP klien di `sourceIp` bidang permintaan, yang dapat berupa alamat IPv4 (misalnya, `203.0.113.42`) atau alamat IPv6 (misalnya, `2001:db8:85a3:8d3:1319:8a2e:370:7348`). Implementasi penyedia identitas kustom Anda harus menangani kedua format alamat dengan tepat.

Important

Jika penyedia identitas kustom Anda melakukan IP-based validasi atau logging, pastikan implementasi Anda menangani format alamat IPv6 dengan benar. Alamat IPv6 lebih panjang dari alamat IPv4 dan menggunakan format notasi yang berbeda.

Note

Saat menangani alamat IPv6 di penyedia identitas kustom Anda, pastikan Anda menggunakan fungsi penguraian alamat IPv6 yang tepat daripada perbandingan string sederhana. Alamat IPv6 dapat direpresentasikan dalam berbagai format kanonik (misalnya `fd00:b600::ec2` atau `fd00:b600:0:0:0:0:ec2`). Gunakan pustaka atau fungsi alamat IPv6 yang sesuai dalam bahasa implementasi Anda untuk memvalidasi dan membandingkan alamat IPv6 dengan benar.

Example Menangani alamat IPv4 dan IPv6 di penyedia identitas khusus

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

Untuk informasi selengkapnya tentang penerapan penyedia identitas kustom, lihat [Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda](#).

Menggunakan AWS Directory Service untuk Microsoft Active Directory

Anda dapat menggunakan AWS Transfer Family untuk mengautentikasi pengguna akhir transfer file Anda menggunakan AWS Directory Service for Microsoft Active Directory. Ini memungkinkan migrasi mulus dari alur kerja transfer file yang mengandalkan otentikasi Active Directory tanpa mengubah kredensial pengguna akhir atau memerlukan otorisasi khusus.

Dengan AWS Managed Microsoft AD, Anda dapat dengan aman memberikan akses kepada Directory Service pengguna dan grup melalui SFTP, FTPS, dan FTP untuk data yang disimpan di Amazon Simple Storage Service (Amazon S3) atau Amazon Elastic File System (Amazon EFS). Jika Anda menggunakan Active Directory untuk menyimpan kredensi pengguna Anda, Anda sekarang memiliki cara yang lebih mudah untuk mengaktifkan transfer file untuk pengguna ini.

Anda dapat memberikan akses ke grup Active Directory AWS Managed Microsoft AD di lingkungan lokal atau di AWS Cloud menggunakan konektor Active Directory. Anda dapat memberi pengguna yang sudah dikonfigurasi di lingkungan Microsoft Windows Anda, baik di AWS Cloud atau di jaringan

lokal mereka, akses ke AWS Transfer Family server yang menggunakan AWS Managed Microsoft AD identitas. Blog AWS penyimpanan berisi posting yang merinci solusi untuk menggunakan Active Directory dengan Transfer Family: [Sederhanakan otentikasi Active Directory dengan penyedia identitas kustom untuk](#). AWS Transfer Family

 Note

- AWS Transfer Family tidak mendukung Simple AD.
- Transfer Family tidak mendukung konfigurasi Direktori Aktif lintas wilayah: kami hanya mendukung integrasi Direktori Aktif yang berada di wilayah yang sama dengan server Transfer Family.
- Transfer Family tidak mendukung penggunaan salah satu AWS Managed Microsoft AD atau AD Connector untuk mengaktifkan otentikasi multi-faktor (MFA) untuk infrastruktur MFA Anda yang ada. RADIUS-based
- AWS Transfer Family tidak mendukung wilayah replikasi Direktori Aktif Terkelola.

Untuk menggunakannya AWS Managed Microsoft AD, Anda harus melakukan langkah-langkah berikut:

1. Buat satu atau lebih AWS Managed Microsoft AD direktori menggunakan Directory Service konsol.
2. Gunakan konsol Transfer Family untuk membuat server yang digunakan AWS Managed Microsoft AD sebagai penyedia identitasnya.
3. Siapkan AWS Direktori menggunakan Konektor Direktori Aktif.
4. Tambahkan akses dari satu atau beberapa Directory Service grup Anda.
5. Meskipun tidak diperlukan, kami menyarankan Anda menguji dan memverifikasi akses pengguna.

Topik

- [Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory](#)
- [Bekerja dengan ranah Active Directory](#)
- [Memilih AWS Managed Microsoft AD sebagai penyedia identitas Anda](#)
- [Menghubungkan ke Microsoft Active Directory di lokasi](#)

- [Memberikan akses ke grup](#)
- [Menguji pengguna](#)
- [Menghapus akses server untuk grup](#)
- [Menghubungkan ke server menggunakan SSH \(Secure Shell\)](#)
- [Menghubungkan AWS Transfer Family ke Active Directory yang dikelola sendiri menggunakan hutan dan trust](#)

Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory

 Note

AWS Transfer Family memiliki batas default 100 grup Active Directory per server. Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Menyediakan pengenal unik untuk grup iklan Anda

Sebelum dapat menggunakan AWS Managed Microsoft AD, Anda harus memberikan pengenal unik untuk setiap grup di direktori Microsoft AD Anda. Anda dapat menggunakan pengenal keamanan (SID) untuk setiap grup untuk melakukan ini. Pengguna grup yang Anda asosiasikan memiliki akses ke sumber daya Amazon S3 atau Amazon EFS Anda melalui protokol yang diaktifkan menggunakan Transfer Family. AWS

Gunakan PowerShell perintah Windows berikut untuk mengambil SID untuk grup, ganti *YourGroupName* dengan nama grup.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```

 Note

Jika Anda menggunakan AWS Directory Service sebagai penyedia identitas Anda, dan jika `userPrincipalName` dan `SamAccountName` memiliki nilai yang berbeda, AWS

Transfer Family terima nilainya. SamAccountName Transfer Family tidak menerima nilai yang ditentukan dalam userPrincipalName.

Tambahkan Directory Service izin ke peran Anda

Anda juga memerlukan izin Directory Service API untuk digunakan AWS Directory Service sebagai penyedia identitas Anda. Izin berikut diperlukan atau disarankan:

- `ds:DescribeDirectories` Diperlukan Transfer Family untuk mencari direktori
- `ds:AuthorizeApplication` diperlukan untuk menambahkan otorisasi untuk Transfer Family
- `ds:UnauthorizeApplication` disarankan untuk menghapus sumber daya apa pun yang dibuat untuk sementara, jika terjadi kesalahan selama proses pembuatan server

Tambahkan izin ini ke peran yang Anda gunakan untuk membuat server Transfer Family Anda. Untuk detail selengkapnya tentang izin ini, lihat Izin [Directory Service API: Referensi tindakan, sumber daya, dan kondisi](#).

Bekerja dengan ranah Active Directory

Saat Anda mempertimbangkan cara agar pengguna Active Directory mengakses AWS Transfer Family server, ingatlah ranah pengguna, dan ranah grup mereka. Idealnya, ranah pengguna dan ranah grup mereka harus cocok. Artinya, baik pengguna maupun grup berada di ranah default, atau keduanya berada di ranah tepercaya. Jika tidak demikian, pengguna tidak dapat diautentikasi oleh Transfer Family.

Anda dapat menguji pengguna untuk memastikan konfigurasi sudah benar. Lihat perinciannya di [Menguji pengguna](#). Jika ada masalah dengan user/group ranah, Anda menerima kesalahan, Tidak ada akses terkait yang ditemukan untuk grup pengguna.

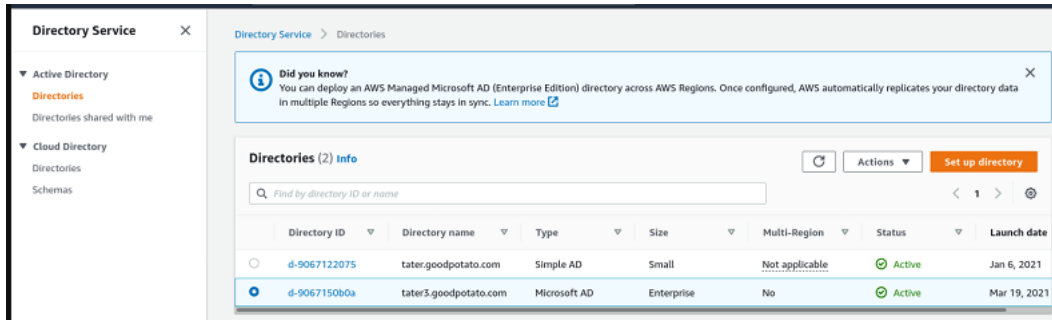
Memilih AWS Managed Microsoft AD sebagai penyedia identitas Anda

Bagian ini menjelaskan cara menggunakan AWS Directory Service for Microsoft Active Directory dengan server.

Untuk digunakan AWS Managed Microsoft AD dengan Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.

Gunakan Directory Service konsol untuk mengonfigurasi satu atau beberapa direktori terkelola. Untuk informasi lebih lanjut, lihat [AWS Managed Microsoft AD](#) dalam Panduan Admin Directory Service .



- Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>, dan pilih Buat server.
- Pada halaman Pilih protokol, pilih satu atau beberapa protokol dari daftar.

Note

Jika Anda memilih FTPS, Anda harus memberikan AWS Certificate Manager sertifikat.

- Untuk Pilih penyedia identitas, pilih AWS Directory Service.

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

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider

Manage users by integrating an identity provider of your choice

Directory

TATER3

Cancel

Previous

Next

5. Daftar Direktori berisi semua direktori terkelola yang telah Anda konfigurasi. Pilih direktori dari daftar, dan pilih Berikutnya.

 Note

- Cross-Account dan Direktori bersama tidak didukung untuk AWS Managed Microsoft AD.
- Untuk menyiapkan server dengan Directory Service sebagai penyedia identitas Anda, Anda perlu menambahkan beberapa Directory Service izin. Lihat perinciannya di [Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory](#).

6. Untuk menyelesaikan pembuatan server, gunakan salah satu prosedur berikut:

- [Buat SFTP-enabled server](#)
- [Buat FTPS-enabled server](#)
- [Buat FTP-enabled server](#)

Dalam prosedur tersebut, lanjutkan dengan langkah berikut memilih penyedia identitas.

 Important

Anda tidak dapat menghapus direktori Microsoft AD Directory Service jika Anda menggunakannya di server Transfer Family. Anda harus menghapus server terlebih dahulu, dan kemudian Anda dapat menghapus direktori.

Menghubungkan ke Microsoft Active Directory di lokasi

Bagian ini menjelaskan cara menyiapkan AWS Direktori menggunakan AD Connector

Untuk mengatur AWS Direktori menggunakan AD Connector

1. Buka konsol [Directory Service](#) dan pilih Directories.
2. Pilih Siapkan direktori.
3. Untuk jenis direktori, pilih AD Connector.

4. Pilih ukuran direktori, pilih Berikutnya, lalu pilih VPC dan Subnet Anda.
5. Pilih Berikutnya, lalu isi kolom sebagai berikut:
 - Nama DNS direktori: masukkan nama domain yang Anda gunakan untuk Microsoft Active Directory Anda.
 - Alamat IP DNS: masukkan alamat IP Microsoft Active Directory Anda.
 - Nama pengguna dan kata sandi akun server: masukkan detail untuk akun layanan yang akan digunakan.
6. Lengkapi layar untuk membuat layanan direktori.

Langkah selanjutnya adalah membuat server Transfer Family dengan protokol SFTP, dan tipe penyedia identitas AWS Directory Service. Dari daftar drop-down Direktori, pilih direktori yang Anda tambahkan di prosedur sebelumnya.

Memberikan akses ke grup

Setelah Anda membuat server, Anda harus memilih grup mana di direktori yang harus memiliki akses untuk mengunggah dan mengunduh file melalui protokol yang diaktifkan menggunakan. AWS Transfer Family Anda melakukan ini dengan membuat akses.

Note

AWS Transfer Family memiliki batas default 100 grup Active Directory per server. Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Note

Pengguna harus menjadi bagian langsung dari grup tempat Anda memberikan akses. Misalnya, asumsikan bahwa Bob adalah pengguna dan milik GroupA, dan GroupA sendiri termasuk dalam GroupB.

- Jika Anda memberikan akses ke GroupA, Bob diberikan akses.
- Jika Anda memberikan akses ke GroupB (dan bukan ke GroupA), Bob tidak memiliki akses.

Untuk memberikan akses ke grup

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Arahkan ke halaman detail server Anda.
3. Di bagian Accesses, pilih Tambah akses.
4. Masukkan SID untuk AWS Managed Microsoft AD direktori yang ingin Anda akses ke server ini.

 Note

Untuk informasi tentang cara menemukan SID untuk grup Anda, lihat [the section called “Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory”](#).

5. Untuk Access, pilih peran AWS Identity and Access Management (IAM) untuk grup.
6. Di bagian Kebijakan, pilih kebijakan. Pengaturan defaultnya adalah None.
7. Untuk direktori Home, pilih bucket Amazon S3 yang sesuai dengan direktori home grup.

 Note

Anda dapat membatasi bagian bucket yang dilihat pengguna dengan membuat kebijakan sesi. Misalnya, untuk membatasi pengguna ke folder mereka sendiri di bawah /filetest direktori, masukkan teks berikut di dalam kotak.

```
/filetest/${transfer:UserName}
```

Untuk mempelajari lebih lanjut tentang membuat kebijakan sesi, lihat [Membuat kebijakan sesi untuk bucket Amazon S3](#).

8. Pilih Tambah untuk membuat asosiasi.
9. Pilih server Anda.
10. Pilih Tambahkan akses.
 - Masukkan SID untuk grup.

Note

Untuk informasi tentang cara menemukan SID, lihat [the section called “Sebelum Anda mulai menggunakan AWS Directory Service for Microsoft Active Directory”](#).

11. Pilih Tambahkan akses.

Di bagian Accesses, akses untuk server terdaftar.

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:

External Id	Home directory	Role
S-...	/padbucket3	ADGuy_S3_And_EFS

Below the table, the 'Additional details' section includes an 'Edit' button and information about the logging role, security policy, and server host key.

Menguji pengguna

Anda dapat menguji apakah pengguna memiliki akses ke AWS Managed Microsoft AD direktori untuk server Anda.

Note

Seorang pengguna harus berada dalam satu grup (ID eksternal) yang tercantum di bagian Access pada halaman konfigurasi Endpoint. Jika pengguna tidak berada dalam grup, atau berada di lebih dari satu grup, pengguna tersebut tidak diberikan akses.

Untuk menguji apakah pengguna tertentu memiliki akses

1. Pada halaman detail server, pilih Tindakan, lalu pilih Uji.
2. Untuk pengujian penyedia Identitas, masukkan kredensi masuk untuk pengguna yang berada di salah satu grup yang memiliki akses.
3. Pilih Uji.

Anda melihat tes penyedia identitas yang berhasil, menunjukkan bahwa pengguna yang dipilih telah diberikan akses ke server.

Identity provider testing

User configuration [Info](#)

Username:
Password:

Response:

```

{
  "Response": "
  {\"homeDirectory\":\"/padbucket3\", \"homeDirectoryDetails\":null, \"homeDirectoryType\":\"PATH\", \"posixProfile\",
  \"null\", \"publicKeys\":null, \"role\":\"arn:aws:iam::195886157073:role/ADGuy_53_Aud_EFS\", \"policy\":\"null\", \"userName\": \"transferuser1\", \"identityProviderType\":null, \"userConfigMessage\":null}",
  "StatusCode": 200,
  "Message": ""
}

```

Cancel Test

Jika pengguna termasuk dalam lebih dari satu grup yang memiliki akses, Anda menerima tanggapan berikut.

```

"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."

```

Menghapus akses server untuk grup

Untuk menghapus akses server untuk grup

1. Pada halaman detail server, pilih Tindakan, lalu pilih Hapus Akses.
2. Di kotak dialog, konfirmasikan bahwa Anda ingin menghapus akses untuk grup ini.

Ketika Anda kembali ke halaman detail server, Anda melihat bahwa akses untuk grup ini tidak lagi terdaftar.

Menghubungkan ke server menggunakan SSH (Secure Shell)

Setelah Anda mengkonfigurasi server dan pengguna Anda, Anda dapat terhubung ke server menggunakan SSH dan menggunakan nama pengguna yang sepenuhnya memenuhi syarat untuk pengguna yang memiliki akses.

```
sftp user@active-directory-domain@vpc-endpoint
```

Sebagai contoh:

```
transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-  
svc-987654zyxabc.us-east-1.vpce.amazonaws.com.
```

Format ini menargetkan pencarian federasi, membatasi pencarian Direktori Aktif yang berpotensi besar.

Note

Anda dapat menentukan nama pengguna sederhana. Namun, dalam hal ini, kode Active Directory harus mencari semua direktori di federasi. Ini mungkin membatasi pencarian, dan otentikasi mungkin gagal bahkan jika pengguna harus memiliki akses.

Setelah mengautentikasi, pengguna berada di direktori home yang Anda tentukan saat Anda mengonfigurasi pengguna.

Menghubungkan AWS Transfer Family ke Active Directory yang dikelola sendiri menggunakan hutan dan trust

Directory Service memiliki opsi berikut yang tersedia untuk terhubung ke Direktori Aktif yang dikelola sendiri:

- One-way forest trust (keluar dari AWS Managed Microsoft AD dan masuk untuk Active Directory lokal) hanya berfungsi untuk domain root.
- Untuk domain anak, Anda dapat menggunakan salah satu dari berikut ini:
 - Gunakan kepercayaan dua arah antara Active AWS Managed Microsoft AD Directory dan lokal
 - Gunakan kepercayaan eksternal satu arah untuk setiap domain anak.

Saat menghubungkan ke server menggunakan domain tepercaya, pengguna perlu menentukan domain tepercaya, misalnya `transferuserexample@mycompany.com`.

Menggunakan AWS Directory Service untuk Entra ID Domain Services

Untuk pelanggan yang membutuhkan Transfer SFTP saja, dan tidak ingin mengelola domain, ada Simple Active Directory. Atau, pelanggan yang menginginkan manfaat Active Directory dan ketersediaan tinggi dalam layanan yang dikelola sepenuhnya dapat menggunakan Microsoft AD yang AWS Dikelola. Terakhir, bagi pelanggan yang ingin memanfaatkan hutan Direktori Aktif yang ada untuk Transfer SFTP mereka, ada Konektor Direktori Aktif.

Perhatikan hal-hal berikut:

- Untuk memanfaatkan hutan Active Directory yang ada untuk kebutuhan Transfer SFTP Anda, Anda dapat menggunakan [Active Directory](#) Connector.
- Jika Anda menginginkan manfaat Active Directory dan ketersediaan tinggi dalam layanan yang dikelola sepenuhnya, Anda dapat menggunakannya AWS Directory Service for Microsoft Active Directory. Lihat perinciannya di [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

Topik ini menjelaskan cara menggunakan Konektor Direktori Aktif dan [Layanan Domain Entra ID \(sebelumnya Azure AD\)](#) untuk mengautentikasi pengguna Transfer SFTP dengan ID Entra.

Topik

- [Sebelum Anda mulai menggunakan AWS Directory Service untuk Entra ID Domain Services](#)

- [Langkah 1: Menambahkan Layanan Domain Entra ID](#)
- [Langkah 2: Membuat akun layanan](#)
- [Langkah 3: Menyiapkan AWS Direktori menggunakan AD Connector](#)
- [Langkah 4: Menyiapkan AWS Transfer Family server](#)
- [Langkah 5: Memberikan akses ke grup](#)
- [Langkah 6: Menguji pengguna](#)

Sebelum Anda mulai menggunakan AWS Directory Service untuk Entra ID Domain Services

 Note

AWS Transfer Family memiliki batas default 100 grup Active Directory per server. Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Untuk AWS, Anda memerlukan yang berikut ini:

- Virtual Private Cloud (VPC) di AWS wilayah tempat Anda menggunakan server Transfer Family
- Setidaknya dua subnet pribadi di VPC Anda
- VPC harus memiliki konektivitas internet
- Gateway pelanggan dan gateway pribadi Virtual untuk koneksi VPN situs-ke-situs dengan Microsoft Entra

Untuk Microsoft Entra, Anda memerlukan yang berikut ini:

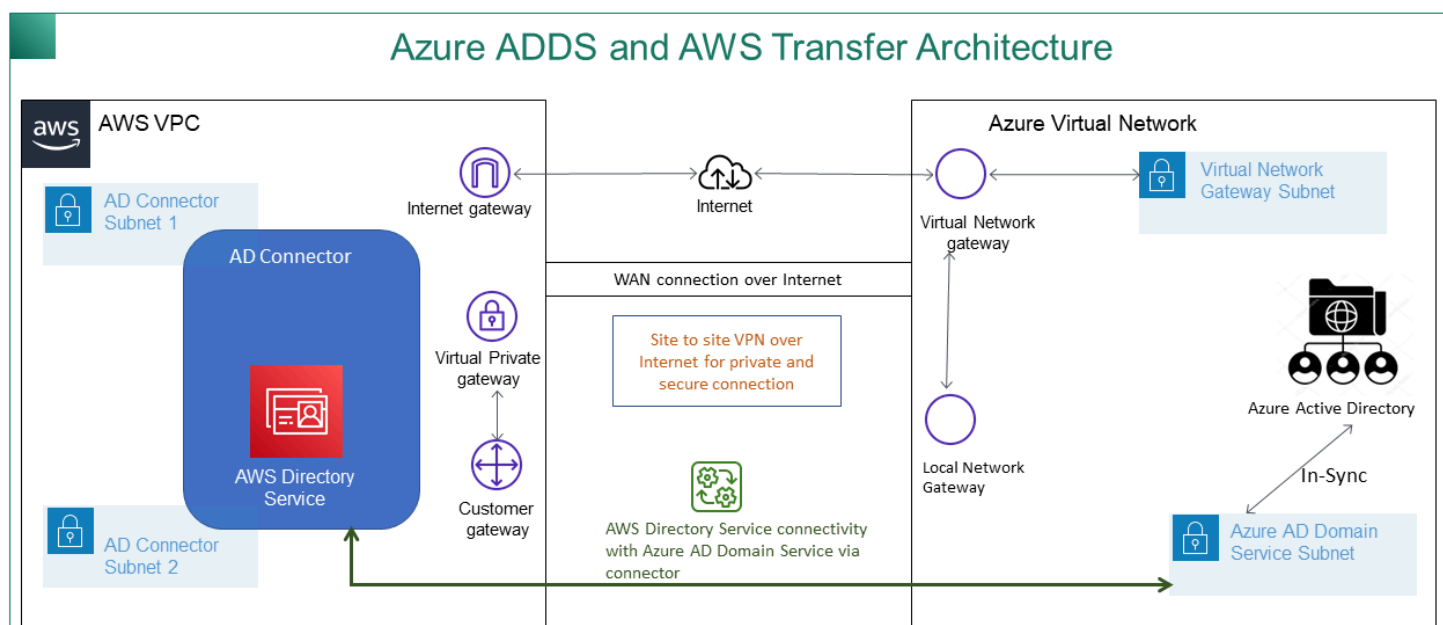
- ID Entra dan layanan domain direktori Aktif
- Grup sumber daya Entra
- Jaringan virtual Entra
- Konektivitas VPN antara VPC Amazon Anda dan grup sumber daya Entra Anda

Note

Ini bisa melalui terowongan IPSEC asli atau menggunakan peralatan VPN. Dalam topik ini, kami menggunakan terowongan IPSEC antara gateway jaringan Virtual Entra dan gateway jaringan lokal. Terowongan harus dikonfigurasi untuk memungkinkan lalu lintas antara titik akhir Layanan Domain Entra Anda dan subnet yang menampung VPC Anda. AWS

- Gateway pelanggan dan gateway pribadi Virtual untuk koneksi VPN situs-ke-situs dengan Microsoft Entra

Diagram berikut menunjukkan konfigurasi yang diperlukan sebelum Anda mulai.



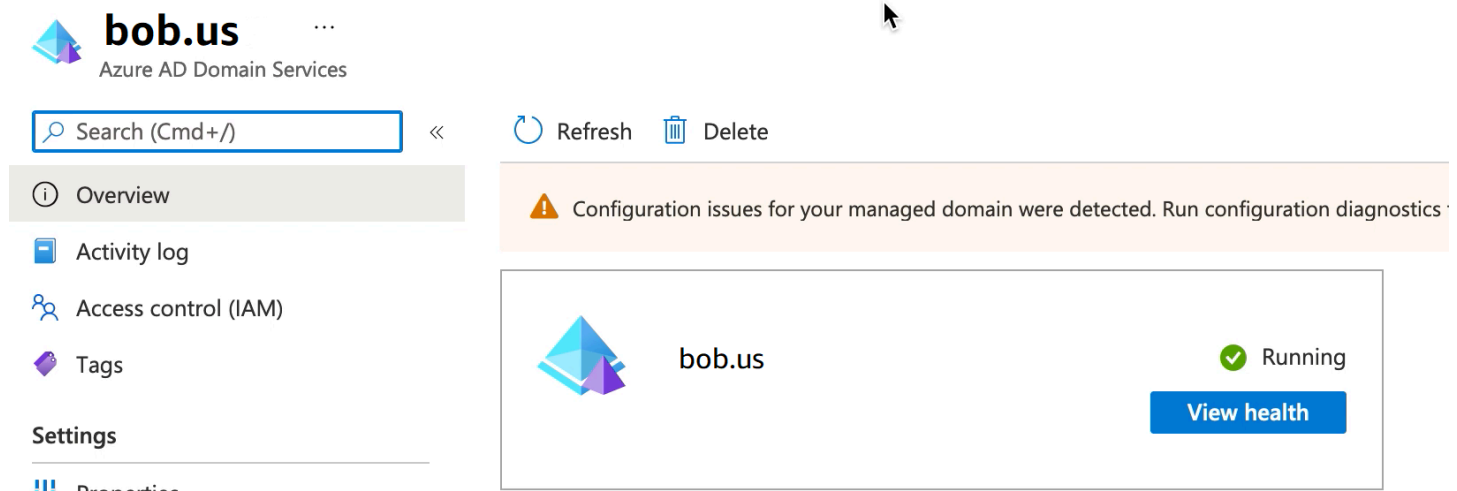
Langkah 1: Menambahkan Layanan Domain Entra ID

Entra ID tidak mendukung instance penggabungan Domain secara default. Untuk melakukan tindakan seperti Gabung Domain, dan untuk menggunakan alat seperti Kebijakan Grup, administrator harus mengaktifkan Layanan Domain ID Entra. Jika Anda belum menambahkan Entra DS, atau implementasi yang ada tidak terkait dengan domain yang ingin digunakan server Transfer SFTP, Anda harus menambahkan instance baru.

Untuk informasi tentang mengaktifkan Layanan Domain ID Entra, lihat [Tutorial: Membuat dan mengonfigurasi domain terkelola Microsoft Entra Domain Services](#).

Note

Saat Anda mengaktifkan Entra DS, pastikan itu dikonfigurasi untuk grup sumber daya dan domain Entra tempat Anda menghubungkan server Transfer SFTP Anda.



Langkah 2: Membuat akun layanan

Entra harus memiliki satu akun layanan yang merupakan bagian dari grup Admin di Entra DS. Akun ini digunakan dengan konektor AWS Active Directory. Pastikan akun ini sinkron dengan Entra DS.

[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



User Sign-ins

30

20

10

0

Oct 10 Oct 17 Oct 24 Oct 31

Group memberships

2

Creation time

10/6/2021, 1:32:27 AM

Identity

Name

bobatusa

First name

Bob

Last name

Smith

User Principal Name

bobsmith@xyz.com

User type

Member

Tip

Multi-factor otentikasi untuk Entra ID tidak didukung untuk server Transfer Family yang menggunakan protokol SFTP. Server Transfer Family tidak dapat menyediakan token MFA setelah pengguna mengautentikasi ke SFTP. Pastikan untuk menonaktifkan MFA sebelum Anda mencoba untuk terhubung.

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

Langkah 3: Menyiapkan AWS Direktori menggunakan AD Connector

Setelah Anda mengonfigurasi Entra DS, dan membuat akun layanan dengan terowongan VPN IPSEC antara AWS VPC dan jaringan Virtual Entra, Anda dapat menguji konektivitas dengan melakukan ping ke alamat IP DNS Entra DS dari instans EC2 mana pun. AWS

Setelah Anda memverifikasi koneksi aktif, Anda dapat melanjutkan di bawah ini.

Untuk mengatur AWS Direktori menggunakan AD Connector

1. Buka konsol [Directory Service](#) dan pilih Directories.
2. Pilih Siapkan direktori.
3. Untuk jenis direktori, pilih AD Connector.
4. Pilih ukuran direktori, pilih Berikutnya, lalu pilih VPC dan Subnet Anda.
5. Pilih Berikutnya, lalu isi kolom sebagai berikut:
 - Nama DNS direktori: masukkan nama domain yang Anda gunakan untuk Entra DS Anda.
 - Alamat IP DNS: masukkan alamat IP Entra DS Anda.
 - Nama pengguna dan kata sandi akun server: masukkan detail untuk akun layanan yang Anda buat di Langkah 2: Buat akun layanan.
6. Lengkapi layar untuk membuat layanan direktori.

Sekarang status direktori harus Aktif, dan siap digunakan dengan server Transfer SFTP.

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

Langkah 4: Menyiapkan AWS Transfer Family server

Buat server Transfer Family dengan protokol SFTP, dan jenis penyedia identitas AWS Directory Service. Dari daftar drop-down Directory, pilih direktori yang Anda tambahkan di Langkah 3: Setup AWS Directory menggunakan AD Connector.

Note

Anda tidak dapat menghapus direktori Microsoft AD di AWS Directory Service jika Anda menggunakannya di server Transfer Family. Anda harus menghapus server terlebih dahulu, dan kemudian Anda dapat menghapus direktori.

Langkah 5: Memberikan akses ke grup

Setelah Anda membuat server, Anda harus memilih grup mana di direktori yang harus memiliki akses untuk mengunggah dan mengunduh file melalui protokol yang diaktifkan menggunakan. AWS Transfer Family Anda melakukan ini dengan membuat akses.

Note

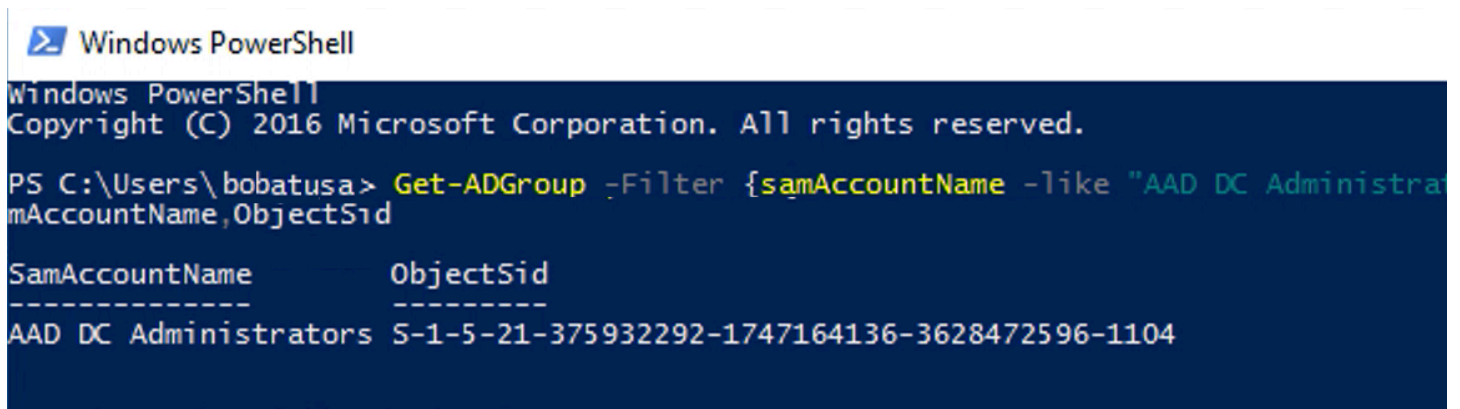
Pengguna harus menjadi bagian langsung dari grup tempat Anda memberikan akses. Misalnya, asumsikan bahwa Bob adalah pengguna dan milik GroupA, dan GroupA sendiri termasuk dalam GroupB.

- Jika Anda memberikan akses ke GroupA, Bob diberikan akses.
- Jika Anda memberikan akses ke GroupB (dan bukan ke GroupA), Bob tidak memiliki akses.

Untuk memberikan akses, Anda perlu mengambil SID untuk grup.

Gunakan PowerShell perintah Windows berikut untuk mengambil SID untuk grup, ganti *YourGroupName* dengan nama grup.

```
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
  
```

Berikan akses ke grup

1. Buka <https://console.aws.amazon.com/transfer/>.
2. Arahkan ke halaman detail server Anda dan di bagian Akses, pilih Tambahkan akses.
3. Masukkan SID yang Anda terima dari output dari prosedur sebelumnya.
4. Untuk Access, pilih AWS Identity and Access Management peran untuk grup.
5. Di bagian Kebijakan, pilih kebijakan. Nilai defaultnya adalah None.
6. Untuk direktori Home, pilih bucket Amazon S3 yang sesuai dengan direktori home grup.
7. Pilih Tambah untuk membuat asosiasi.

Detail dari server Transfer Anda akan terlihat mirip dengan yang berikut ini:

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-bucket	sftp-user-role ↗

Langkah 6: Menguji pengguna

Anda dapat menguji ([Menguji pengguna](#)) apakah pengguna memiliki akses ke AWS Managed Microsoft AD direktori untuk server Anda. Seorang pengguna harus berada dalam satu grup (ID eksternal) yang tercantum di bagian Access pada halaman konfigurasi Endpoint. Jika pengguna tidak berada dalam grup, atau berada di lebih dari satu grup, pengguna tersebut tidak diberikan akses.

Menggunakan direktori logis untuk menyederhanakan struktur direktori Transfer Family Anda

Direktori logis menyederhanakan struktur direktori AWS Transfer Family server Anda. Dengan direktori logis, Anda dapat membuat struktur direktori virtual dengan nama yang mudah digunakan yang dinavigasi pengguna saat menghubungkan ke bucket Amazon S3 atau sistem file Amazon EFS Anda. Ini mencegah pengguna melihat jalur direktori, nama bucket, dan nama sistem file yang sebenarnya.

Note

Anda harus menggunakan kebijakan sesi sehingga pengguna akhir Anda hanya dapat melakukan operasi yang Anda izinkan untuk mereka lakukan.

Anda harus menggunakan direktori logis untuk membuat direktori virtual yang ramah pengguna untuk pengguna akhir Anda dan mengabstraksi nama bucket. Pemetaan direktori logis hanya memungkinkan pengguna untuk mengakses jalur logis dan subdirektori yang ditunjuk, dan melarang jalur relatif yang melintasi akar logis.

Transfer Family memvalidasi setiap jalur yang mungkin menyertakan elemen relatif dan secara aktif memblokir jalur ini agar tidak diselesaikan sebelum kami meneruskan jalur ini ke Amazon S3; ini mencegah pengguna Anda bergerak melampaui pemetaan logisnya.

Meskipun Transfer Family mencegah pengguna akhir mengakses direktori di luar direktori logisnya, kami sarankan Anda juga menggunakan peran unik atau kebijakan sesi untuk menerapkan hak istimewa paling sedikit di tingkat penyimpanan.

Memahami struktur chroot dan direktori

Operasi chroot memungkinkan Anda mengatur direktori root pengguna ke lokasi mana pun dalam hierarki penyimpanan Anda. Ini membatasi pengguna ke direktori home atau root yang dikonfigurasi, mencegah akses ke direktori tingkat yang lebih tinggi.

Pertimbangkan kasus di mana pengguna Amazon S3 terbatas. `amzn-s3-demo-bucket/home/${transfer:UserName}` Tanpa chroot, beberapa klien mungkin mengizinkan pengguna untuk pindah ke `amzn-s3-demo-bucket/home`, memerlukan logout dan login untuk kembali ke direktori yang tepat. Melakukan operasi chroot mencegah masalah ini.

Anda dapat membuat struktur direktori kustom di beberapa bucket dan awalan. Ini berguna jika alur kerja Anda memerlukan tata letak direktori tertentu yang tidak dapat disediakan oleh awalan bucket saja. Anda juga dapat menautkan ke beberapa lokasi yang tidak berdekatan dalam Amazon S3, mirip dengan membuat tautan simbolis dalam sistem file Linux di mana jalur direktori Anda mereferensikan lokasi yang berbeda dalam sistem file.

Aturan untuk menggunakan direktori logis

Bagian ini menjelaskan beberapa aturan dan pertimbangan lain untuk menggunakan direktori logis.

Batas pemetaan

- Hanya satu pemetaan yang diizinkan saat Entry `"/` (tidak ada jalur tumpang tindih yang diizinkan).
- Direktori logis mendukung pemetaan hingga 2,1 MB untuk pengguna IDP dan AD khusus, dan 2.000 entri untuk pengguna yang dikelola layanan. Anda dapat menghitung ukuran pemetaan Anda sebagai berikut:
 1. Tuliskan pemetaan khas dalam format `{"Entry": "/entry-path", "Target": "/target-path"}`, di mana *entry-path* dan *target-path* merupakan nilai aktual yang akan Anda gunakan.
 2. Hitung karakter dalam string itu, lalu tambahkan satu (1).
 3. Kalikan angka itu dengan perkiraan jumlah pemetaan yang Anda miliki untuk server Anda.

Jika jumlah yang Anda perkirakan pada langkah 3 kurang dari 2,1 MB, maka pemetaan Anda berada dalam batas yang dapat diterima.

Persyaratan jalur target

- Gunakan `${transfer:UserName}` variabel jika bucket atau jalur sistem file telah diparameterisasi berdasarkan nama pengguna.

- Target dapat dikonfigurasi untuk menunjuk ke bucket Amazon S3 atau sistem file yang berbeda, selama peran IAM terkait memiliki izin yang diperlukan untuk mengakses lokasi penyimpanan tersebut.
- Semua target harus dimulai dengan garis miring (/) tetapi tidak dapat diakhiri dengan satu. Misalnya, /amzn-s3-demo-bucket/images benar, sementara amzn-s3-demo-bucket/images dan /amzn-s3-demo-bucket/images/ tidak.

Pertimbangan penyimpanan

- Amazon S3 adalah toko objek di mana folder hanya ada sebagai konsep virtual. Saat menggunakan penyimpanan Amazon S3, Transfer Family melaporkan awalan sebagai direktori dalam operasi STAT, meskipun tidak ada objek zero-byte dengan garis miring. Objek zero-byte yang tepat dengan garis miring juga dilaporkan sebagai direktori dalam operasi STAT. Perilaku ini dijelaskan dalam [Mengatur objek di konsol Amazon S3 menggunakan folder](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- Untuk aplikasi yang perlu membedakan antara file dan folder, gunakan Amazon Elastic File System (Amazon EFS) sebagai opsi penyimpanan Transfer Family Anda.
- Jika Anda menentukan nilai direktori logis untuk pengguna Anda, parameter yang Anda gunakan bergantung pada jenis pengguna:
 - Untuk pengguna yang dikelola layanan, berikan nilai direktori logis di `HomeDirectoryMappings`
 - Untuk pengguna penyedia identitas kustom, berikan nilai direktori logis di `diHomeDirectoryDetails`.

Nilai direktori pengguna

- Parameter untuk menentukan nilai direktori logis tergantung pada jenis pengguna Anda:
 - Untuk pengguna yang dikelola layanan, berikan nilai direktori logis di `HomeDirectoryMappings`
 - Untuk pengguna penyedia identitas kustom, berikan nilai direktori logis di `diHomeDirectoryDetails`.
- Saat menggunakan LOGICAL HomeDirectoryType, Anda dapat menentukan HomeDirectory nilai untuk pengguna yang Dikelola Layanan, akses Direktori Aktif, dan implementasi Penyedia

Identitas Kustom HomeDirectoryDetails yang disediakan dalam respons. Jika tidak ditentukan, HomeDirectory default ke. /

Untuk detail tentang cara menerapkan direktori logis, lihat [Menerapkan direktori logis](#).

Menerapkan direktori logis

Important

Persyaratan direktori root

- Jika Anda tidak menggunakan pengaturan optimasi kinerja Amazon S3 direktori root Anda harus ada saat startup.
- Untuk Amazon S3, ini berarti membuat objek zero-byte yang diakhiri dengan garis miring (/).
- Untuk menghindari persyaratan ini, pertimbangkan untuk mengaktifkan pengoptimalan kinerja Amazon S3 saat Anda membuat atau memperbarui server.
- Saat menentukan HomeDirectory dengan LOGICAL HomeDirectoryType, nilainya harus dipetakan ke salah satu pemetaan direktori logis Anda. Layanan memvalidasi ini selama pembuatan dan pembaruan pengguna untuk mencegah konfigurasi yang tidak berfungsi.

Konfigurasi direktori home logis

Saat menggunakan LOGICAL sebagai milik Anda HomeDirectoryType, perhatikan hal berikut:

- HomeDirectory Nilai harus sesuai dengan salah satu pemetaan direktori logis yang ada.
- Sistem secara otomatis memvalidasi ini selama pembuatan dan pembaruan pengguna.
- Validasi ini mencegah konfigurasi yang akan menyebabkan masalah akses.

Aktifkan direktori logis

Untuk menggunakan direktori logis untuk pengguna, atur HomeDirectoryType parameter ke LOGICAL. Lakukan ini saat Anda membuat pengguna baru atau memperbarui pengguna yang sudah ada.

```
"HomeDirectoryType": "LOGICAL"
```

Aktifkan **chroot** untuk pengguna

Untuk **chroot**, buat struktur direktori yang terdiri dari satu Entry dan Target pasangan untuk setiap pengguna. Entri/mewakili folder root, sedangkan Target menentukan lokasi sebenarnya di bucket atau sistem file Anda.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

Anda dapat menggunakan jalur absolut seperti pada contoh sebelumnya, atau Anda dapat menggunakan substitusi dinamis untuk nama pengguna dengan `${transfer:UserName}`, seperti pada contoh berikut.

```
[{"Entry": "/", "Target":  
"/amzn-s3-demo-bucket/${transfer:UserName}"}]
```

Dalam contoh sebelumnya, pengguna dikunci ke direktori root mereka dan tidak dapat melintasi lebih tinggi dalam hierarki.

Struktur direktori virtual

Untuk struktur direktori virtual, Anda dapat membuat beberapa Entry Target pasangan, dengan target di mana saja di bucket S3 atau sistem file EFS Anda, termasuk di beberapa bucket atau sistem file, selama pemetaan peran IAM pengguna memiliki izin untuk mengaksesnya.

Dalam contoh struktur virtual berikut, ketika pengguna login ke AWS SFTP, mereka berada di direktori root dengan sub-direktori/pics,,, /doc dan. /reporting /anotherpath/subpath/financials

Note

Kecuali Anda memilih untuk mengoptimalkan kinerja untuk direktori Amazon S3 Anda (saat Anda membuat atau memperbarui server), baik pengguna atau administrator perlu membuat

direktori jika belum ada. Menghindari masalah ini adalah alasan untuk mempertimbangkan mengoptimalkan kinerja Amazon S3.

Untuk Amazon EFS, Anda masih memerlukan administrator untuk membuat pemetaan logis atau direktori. /

```
[
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/financials"}]
```

Note

Anda hanya dapat mengunggah file ke folder tertentu yang Anda petakan. Ini berarti bahwa dalam contoh sebelumnya, Anda tidak dapat mengunggah ke `/anotherpath` atau `anotherpath/subpath` direktori; hanya `anotherpath/subpath/financials`. Anda juga tidak dapat memetakan ke jalur tersebut secara langsung, karena jalur yang tumpang tindih tidak diperbolehkan.

Misalnya, asumsikan Anda membuat pemetaan berikut:

```
{
  "Entry": "/pics",
  "Target": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

Anda hanya dapat mengunggah file ke bucket tersebut. Ketika Anda pertama kali terhubung `ftp`, Anda diijinkan ke direktori root, `/`. Jika Anda mencoba mengunggah file ke direktori itu, unggahan gagal. Perintah berikut menunjukkan urutan contoh:

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

Untuk mengunggah ke salah satu `directory`/sub-`directory`, Anda harus secara eksplisit memetakan jalur ke sub-`directory`.

Untuk informasi selengkapnya tentang mengonfigurasi direktori logis dan chroot untuk pengguna Anda, termasuk AWS CloudFormation templat yang dapat Anda unduh dan gunakan, lihat [Menyederhanakan Struktur AWS SFTP Anda dengan direktori chroot dan logis](#) di Blog Penyimpanan. AWS

Konfigurasi contoh direktori logis

Dalam contoh ini, kami membuat pengguna dan menetapkan dua direktori logis. Perintah berikut membuat pengguna baru (untuk server Transfer Family yang ada) dengan direktori logis `pics` dan `doc`.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Jika **marymajor** adalah pengguna yang sudah ada dan jenis direktori home nya `PATH`, Anda dapat mengubahnya `LOGICAL` dengan perintah yang sama seperti yang sebelumnya.

```
aws transfer update-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
```

```
--home-directory-mappings "[{"Entry\\":\\"/pics\\", \"Target\\":\\"/amzn-s3-demo-bucket1/pics\\"}, {"Entry\\":\\"/doc\\", \"Target\\":\\"/amzn-s3-demo-bucket2/test/mydocs\\"}]"
```

Perhatikan hal-hal berikut:

- Jika direktori `/amzn-s3-demo-bucket1/pics` dan `/amzn-s3-demo-bucket2/test/mydocs` belum ada, pengguna (atau administrator) perlu membuatnya.

Note

Direktori ini dibuat secara otomatis oleh server Transfer Family jika Anda telah mengonfigurasi direktori yang dioptimalkan.

- Ketika **marymajor** terhubung ke server, dan menjalankan `ls -l` perintah, Mary melihat yang berikut:

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor** tidak dapat membuat file atau direktori apa pun pada level ini. Namun, di dalam `pics` dan `doc`, dia dapat menambahkan sub-direktori.
- File yang ditambahkan Mary `pics` dan `doc` ditambahkan ke jalur Amazon S3 `/amzn-s3-demo-bucket1/pics` dan `/amzn-s3-demo-bucket2/test/mydocs` masing-masing.
- Dalam contoh ini, kami menentukan dua ember berbeda untuk menggambarkan kemungkinan itu. Namun, Anda dapat menggunakan bucket yang sama untuk beberapa atau semua direktori logis yang Anda tentukan untuk pengguna.

Contoh ini menyediakan konfigurasi alternatif untuk jalur rumah logis.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory /home/marymajor \
  --home-directory-mappings "[{"Entry\\":\\"/home/marymajor/pics\\", \"Target\\":\\"/amzn-s3-demo-bucket1/pics\\"}, {"Entry\\":\\"/home/marymajor/doc\\", \"Target\\":\\"/amzn-s3-demo-bucket2/test/mydocs\\"}]" \
```



```
--ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Perhatikan hal-hal berikut:

- Pemetaan menyediakan jalur umum/home/marymajor, yang merupakan bagian pertama dari dua jalur logis. File kemudian dapat ditambahkan ke doc folder pics dan.
- Seperti pada contoh sebelumnya, direktori home,/home/marymajor, adalah read-only.

Konfigurasikan direktori logis untuk Amazon EFS

Jika server Transfer Family Anda menggunakan Amazon EFS, direktori home untuk pengguna harus dibuat dengan akses baca dan tulis sebelum pengguna dapat bekerja di direktori home logisnya. Pengguna tidak dapat membuat direktori ini sendiri, karena mereka akan kekurangan izin untuk `mkdir` direktori home logis mereka.

Jika direktori home pengguna tidak ada, dan mereka menjalankan `ls` perintah, sistem merespons sebagai berikut:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Seorang pengguna dengan akses administratif ke direktori induk perlu membuat direktori home logis pengguna.

AWS Lambda Tanggapan khusus

Anda dapat menggunakan direktori logis dengan fungsi Lambda yang terhubung ke penyedia identitas kustom Anda. Untuk melakukannya, dalam fungsi Lambda Anda, Anda menentukan `HomeDirectoryType` sebagai **LOGICAL**, dan menambahkan `Entry` dan `Target` nilai untuk parameter. `HomeDirectoryDetails` Contoh:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{"Entry": "\\", \"Target\": \"/amzn-s3-demo-bucket/
theRealFolder"}]"
```

Kode berikut adalah contoh respons yang berhasil dari panggilan otentikasi Lambda kustom.

```
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": "{\n\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",
    \n\"HomeDirectoryType\": \"LOGICAL\",
    \n\"HomeDirectoryDetails\": \"[{\\\"Entry\\\":\\\"/myhome\\\",\\\"
\\\"Target\\\":\\\"/amzn-s3-demo-bucket/theRealFolder\\\"]\\\",
    \n\"PublicKeys\": \"[ssh-rsa myrsapubkey]\"",
  "StatusCode": 200
}
```

Note

"Url": Baris dikembalikan hanya jika Anda menggunakan metode API Gateway sebagai penyedia identitas kustom Anda.

Akses fsX Anda untuk sistem file NetApp ONTAP dengan Transfer Family

Daftar Isi

- [Ikhtisar](#)
- [Prasyarat](#)
 - [FSx untuk NetApp persyaratan ONTAP](#)
 - [Izin IAM yang diperlukan](#)
- [Bagaimana penyimpanan FSx bekerja dengan Transfer Family](#)
 - [Identitas pengguna sistem file](#)
- [Membuat titik akses S3 untuk FSx](#)
 - [Penamaan titik akses](#)
 - [Membuat titik akses untuk FSx untuk ONTAP NetApp](#)
 - [Mengkonfigurasi izin sistem file](#)
- [Menggunakan alias titik akses S3 dengan FSx](#)

- [Tentang alias titik akses](#)
- [Menemukan alias titik akses Anda](#)
- [Mengkonfigurasi Transfer Family untuk penyimpanan FSx](#)
 - [Membuat peran IAM](#)
- [Mengelola pengguna untuk penyimpanan FSx](#)
 - [Membuat pengguna](#)
 - [Mengkonfigurasi beberapa pemetaan direktori](#)
- [Mengkonfigurasi klien transfer file](#)
 - [Konfigurasi WinSCP](#)
 - [Klien SFTP lainnya](#)
- [Memecahkan masalah penyimpanan FSx](#)
 - [Masalah operasi file](#)

Ikhtisar

Transfer Family mendukung Amazon FSx untuk NetApp ONTAP melalui jalur akses S3. Amazon FSx untuk NetApp ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja tinggi, dan kaya fitur yang dibangun di atas sistem file ONTAP yang populer. NetApp Saat Anda mengonfigurasi Transfer Family dengan sistem file FSx, pengguna Anda terhubung ke titik akhir Transfer Family menggunakan klien transfer file standar. Transfer Family merutekan operasi file melalui jalur akses S3 yang dilampirkan ke volume FSx Anda, sementara data Anda tetap berada di sistem file FSx. Untuk mempelajari lebih lanjut tentang fsX untuk NetApp ONTAP, lihat [Apa itu Amazon FSx untuk ONTAP?](#) NetApp

Integrasi ini memungkinkan Anda untuk:

- Transfer file menggunakan protokol SFTP, FTPS, atau FTP ke penyimpanan file kelas perusahaan
- Akses data yang sama melalui beberapa protokol (SFTP, NFS, SMB)
- Gunakan fitur fsX seperti snapshot, backup, dan tiering data

Important

Beberapa operasi file tidak didukung saat menggunakan sistem file FSx dengan Transfer Family, termasuk mengganti nama dan menambahkan operasi. Untuk operasi unggahan,

ukuran file dibatasi hingga 5 GB. Untuk daftar lengkap batasan, lihat [Kompatibilitas titik akses](#).

Prasyarat

Sebelum Anda mengonfigurasi Transfer Family dengan Amazon FSx, Anda harus memenuhi persyaratan berikut.

FSx untuk NetApp persyaratan ONTAP

Untuk menggunakan FSx untuk NetApp ONTAP dengan Transfer Family, Anda memerlukan:

- Sebuah fsX untuk sistem file ONTAP yang menjalankan NetApp ONTAP versi 9.17.1 atau yang lebih baru
- Sistem file dan titik akses S3 di Wilayah yang sama AWS
- AWS Akun yang sama yang memiliki sistem file dan titik akses

Untuk mempelajari lebih lanjut, lihat [Memulai Amazon FSx untuk NetApp](#) ONTAP.

Izin IAM yang diperlukan

Anda dapat mengonfigurasi setiap titik akses S3 dengan izin dan kontrol jaringan yang berbeda yang diterapkan S3 untuk setiap permintaan yang dibuat menggunakan jalur akses tersebut. Jalur akses S3 mendukung kebijakan sumber daya IAM yang dapat Anda gunakan untuk mengontrol penggunaan titik akses berdasarkan sumber daya, pengguna, atau kondisi lainnya. Untuk aplikasi atau pengguna untuk mengakses file melalui titik akses, baik titik akses dan volume yang mendasarinya harus mengizinkan permintaan. Untuk informasi selengkapnya, lihat [kebijakan jalur akses IAM](#).

Jalur akses Amazon S3 untuk FSx menggunakan model otorisasi lapisan ganda yang menggabungkan izin IAM dengan izin tingkat sistem file. Pendekatan ini memastikan bahwa permintaan akses data diotorisasi dengan benar pada tingkat AWS layanan dan tingkat sistem file yang mendasarinya.

Agar aplikasi atau pengguna berhasil mengakses data melalui titik akses, kebijakan jalur akses S3 dan volume FSx yang mendasarinya harus mengizinkan permintaan tersebut.

Untuk membuat dan mengonfigurasi integrasi ini, Anda memerlukan izin berikut:

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(jika membuat kebijakan jalur akses opsional)

Bagaimana penyimpanan FSx bekerja dengan Transfer Family

Saat Anda mengonfigurasi Transfer Family dengan sistem file FSx, komponen berikut bekerja sama untuk mengaktifkan transfer file:

1. Pengguna terhubung ke server Transfer Family menggunakan klien SFTP, FTPS, atau FTP.
2. Transfer Family mengautentikasi pengguna menggunakan identitas yang dikelola layanan, penyedia identitas kustom, atau AWS Directory Service for Microsoft Active Directory. Setelah diautentikasi, Transfer Family mengasumsikan peran IAM yang terkait dengan pengguna.
3. Untuk setiap operasi file, Transfer Family bertindak sebagai klien API S3 standar, membuat permintaan ke Titik Akses S3 menggunakan peran IAM pengguna yang diasumsikan dan memverifikasi izin terhadap kebijakan jalur akses S3.
4. Sistem file FSx memverifikasi bahwa pengguna sistem file yang terkait dengan titik akses memiliki izin untuk melakukan operasi yang diminta. Operasi file kemudian dilakukan pada volume FSx.

Agar operasi file berhasil, kedua lapisan otorisasi harus mengizinkan permintaan.

Note

Melampirkan titik akses S3 ke volume FSx tidak mengubah bagaimana volume berperilaku ketika diakses langsung melalui NFS atau SMB. Akses protokol file yang ada terus bekerja tidak berubah.

Identitas pengguna sistem file

Setiap titik akses menggunakan identitas pengguna sistem file yang Anda tentukan saat membuat titik akses. Identitas ini mengotorisasi semua permintaan akses file yang dibuat melalui titik akses itu. Pengguna sistem file adalah akun pengguna pada sistem file Amazon FSx yang mendasarinya. Jika pengguna sistem file memiliki akses hanya-baca, maka hanya permintaan baca yang dibuat menggunakan titik akses yang diotorisasi, dan permintaan tulis diblokir. Jika pengguna sistem

file memiliki akses baca-tulis, maka permintaan baca dan tulis ke volume terlampir yang dibuat menggunakan titik akses diotorisasi.

Membuat titik akses S3 untuk FSx

Sebelum Anda mengkonfigurasi Transfer Family, Anda harus membuat titik akses S3 yang dilampirkan ke volume FSx Anda. Titik akses S3 diberi nama titik akhir jaringan yang dilampirkan ke sumber data seperti bucket atau Amazon FSx untuk volume ONTAP. Anda dapat membuat dan melampirkan jalur akses ke FSx untuk NetApp ONTAP menggunakan konsol Amazon FSx, AWS CLI, atau API. Setelah dilampirkan, Anda dapat menggunakan API objek S3 untuk mengakses data file Anda. Data Anda terus berada di sistem file Amazon FSx dan terus dapat diakses langsung untuk beban kerja Anda yang ada. Anda terus mengelola penyimpanan Anda menggunakan semua fsX untuk kemampuan manajemen penyimpanan NetApp ONTAP, termasuk backup, snapshot, kuota pengguna dan grup, dan kompresi.

Untuk informasi selengkapnya, lihat [Membuat titik akses](#).

Penamaan titik akses

Saat Anda memberi nama jalur akses Anda, ikuti panduan ini:

- Nama titik akses harus unik dalam AWS akun dan Wilayah Anda.
- Nama tidak dapat diakhiri dengan `-ext-s3alias` (dicadangkan untuk alias).
- Hindari memasukkan informasi sensitif dalam nama karena dipublikasikan di DNS.

Untuk daftar lengkap aturan penamaan, lihat Aturan, [batasan, dan batasan penamaan titik akses](#).

Membuat titik akses untuk FSx untuk ONTAP NetApp

Gunakan prosedur berikut untuk membuat jalur akses S3 untuk FSx NetApp untuk volume ONTAP.

Untuk membuat titik akses (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>
2. Di panel navigasi, pilih Sistem file.
3. Pilih fsX Anda untuk sistem file NetApp ONTAP.
4. Pilih tab Volume.
5. Pilih volume yang ingin Anda lampirkan.

6. Untuk Tindakan, pilih Buat titik akses S3.
7. Untuk nama Access point, masukkan nama deskriptif (misalnya, transfer-family-ap).
8. Untuk tipe identitas pengguna sistem File, pilih salah satu dari berikut ini:
 - Identitas UNIX - Untuk volume dengan gaya keamanan UNIX
 - Identitas Windows - Untuk volume dengan gaya keamanan NTFS
9. (Opsional) Untuk kebijakan Access point, masukkan kebijakan IAM yang menentukan prinsipal IAM mana yang dapat melakukan operasi pada objek yang diakses melalui jalur akses ini. Untuk informasi selengkapnya, lihat [Mengelola akses titik akses](#).
10. Pilih Buat.
11. Setelah pembuatan, perhatikan alias titik akses untuk digunakan dalam konfigurasi Transfer Family.

Note

Saat AWS Transfer Family mengakses sumber daya S3 atas nama SFTP/FTPS pengguna Anda yang terhubung, permintaan berasal dari AWS Transfer Family infrastruktur, bukan dari VPC Anda. Karena itu, Titik Akses S3 yang dikonfigurasi dengan asal jaringan VPC akan menolak permintaan ini. Namun, bahkan jika Anda menggunakan Access Point yang dikonfigurasi dengan asal jaringan Internet, semua lalu lintas antara Transfer Family dan Access Point tetap pribadi dan melakukan perjalanan melalui jaringan AWS backbone - itu tidak melintasi internet publik.

Mengkonfigurasi izin sistem file

Pengguna sistem file yang Anda tentukan menentukan operasi apa yang dapat dilakukan pengguna Transfer Family. Anda harus mengonfigurasi izin yang sesuai pada volume FSx Anda.

Contoh UNIX:

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users
```

```
# Set permissions
chmod 755 /vol1/transfer-users
```

Contoh Windows:

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Menggunakan alias titik akses S3 dengan FSx

Saat Anda menggunakan sistem file FSx dengan Transfer Family, Anda harus menggunakan alias titik akses S3. Transfer Family tidak mendukung penggunaan ARN titik akses atau metode referensi lainnya untuk penyimpanan FSx.

Important

AWS Transfer Family hanya mendukung alias titik akses S3 saat menggunakan sistem file FSx. Anda tidak dapat menggunakan ARN titik akses atau URI bergaya host virtual.

Important

Titik akses harus berada di Wilayah yang sama dengan volume.

Tentang alias titik akses

Saat Anda membuat titik akses S3 yang dilampirkan ke volume FSx, Amazon S3 secara otomatis menghasilkan alias titik akses. Alias ini adalah pengenalan unik yang dapat Anda gunakan di mana pun Anda menggunakan nama bucket S3.

Untuk titik akses yang dilampirkan ke volume FSx, alias menggunakan format berikut:


```
access-point-name-metadata-ext-s3alias
```

Contoh alias:

```
my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias
```

 Note

-ext-s3alias Akhirnya dicadangkan untuk alias titik akses FSx. Anda tidak dapat menggunakan akhiran ini dalam nama titik akses.

Menemukan alias titik akses Anda

Anda dapat menemukan alias titik akses setelah membuat titik akses.

Untuk menemukan alias titik akses (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>
2. Di panel navigasi, pilih Sistem file.
3. Pilih sistem file Anda.
4. Pilih tab Volume dan pilih volume yang Anda buat untuk titik akses.
5. Buka kolom detail titik akses S3.
6. Alias ditampilkan di kolom Alias.

Untuk menemukan alias titik akses (CLI)

Gunakan perintah `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Tanggapan termasuk alias:

```
{
  "S3AccessPointAttachments": [
    {
      "S3AccessPoint": {
```

```
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-  
ap",  
        "Alias": "my-fsx-ap-aqfqprinstn7aefdfbarligizwgyfouse1a-ext-s3alias"  
    }  
]  
}
```

Saat Anda mengonfigurasi pengguna Transfer Family, gunakan alias access point di pemetaan direktori home.

Format direktori rumah:

```
/access-point-alias/path/to/directory
```

Contoh:

```
/my-fsx-ap-aqfqprinstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith
```

Mengkonfigurasi Transfer Family untuk penyimpanan FSx

Setelah Anda membuat titik akses S3, konfigurasikan server Transfer Family untuk menggunakannya.

Membuat peran IAM

Anda harus membuat peran IAM yang memberikan akses Transfer Family ke jalur akses S3.

Important

Kebijakan IAM memerlukan format ARN Access Point, bukan alias. Gunakan format `arn:aws:s3:region:account-id:accesspoint/access-point-name` dalam pernyataan Sumber daya kebijakan IAM Anda. Alias access point (diakhiri dengan `-ext-s3alias`) hanya digunakan untuk pemetaan direktori home.

Untuk membuat peran IAM

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, pilih Peran, lalu pilih Buat peran.

3. Untuk jenis entitas Tepercaya, pilih AWS layanan.
4. Untuk kasus penggunaan, pilih Transfer.
5. Pilih Berikutnya.
6. Pilih Buat kebijakan dan masukkan kebijakan Anda (lihat contoh kebijakan di bawah).
7. Lampirkan kebijakan ke peran dan pilih Buat peran.

Contoh kebijakan IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/
object/*"
    },
    {
      "Sid": "AllowDirectoryOperations",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"
    }
  ]
}
```

Mengelola pengguna untuk penyimpanan FSx

Buat pengguna Transfer Family dengan pemetaan direktori home yang menggunakan alias access point S3.

Membuat pengguna

Saat Anda membuat pengguna untuk penyimpanan FSx, gunakan alias titik akses di pemetaan direktori home.

Untuk membuat pengguna yang Dikelola Layanan (konsol)

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih server Anda.
4. Di bagian Pengguna, pilih Tambah pengguna.
5. Untuk Nama Pengguna, masukkan nama pengguna.
6. Untuk Peran, pilih peran IAM yang Anda buat.
7. Untuk direktori Home, pilih Restricted.
8. Untuk pemetaan direktori Home, tambahkan pemetaan menggunakan alias access point:

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith"}]
```

Untuk membuat pengguna (CLI)

Gunakan perintah `create-user`. Ganti alias titik akses dengan alias Anda.

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith"  
    }  
  ]'
```

Mengkonfigurasi beberapa pemetaan direktori

Anda dapat memetakan beberapa direktori virtual ke jalur yang berbeda pada volume FSx.

Contoh: Direktori upload dan download terpisah

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/inbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/inbox"  
    },  
    {  
      "Entry": "/outbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/outbox"  
    }  
  ]'
```

Mengkonfigurasi klien transfer file

Saat menggunakan sistem file FSx dengan Transfer Family, Anda harus mengonfigurasi klien transfer file Anda untuk menonaktifkan fitur yang tidak didukung.

Konfigurasi WinSCP

WinSCP menggunakan fitur ganti nama sementara secara default yang tidak didukung dengan jalur akses S3 untuk FSx.

Warning

Jika Anda tidak menonaktifkan fitur ganti nama sementara di WinSCP, unggahan file akan gagal.

Untuk menonaktifkan penggantian nama sementara di WinSCP

1. Buka WinSCP.
2. Pada dialog Login, pilih Edit untuk mengubah pengaturan sesi Anda.
3. Pilih Lanjutan.
4. Di navigasi kiri, di bawah Transfer, pilih Endurance.
5. Untuk Aktifkan transfer resume/transfer ke nama file sementara, pilih Nonaktifkan.
6. Pilih OK untuk menyimpan pengaturan.

Atau, Anda dapat menonaktifkan pengaturan ini untuk sesi yang ada:

1. Connect ke server Transfer Family Anda.
2. Pilih Opsi, lalu Preferensi.
3. Pilih Transfer, lalu Daya Tahan.
4. Untuk Aktifkan transfer resume/transfer ke nama file sementara, pilih Nonaktifkan.
5. Pilih OK.

Klien SFTP lainnya

Untuk klien SFTP lainnya, nonaktifkan fitur berikut jika tersedia:

- Unggahan file sementara (unggah ke file temp, lalu ganti nama)
- Lanjutkan transfer menggunakan file sementara
- Unggahan atom menggunakan operasi ganti nama
- Menambahkan mode untuk upload

Konsultasikan dokumentasi klien Anda untuk langkah-langkah konfigurasi tertentu.

Memecahkan masalah penyimpanan FSx

Bagian ini menjelaskan cara mengidentifikasi dan menyelesaikan masalah umum saat menggunakan Transfer Family dengan sistem file FSx.

Masalah operasi file

Izin ditolak

Jika Anda menerima kesalahan izin ditolak:

1. Verifikasi peran IAM memiliki izin yang benar untuk alias titik akses. Anda dapat melakukan ini dengan menguji langsung dengan API S3.
2. Periksa apakah kebijakan titik akses memungkinkan peran IAM.
3. Verifikasi bahwa pengguna sistem file memiliki izin pada jalur target.
4. Konfirmasikan pemetaan direktori home menggunakan alias access point yang benar.

Unggahan gagal dengan WinSCP

Jika unggahan file gagal dengan WinSCP, nonaktifkan penggantian nama sementara:

1. Di WinSCP, pilih Opsi, lalu Preferensi.
2. Pilih Transfer, lalu Daya Tahan.
3. Untuk Aktifkan transfer resume/transfer ke nama file sementara, pilih Nonaktifkan.

Untuk informasi selengkapnya, lihat [the section called “Mengkonfigurasi klien transfer file”](#).

Unggahan file gagal

Jika unggahan file gagal:

1. Verifikasi ukuran file di bawah 5 GB.
2. Periksa apakah volume FSx memiliki penyimpanan yang tersedia cukup.
3. Pantau CloudWatch metrik untuk pelambatan.

Aplikasi web Transfer Family

Anda dapat membuat aplikasi web untuk mengaktifkan antarmuka sederhana untuk mentransfer data ke dan dari Amazon Simple Storage Service (S3) melalui browser web. Ini tidak mengharuskan Anda untuk membuat atau menyediakan AWS Transfer Family server.

Sebelum memperkenalkan aplikasi web Transfer Family, pengguna akhir harus menggunakan klien, custom-built, atau solusi pihak ketiga untuk mengakses data mereka di Amazon S3. Ini karena persyaratan keamanan yang ketat untuk pelanggan dan mitra, dan karena aplikasi klien menantang bagi pengguna non-teknis untuk beroperasi.

Dengan peluncuran aplikasi web, Anda sekarang dapat memperluas portal bermerek, aman, dan sangat tersedia bagi pengguna akhir Anda untuk menelusuri, mengunggah, dan mengunduh data di Amazon S3. Aplikasi web terintegrasi secara native dengan AWS IAM Identity Center dan Amazon S3 Access Grants. Ini berarti bahwa hanya pengguna yang diautentikasi yang dapat melihat data yang diizinkan untuk diakses. Aplikasi web dibuat menggunakan [Browser Penyimpanan untuk Amazon S3](#) dan menawarkan fungsionalitas pengguna akhir yang sama dalam penawaran yang dikelola sepenuhnya tanpa harus menulis kode atau meng-host aplikasi Anda sendiri.

Untuk informasi selengkapnya tentang aplikasi lain Layanan AWS yang Anda gunakan dengan aplikasi web Transfer Family, lihat dokumentasi berikut:

- [Mengelola akses dengan S3 Access Grants di Panduan Pengguna Amazon Simple Storage Service](#)
- [AWS IAM Identity Center Panduan Pengguna](#)
- [Lokakarya Hibah Akses Amazon S3](#)
- [Mengumumkan aplikasi AWS Transfer Family web untuk transfer file Amazon S3 yang dikelola sepenuhnya](#)

Sumber daya berikut tersedia untuk membantu Anda memulai aplikasi web Transfer Family.

- Panduan pengguna menawarkan panduan langkah demi langkah terperinci untuk menyiapkan aplikasi web Transfer Family di sini: [Tutorial: Menyiapkan aplikasi web Transfer Family dasar](#)
- Pusat Sumber Daya AWS Memulai menawarkan tutorial di sini: [Memulai dengan aplikasi AWS Transfer Family web](#).
- Lihat [Memulai dengan aplikasi AWS Transfer Family web](#).

Wilayah AWS untuk aplikasi web Transfer Family

AWS Transfer Family aplikasi web tersedia di semua wilayah yang didukung Transfer Family, sebagaimana tercantum dalam [Tabel AWS Wilayah](#), kecuali untuk Asia Pasifik (Selandia Baru) AWS European Sovereign Cloud dan.

Titik akhir VPC untuk aplikasi web didukung di semua Wilayah AWS tempat aplikasi web tersedia.

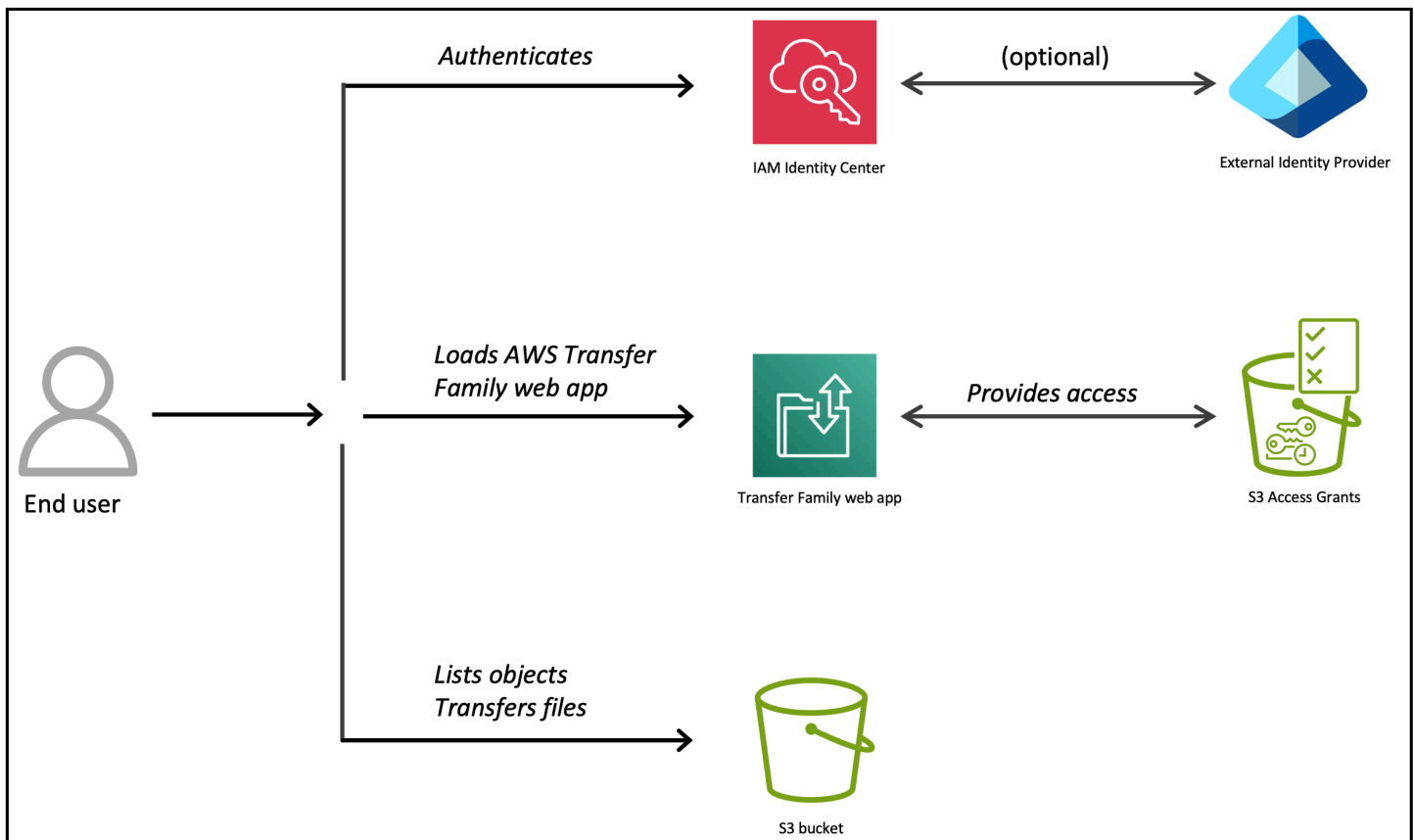
Kompatibilitas browser untuk aplikasi AWS Transfer Family web

Aplikasi web Transfer Family mendukung browser berikut.

Peramban	Versi	Kompatibilitas
Microsoft Edge	3 versi terbaru	Kompatibel
Mozilla Firefox	3 versi terbaru	Kompatibel
Google Chrome	3 versi terbaru	Kompatibel
Apple Safari	3 versi terbaru	Kompatibel

Cara membuat aplikasi web Transfer Family

Diagram berikut mengilustrasikan arsitektur aplikasi web Transfer Family.



Berdasarkan diagram, Anda dapat melihat bahwa aplikasi web Transfer Family berinteraksi dengan yang berikut Layanan AWS:

- Amazon S3 untuk penyimpanan dan Hibah Akses Amazon S3 untuk memperoleh kredensial sesi.
- AWS IAM Identity Center sebagai penyedia identitas federasi.
- Amazon CloudFront jika Anda mengonfigurasi URL khusus untuk aplikasi web Anda.

Perhatikan batasan berikut saat menggunakan aplikasi web.

- Jumlah maksimum hasil pencarian per kueri: 10.000
- Bucket Amazon S3 yang digunakan oleh aplikasi web Transfer Family harus berada di akun yang sama dengan aplikasi web itu sendiri. Cross-account bucket saat ini tidak didukung.
- Luas pencarian maksimum per kueri: 10.000 file yang dicari
- Ukuran unggahan maksimal per file: 160 GB (149 GiB)
- Ukuran file maksimal untuk disalin: 5,36 GB (5 GiB)
- Nama folder yang dimulai atau diakhiri dengan titik (.) tidak didukung

Prasyarat

Dalam AWS Identity and Access Management, konfigurasi peran yang diperlukan. Tempel di blok kode yang kami berikan dalam instruksi. Untuk informasi tentang mengonfigurasi peran yang diperlukan, lihat [Konfigurasi peran IAM untuk aplikasi web Transfer Family](#).

- Buat peran pembawa identitas.
- Buat peran IAM untuk digunakan oleh S3 Access Grants. S3 Access Grants mengasumsikan peran IAM ini untuk menjual kredensial sementara kepada penerima hibah untuk lokasi Amazon S3 yang terdaftar.

Proses untuk membuat aplikasi web Transfer Family

Untuk membuat aplikasi web dan mengaktifkan dan menjalankan pengguna akhir, Anda melakukan tugas-tugas berikut:

1. Konfigurasi Pusat Identitas IAM untuk bertindak sebagai penyedia identitas federasi Anda. Lakukan tugas-tugas berikut di IAM Identity Center. Untuk detail selengkapnya tentang mengonfigurasi Pusat Identitas IAM, lihat. [Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family](#)
 - a. Buat instance IAM Identity Center, jika Anda belum memilikinya.
 - b. Tentukan sumber identitas Anda. Ini bisa menjadi direktori Pusat Identitas IAM default atau penyedia pihak ketiga (misalnya Okta).
 - c. Buat atau identifikasi pengguna atau grup yang akan menggunakan aplikasi web Anda.
 - d. Jika Anda menggunakan direktori IAM Identity Center untuk sumber identitas Anda, perhatikan ID pengguna atau grup yang Anda buat. Anda membutuhkannya nanti saat membuat hibah akses dengan menggunakan S3 Access Grants.
2. Di Amazon S3, konfigurasi Hibah Akses Amazon S3. Untuk informasi selengkapnya tentang Hibah Akses S3, lihat. [Konfigurasi Hibah Akses Amazon S3 untuk aplikasi web Transfer Family](#)
 - Buat instance S3 Access Grants jika Anda belum memilikinya. Wilayah AWS
 - Daftarkan lokasi Anda menggunakan peran IAM.
 - Buat hibah akses.
3. Di Transfer Family, lakukan tugas-tugas berikut.

- a. Buat aplikasi web Transfer Family. Untuk informasi selengkapnya tentang cara membuat aplikasi web Transfer Family, lihat [Mengkonfigurasi aplikasi web Transfer Family](#).

 Important

Siapkan berbagi Cross-origin sumber daya (CORS) untuk semua bucket Amazon S3 yang digunakan oleh aplikasi web Anda. Untuk informasi tentang pengaturan CORS, lihat [Siapkan berbagi Cross-origin sumber daya \(CORS\) untuk bucket Anda](#).

- b. Tetapkan pengguna atau grup ke aplikasi web. Untuk informasi selengkapnya tentang cara menetapkan pengguna dan grup, lihat [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).
- c. (Opsional) Perbarui titik akhir akses untuk aplikasi web Anda dengan URL khusus. Untuk informasi tentang membuat URL kustom, lihat [Perbarui titik akhir akses Anda dengan URL khusus](#).
- d. Berikan URL titik akhir akses kepada pengguna akhir Anda sehingga mereka dapat masuk dan berinteraksi dengan aplikasi web Anda.

Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family

Bagian berikut menjelaskan cara mengonfigurasi penyedia identitas Anda.

Untuk memulai, Anda harus memiliki sumber identitas. Anda dapat menggunakan direktori Pusat Identitas IAM AWS Directory Service for Microsoft Active Directory, atau penyedia identitas eksternal. Transfer Family menggunakan IAM Identity Center sebagai penyedia identitas federasi, yang merupakan sistem yang menyimpan kredensi pengguna dan mengautentikasi pengguna di beberapa organisasi.

Jika Anda tidak menggunakan direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat topik berikut:

- [Mengelola penyedia identitas eksternal](#)
- [Connect ke direktori Microsoft AD](#)
- [Organisasi dan instans akun Pusat Identitas IAM](#)
- [Tutorial sumber identitas Pusat Identitas IAM](#)

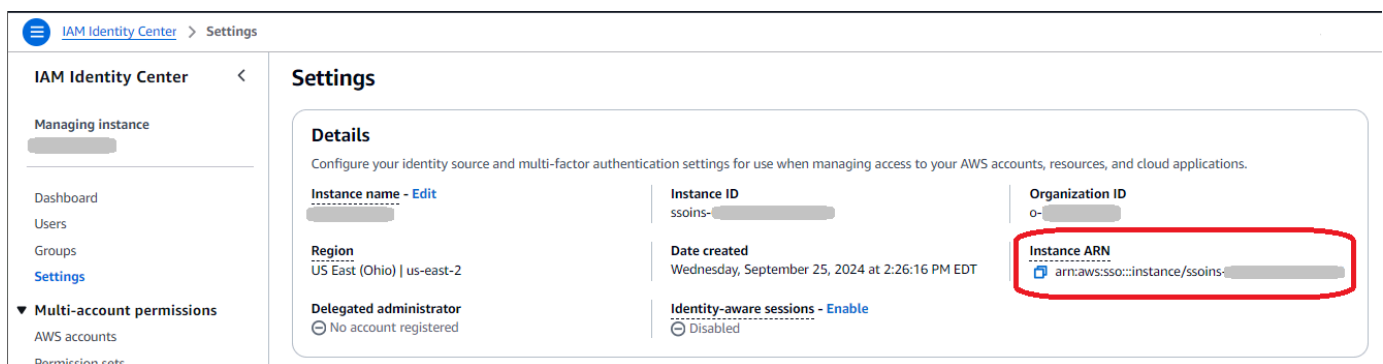
Note

Anda hanya dapat memiliki satu sumber identitas di IAM Identity Center, per instance, per Wilayah AWS. Untuk detailnya, lihat [prasyarat dan pertimbangan Pusat Identitas IAM](#).

Jika Anda berencana untuk menggunakan direktori IAM Identity Center sebagai sumber identitas Anda, dan ingin pengaturan cepat, Anda dapat melewati topik ini dan pergi [Membuat aplikasi web Transfer Family](#) untuk membuat instance IAM Identity Center dari wizard.

Mengkonfigurasi AWS IAM Identity Center untuk digunakan dengan aplikasi web Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Anda dapat membuat dan menggunakan instance akun atau instance organisasi AWS IAM Identity Center.
 - Untuk detail tentang instance akun, lihat [Membuat instance akun dari. AWS IAM Identity Center](#) Dengan instance akun IAM Identity Center, Anda dapat menerapkan aplikasi terkelola yang didukung dan aplikasi AWS terkelola pelanggan berbasis OpenID Connect (OIDC). Instans akun mendukung penerapan aplikasi yang terisolasi dalam satu Akun AWS, memanfaatkan identitas tenaga kerja IAM Identity Center dan mengakses fitur portal.
 - Untuk detail tentang instans organisasi, lihat Instans [organisasi Pusat Identitas IAM](#). Anda dapat mengelola akses pengguna dan grup secara terpusat dengan satu instans organisasi.
3. Pada halaman Pengaturan Pusat Identitas IAM, catat ARN Instance Anda. Anda akan memerlukan nilai ini saat membuat instans Amazon S3 Access Grant.



4. Buat satu atau beberapa pengguna dan, secara opsional, grup, untuk digunakan dengan aplikasi web Transfer Family Anda. Jika Anda menggunakan direktori IAM Identity Center sebagai penyedia identitas Anda, Anda juga dapat menambahkan pengguna langsung dari aplikasi web

itu sendiri. Untuk informasi selengkapnya, lihat [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).

Konfigurasi peran IAM untuk aplikasi web Transfer Family

Anda akan memerlukan dua peran: satu untuk digunakan sebagai peran pembawa identitas untuk aplikasi web Anda, dan yang kedua digunakan untuk mengonfigurasi hibah akses. Peran pembawa identitas adalah peran yang mencakup identitas pengguna yang diautentikasi dalam sesinya. Ini digunakan untuk membuat permintaan ke S3 Access Grants untuk akses data atas nama pengguna.

Note

Anda dapat melewati prosedur untuk membuat peran pembawa identitas. Untuk informasi tentang meminta layanan Transfer Family membuat peran pembawa identitas, lihat [Membuat aplikasi web Transfer Family](#).

Anda dapat melewati prosedur untuk membuat peran hibah akses. Dalam prosedur untuk membuat hibah akses, pada langkah di mana Anda mendaftarkan lokasi S3, pilih Buat peran baru.

Buat peran pembawa identitas

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Pilih Peran, lalu Buat peran.
3. Pilih Kebijakan kepercayaan khusus, lalu tempelkan kode berikut.

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

```

    ]
  }
]
}

```

4. Pilih Berikutnya dan kemudian lewati Tambahkan izin dan pilih Berikutnya lagi.
5. Masukkan nama, misalnya `web-app-identity-bearer`.
6. Pilih Buat peran untuk membuat peran pembawa identitas.
7. Pilih peran yang baru saja Anda buat dari daftar, lalu di panel Kebijakan izin, pilih Tambahkan izin > Buat kebijakan sebaris.
8. Di editor Kebijakan, pilih JSON dan kemudian tempel di blok kode berikut.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}

```

9. Untuk nama kebijakan, masukkan `AllowS3AccessGrants`, lalu pilih Buat kebijakan.

Selanjutnya, Anda membuat peran yang diasumsikan oleh S3 Access Grants untuk menjual kredensi sementara kepada penerima hibah.

Note

Jika Anda mengizinkan layanan untuk membuat peran pembawa identitas untuk Anda, peran itu menetapkan perlindungan wakil yang membingungkan. Oleh karena itu, kodenya berbeda dari apa yang ditampilkan di sini.

Buat peran hibah akses

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Pilih Peran, lalu Buat peran. Peran ini harus memiliki izin untuk mengakses data S3 Anda di file. Wilayah AWS
3. Pilih Kebijakan kepercayaan khusus, lalu tempelkan kode berikut.

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

4. Pilih Berikutnya tambahkan kebijakan minimal seperti yang dijelaskan dalam [Daftarkan lokasi](#). Meskipun tidak disarankan, Anda dapat menambahkan kebijakan AmazonS3FullAccesssterkelola, yang mungkin terlalu permisif untuk kebutuhan Anda.
5. Pilih Berikutnya, dan masukkan nama (misalnyaaccess-grants-location).
6. Pilih Buat peran untuk membuat peran.

Note

Jika Anda mengizinkan layanan untuk membuat peran hibah akses untuk Anda, peran tersebut menetapkan perlindungan wakil yang membingungkan. Oleh karena itu, kodenya berbeda dari apa yang ditampilkan di sini.

Mengkonfigurasi aplikasi web Transfer Family

Bagian ini menjelaskan prosedur untuk membuat aplikasi web Transfer Family. Untuk menetapkan pengguna dan grup yang dapat menggunakannya, lihat [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).

Note

Ulangi prosedur ini untuk menambahkan aplikasi web tambahan. Anda dapat menggunakan kembali peran IAM yang Anda buat sebelumnya. Pastikan untuk menambahkan titik akhir akses untuk aplikasi web baru ke kebijakan berbagi Cross-origin sumber daya (CORS) setiap bucket.

Membuat aplikasi web Transfer Family

Note

Jika Anda tidak menggunakan direktori Pusat Identitas IAM untuk penyedia identitas Anda, jangan mencoba membuat aplikasi web sampai Anda telah menyiapkan Pusat Identitas IAM dan mengonfigurasi penyedia identitas pihak ketiga, seperti yang dijelaskan dalam [Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family](#)

Selesaikan langkah-langkah berikut untuk membuat aplikasi web Transfer Family.

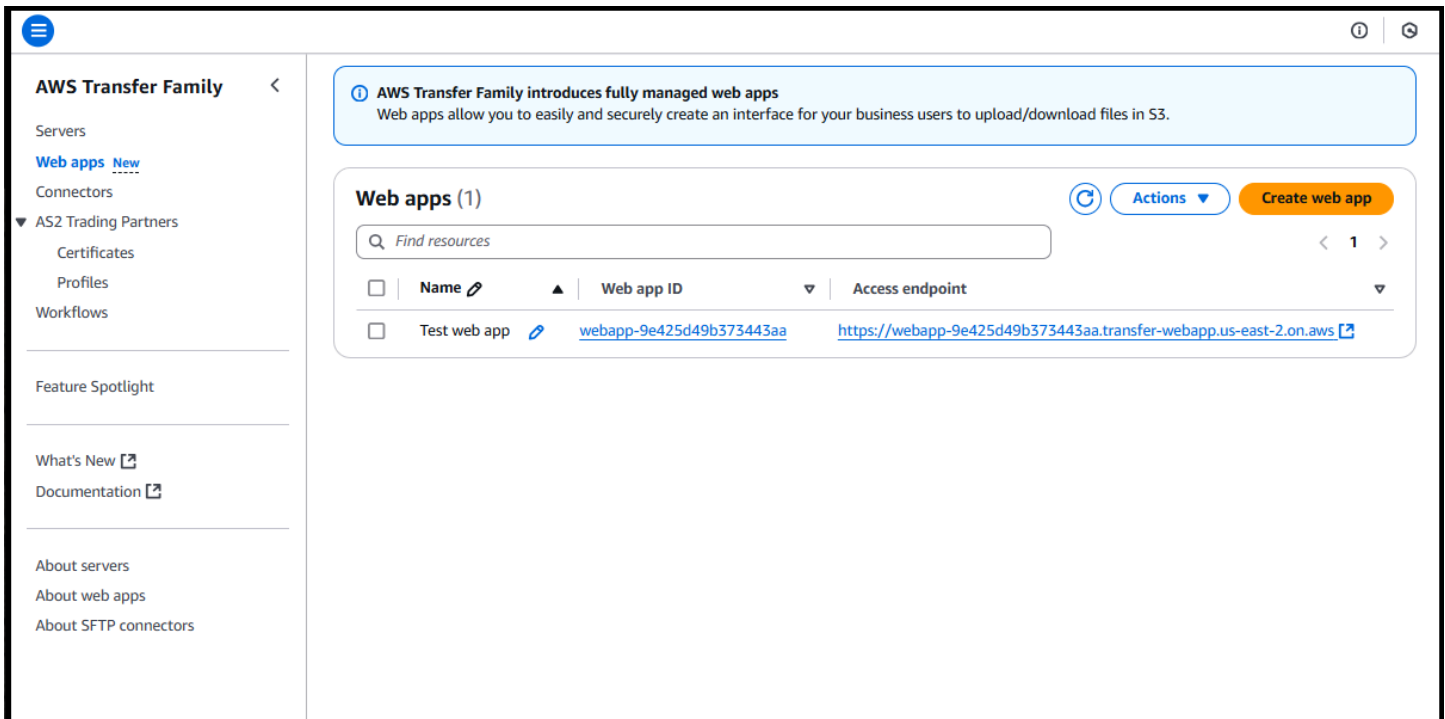
Untuk membuat aplikasi web Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Aplikasi Web.
3. Pilih Buat aplikasi web.

Untuk akses otentikasi, panel diisi sebagai berikut.

- Jika Anda telah membuat instansi organisasi atau akun AWS IAM Identity Center, maka Anda melihat pesan ini: AWS Transfer Family Aplikasi Anda terhubung ke instance akun IAM Identity Center.

- Jika Anda sudah memiliki instans akun dan merupakan anggota instans organisasi, Anda memiliki opsi untuk memilih instance mana yang akan dihubungkan.
 - Jika Anda belum memiliki instance akun, atau merupakan anggota dalam instance organisasi, Anda akan diberikan opsi untuk membuat instance akun.
4. Untuk tipe Endpoint, pilih tipe titik akhir yang dapat diakses publik. Untuk titik akhir yang dihosting VPC, lihat. [Membuat aplikasi web Transfer Family di VPC](#)
 5. Di panel Jenis izin, Anda dapat menggunakan peran yang dibuat sebelumnya, atau meminta layanan membuatnya untuk Anda.
 - Jika Anda telah membuat peran pembawa identitas, pilih Gunakan peran yang ada dan pilih peran Anda dari menu Pilih peran yang ada.
 - Agar layanan membuat peran untuk Anda, pilih Buat dan gunakan peran layanan baru.
 6. Di panel unit aplikasi Web, pilih nilai. Satu unit aplikasi web memungkinkan aktivitas aplikasi web hingga 250 sesi unik. Saat membuat aplikasi web, Anda menyediakan jumlah unit yang Anda butuhkan berdasarkan volume beban kerja puncak yang diharapkan. Mengubah unit aplikasi web berdampak pada penagihan Anda. Untuk informasi tentang harga, lihat [AWS Transfer Family Harga](#).
 7. Jika Anda menggunakan Transfer Family di AWS GovCloud (US) Region, Anda dapat memilih kotak centang FIPS Enabled endpoint di panel FIPS Enabled. Untuk semua yang lain Wilayah AWS, opsi ini tidak tersedia.
 8. (Opsional) Tambahkan tag untuk membantu Anda mengatur aplikasi web Anda. Kami menyarankan Anda menambahkan tag dengan Nama sebagai kunci dan nama deskriptif sebagai nilai.
 9. Pilih Berikutnya. Di layar ini, Anda dapat memberikan judul untuk aplikasi web Anda secara opsional. Jika Anda tidak memberikan judul, judul default Transfer Web App disediakan. Anda juga dapat mengunggah file gambar untuk logo dan favicon Anda.
 10. Pilih Berikutnya, lalu pilih Buat aplikasi web.



Note

Pastikan untuk menyiapkan kebijakan berbagi Cross-origin sumber daya (CORS) untuk semua bucket yang diakses dari titik akhir aplikasi web.

Penentuan alamat IP

Aplikasi web Transfer Family menggunakan endpoint dual-stack, mendukung konektivitas IPv4 dan IPv6. Untuk otentikasi, aplikasi web menggunakan AWS IAM Identity Center, yang juga mendukung IPv6 melalui titik akhir dual-stack.

Jika akun Anda memiliki aplikasi web di Wilayah saat dukungan endpoint IAM Identity Center dual-stack diluncurkan, semua aplikasi web di akun tersebut dan Wilayah akan terus menggunakan titik akhir Pusat Identitas IPv4-only IAM untuk kompatibilitas mundur. Ini berlaku untuk aplikasi web yang ada dan yang baru dibuat. Akun yang tidak memiliki aplikasi web pada saat peluncuran menggunakan endpoint dual-stack IAM Identity Center. Jika Anda perlu mengubah titik akhir IAM Identity Center yang digunakan aplikasi web Anda, hubungi Support AWS .

 Note

Untuk menentukan titik akhir yang digunakan aplikasi web Anda, periksa URL saat Anda diarahkan ke halaman masuk Pusat Identitas IAM:

- IPv4-only: [Region].signin.aws.amazon.com
- Dual-stack: [Region].sso.signin.aws

Jika organisasi Anda menggunakan firewall atau gateway jaringan, izinkan daftar IPv4 yang ada dan titik akhir IAM Identity Center dual-stack baru untuk memastikan akses tanpa gangguan terlepas dari titik akhir yang digunakan aplikasi web Anda. Untuk daftar lengkap domain dan titik akhir URL yang diizinkan, lihat [Memperbarui firewall dan gateway untuk mengizinkan akses ke portal AWS akses di Panduan Pengguna Pusat Identitas IAM](#).

Membuat aplikasi web Transfer Family di VPC

Bagian ini menjelaskan prosedur untuk membuat aplikasi web Transfer Family di VPC. Anda dapat meng-host endpoint aplikasi web Anda di dalam virtual private cloud (VPC) untuk digunakan untuk mentransfer data ke dan dari bucket Amazon S3 tanpa melalui internet publik. Untuk menetapkan pengguna dan grup yang dapat menggunakan aplikasi web Anda, lihat [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).

 Note

Untuk memastikan aliran data end-to-end pribadi saat menggunakan titik akhir VPC aplikasi web Transfer Family, Anda harus menerapkan tiga komponen tambahan. Pertama, siapkan PrivateLink titik akhir untuk operasi API Kontrol Amazon S3, yang diperlukan untuk panggilan API Amazon S3 Access Grants. Kedua, konfigurasi titik akhir untuk akses data Amazon S3 menggunakan titik akhir Amazon PrivateLink S3 Gateway (untuk lalu lintas dari dalam VPC Anda) atau titik akhir Antarmuka Amazon S3 (untuk lalu lintas dari jaringan lokal melalui VPN atau Direct Connect). Ketiga, kunci akses bucket Amazon S3 Anda dengan memperbarui kebijakan bucket untuk hanya mengizinkan lalu lintas dari titik akhir VPC ini. Kombinasi ini memastikan semua transfer data tetap berada dalam infrastruktur jaringan pribadi Anda dan tidak pernah melintasi internet publik.

Membuat aplikasi web Transfer Family

Prasyarat

- AWS IAM Identity Center diatur dengan penyedia identitas yang dikonfigurasi. Lihat [Konfigurasi penyedia identitas Anda untuk aplikasi web Transfer Family](#).
- VPC dan komponen jaringan diatur. Lihat [Membuat VPC](#).
- Titik akhir API disiapkan untuk operasi Kontrol Amazon S3. Lihat [Mengakses titik akhir antarmuka Amazon S3](#).
- Titik akhir VPC untuk Amazon S3 (Gateway atau Antarmuka) disiapkan. Lihat [Jenis titik akhir VPC untuk Amazon S3](#). Jika Anda menggunakan titik akhir antarmuka, Anda harus mengaktifkan DNS pribadi. Sebagai contoh, lihat [Memperkenalkan dukungan DNS pribadi untuk Amazon AWS PrivateLink S3](#) dengan.

Note

AWS IAM Identity Center tidak mendukung titik akhir VPC; semua permintaan otentikasi mengangkut internet publik. Selain itu, aplikasi web Transfer Family memerlukan akses internet untuk memuat konten statis (seperti JavaScript, CSS, dan file HTML). Persyaratan untuk akses internet publik terpisah dari akses data. Titik akhir VPC Anda memastikan bahwa koneksi dirutekan melalui infrastruktur VPC Anda.

Untuk membuat aplikasi web Transfer Family

1. Masuk ke Konsol Manajemen AWS dan buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Aplikasi Web.
3. Pilih Buat aplikasi web. Untuk akses otentikasi, panel diisi sebagai berikut.
 - Jika Anda telah membuat instans organisasi atau akun AWS IAM Identity Center, maka Anda melihat pesan ini: AWS Transfer Family Aplikasi Anda terhubung ke instance akun IAM Identity Center.
 - Jika Anda sudah memiliki instans akun dan merupakan anggota instans organisasi, Anda memiliki opsi untuk memilih instance mana yang akan dihubungkan.

- Jika Anda belum memiliki instance akun, atau merupakan anggota dalam instance organisasi, Anda akan diberikan opsi untuk membuat instance akun.
4. Di bagian konfigurasi Endpoint, pilih bagaimana pengguna Anda akan mengakses aplikasi web Anda:
- Dapat diakses publik: Titik akhir aplikasi web Anda dapat diakses melalui publik melalui HTTPS. Opsi ini tidak memerlukan konfigurasi VPC apa pun, sehingga mudah diatur dan cocok untuk aplikasi yang ditujukan untuk penggunaan umum secara luas.
 - Dihosting VPC: Titik akhir aplikasi web Anda di-host dalam Virtual Private Cloud (VPC), menyediakan akses jaringan pribadi melalui jaringan VPC, atau koneksi VPN Anda. AWS Direct Connect Opsi ini menawarkan peningkatan keamanan melalui isolasi jaringan dan direkomendasikan untuk aplikasi internal.

Saat mengonfigurasi titik akhir yang dihosting VPC, Anda harus menentukan:

- VPC: Pilih VPC yang ada atau buat yang baru. Tombol Buat VPC tersedia.
- Availability zones: Pilih zona ketersediaan tempat endpoint Anda akan digunakan.
- Subnet: Pilih subnet dalam setiap zona ketersediaan yang dipilih.
- Grup keamanan: Pilih atau buat grup keamanan untuk mengontrol akses berdasarkan alamat IP sumber. Jika tidak ditentukan, grup keamanan default VPC digunakan. Kelola grup keamanan melalui Konsol VPC. Konfigurasikan grup keamanan VPC Anda untuk mengizinkan lalu lintas masuk dari jaringan Anda melalui HTTPS pada port TCP 443. Ini diperlukan untuk autentikasi IAM Identity Center dan pemuatan konten statis aplikasi web.

 Note

Titik akhir akses tidak dapat disesuaikan untuk titik akhir VPC. Untuk menambahkan URL kustom, gunakan titik akhir publik.

Post-creation langkah

- Pastikan untuk menyiapkan kebijakan berbagi Cross-origin sumber daya (CORS) untuk semua bucket yang diakses dari titik akhir aplikasi web. Lihat [Cross-origin kebijakan berbagi sumber daya \(CORS\)](#).
- Perbarui kebijakan bucket Anda untuk mengizinkan lalu lintas hanya berasal dari VPC Anda melalui titik akhir VPC Anda. Lihat [Membatasi akses ke titik akhir VPC kustom](#).

- Tetapkan atau tambahkan pengguna atau grup ke aplikasi web Transfer Family. Lihat [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).

Cross-origin kebijakan berbagi sumber daya (CORS)

Anda harus menyiapkan berbagi sumber daya lintas asal (CORS) untuk semua bucket yang digunakan oleh aplikasi web Anda. Untuk informasi selengkapnya tentang CORS, lihat [Siapkan berbagi Cross-origin sumber daya \(CORS\) untuk bucket Anda](#).

Important

Sebelum menggunakan kebijakan contoh berikut, ganti Asal yang Diizinkan dengan titik akhir akses Anda. Jika tidak, pengguna akhir Anda akan menerima kesalahan saat mereka mencoba mengakses lokasi di aplikasi web Anda.

Contoh kebijakan:

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
```

```

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

Membatasi akses ke titik akhir VPC kustom

Berikut ini adalah contoh kebijakan bucket Amazon S3 yang membatasi akses ke bucket tertentu, `amzn-s3-demo-bucket`, hanya dari titik akhir VPC dengan ID `vpce-1a2b3c4d`. Jika titik akhir yang ditentukan tidak digunakan, kebijakan menolak semua akses ke bucket. `aws:SourceVpceKondisi` menentukan titik akhir. `aws:SourceVpceKondisi` ini tidak memerlukan ARN untuk sumber daya titik akhir VPC, hanya ID titik akhir VPC. Untuk informasi selengkapnya tentang memperbarui kebijakan bucket agar hanya mengizinkan lalu lintas yang berasal dari VPC, [lihat Mengontrol akses dari titik akhir VPC](#) dengan kebijakan bucket. Untuk informasi selengkapnya tentang penggunaan kondisi dalam kebijakan, lihat [Contoh kebijakan Bucket menggunakan kunci kondisi](#). Sebagai prasyarat untuk menerapkan kebijakan ini, Anda harus membuat titik akhir VPC Amazon [S3](#).

Important

Sebelum menggunakan kebijakan contoh berikut ini, ganti ID titik akhir VPC dengan nilai yang sesuai untuk kasus penggunaan Anda. Jika tidak, Anda tidak akan dapat mengakses bucket Anda.

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```



```
"Condition": {
  "StringNotEquals": {
    "aws:SourceVpce": "vpce-1a2b3c4d"
  }
}
]
```

Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family

Setelah membuat aplikasi web Transfer Family, Anda dapat menetapkan pengguna dan grup yang kemudian dapat mengakses aplikasi web. Anda dapat mengambil pengguna yang sudah dibuat dan disimpan di Pusat Identitas IAM, atau Anda dapat [menambahkan pengguna baru secara langsung](#) (jika Anda menggunakan direktori Pusat Identitas IAM sebagai penyedia identitas Anda). Jika Anda menambahkan pengguna baru, mereka juga ditambahkan ke instans Pusat Identitas IAM Anda.

Perhatikan hal-hal berikut:

- Anda hanya dapat menambahkan pengguna baru jika Anda menggunakan direktori IAM Identity Center sebagai sumber identitas Anda dan memiliki izin yang tepat. Jika Anda adalah anggota instans organisasi, Anda mungkin tidak memiliki izin yang diperlukan untuk menambahkan pengguna.

Note

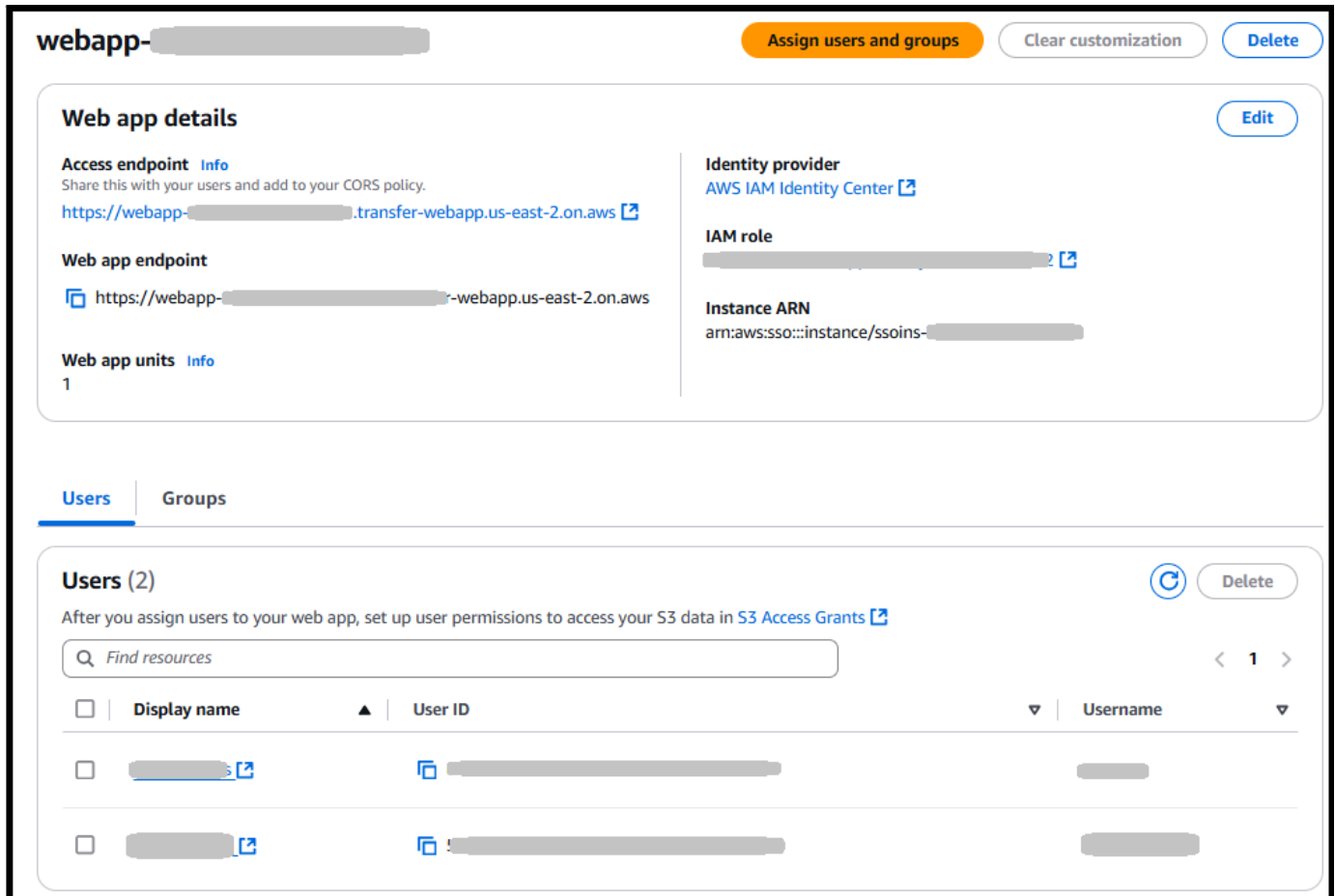
Jika Anda tidak menetapkan pengguna atau grup ke aplikasi Anda, pengguna Anda akan mendapatkan kesalahan saat mereka mencoba masuk ke aplikasi web Anda.

- Jika Anda membuat pengguna baru, Anda juga harus membuat hibah akses S3 untuk pengguna ini sehingga mereka dapat mengakses data di aplikasi web Anda.
- Setelah Anda membuat pengguna baru, pengguna tersebut menerima email orientasi dari IAM Identity Center dengan petunjuk cara untuk melanjutkan.

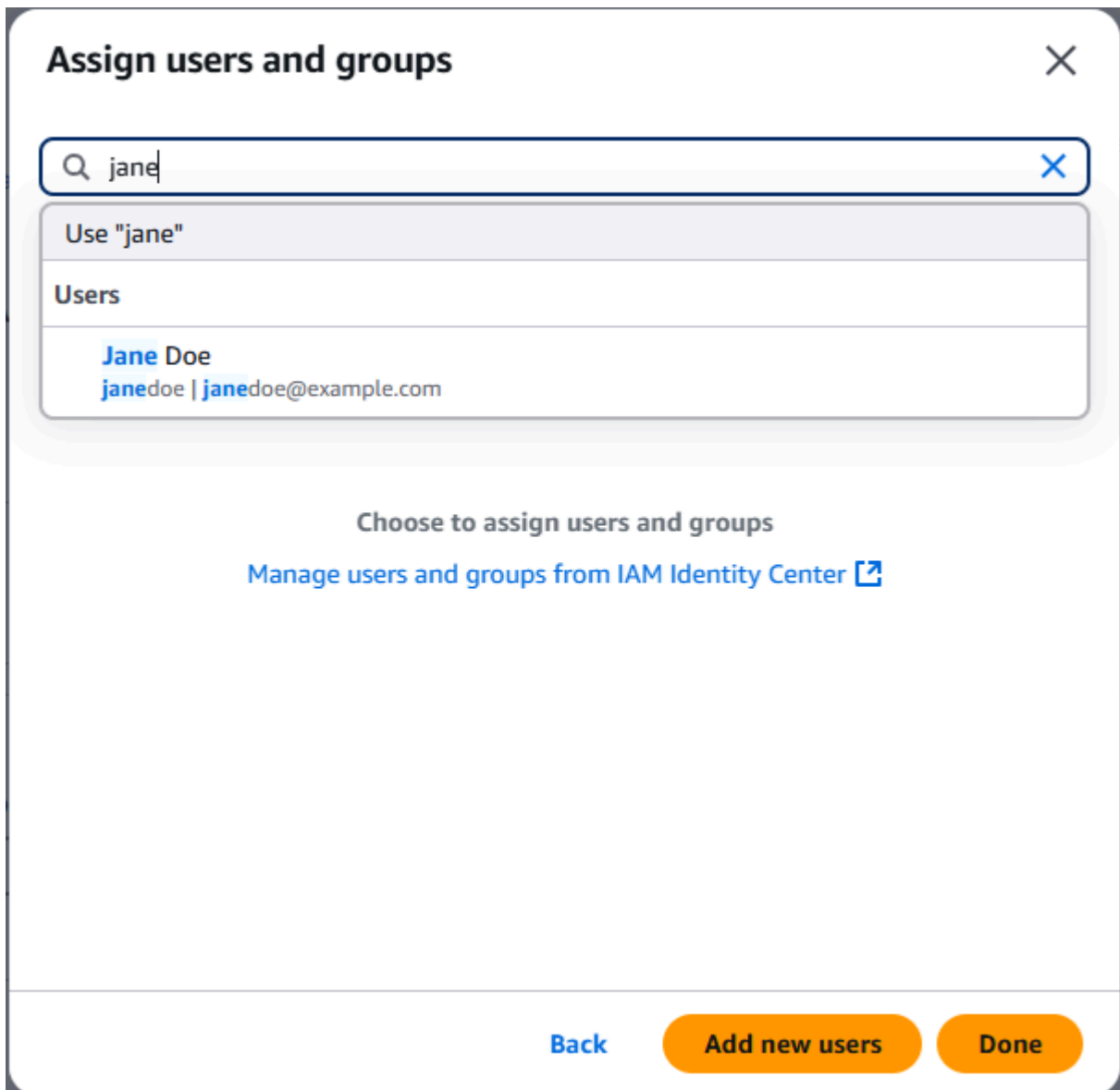
Untuk menetapkan pengguna ke aplikasi web Transfer Family

1. Arahkan ke daftar aplikasi web Anda, dan pilih salah satu yang ingin Anda edit.

2. Pilih Tetapkan pengguna dan grup.



3. Untuk menetapkan pengguna yang sebelumnya Anda buat di Pusat Identitas IAM, pilih Tetapkan pengguna dan grup yang ada. Untuk membuat pengguna baru, lompat ke langkah 4.
 - a. Layar informasi muncul. Pilih Mulai untuk melanjutkan.
 - b. Cari pengguna. Perhatikan bahwa tidak ada pengguna yang muncul sampai Anda mulai memasukkan kriteria pencarian Anda. Anda harus mencari berdasarkan nama tampilan, bukan nama pengguna, jika berbeda. Hanya kecocokan persis yang dikembalikan. Jika Anda tidak dapat menemukan pengguna, navigasikan ke konsol manajemen Pusat Identitas IAM, temukan pengguna, lalu salin dan tempel nama tampilannya di sini.



- c. Pilih pengguna dan grup yang akan ditambahkan, lalu pilih Tetapkan.
4. Untuk membuat pengguna baru, pilih Tambah dan tetapkan pengguna baru.
 - a. Layar informasi muncul. Pilih Mulai untuk melanjutkan.
 - b. Pilih Tambahkan pengguna baru.
 - c. Masukkan detail pengguna berikut ke dalam kotak dialog: nama pengguna, nama depan dan belakang, dan alamat email.

Add new users [X]

Info Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) [X]

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +, -, @, _

First name **Last name**

Email address **Confirm email address**

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

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

- d. Pilih Berikutnya, lalu pilih Tambah untuk menambahkan pengguna dan menutup kotak dialog, atau Tambahkan pengguna baru untuk membuat pengguna lain.

Siapkan berbagi Cross-origin sumber daya (CORS) untuk bucket Anda

Anda harus menyiapkan berbagi sumber daya lintas asal (CORS) untuk semua bucket yang digunakan oleh aplikasi web Anda. Konfigurasi CORS adalah dokumen yang mendefinisikan aturan yang mengidentifikasi asal yang Anda izinkan untuk mengakses bucket Anda. Untuk informasi selengkapnya tentang CORS, lihat [Mengonfigurasi berbagi sumber daya lintas asal \(CORS\)](#).

⚠ Important

Jika Anda tidak menyiapkan CORS, pengguna akhir Anda akan menerima kesalahan saat mereka mencoba mengakses lokasi di aplikasi web Anda.

Untuk menyiapkan berbagi Cross-origin sumber daya (CORS) untuk bucket Amazon S3

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Pilih Bucket dari panel navigasi kiri dan cari bucket Anda di dialog pencarian, lalu pilih tab Izin.
3. Dalam berbagi Cross-origin sumber daya (CORS), pilih Edit dan tempel dalam kode berikut. Ganti *WebAppEndpoint* dengan titik akhir akses aktual untuk aplikasi web Anda. Ini bisa berupa titik akhir akses publik yang dihosting VPC atau yang dibuat saat aplikasi web dibuat, atau titik akhir akses khusus, jika Anda membuatnya. Pastikan untuk tidak memasukkan garis miring, karena hal itu menyebabkan kesalahan saat pengguna mencoba masuk ke aplikasi web Anda.
 - Contoh yang salah: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Contoh yang benar:
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Jika Anda menggunakan kembali bucket untuk beberapa aplikasi web, tambahkan titik akhir mereka ke daftar. `AllowedOrigins`

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

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

4. Pilih Simpan perubahan untuk memperbarui CORS.

Untuk menguji konfigurasi CORS Anda, lihat [Menguji CORS](#).

Konfigurasi Hibah Akses Amazon S3 untuk aplikasi web Transfer Family

Topik ini menjelaskan cara menambahkan hibah akses menggunakan Amazon S3 Access Grants. Hibah akses ini mendefinisikan akses ke data Anda langsung ke pengguna dan grup Anda di direktori perusahaan Anda dan menjual kredensial sementara yang tepat waktu, paling tidak istimewa, berdasarkan hibah. Hibah individu dalam instans S3 Access Grants memungkinkan pengguna atau grup tertentu di direktori perusahaan—untuk mendapatkan akses di lokasi yang terdaftar di instans Hibah Akses S3 Anda. Untuk detail selengkapnya, lihat [konsep S3 Access Grants](#) di Panduan Pengguna Amazon S3.

 Note

Anda tidak dapat menggunakan direktori IAM Identity Center dengan S3 Access Grants selain dengan aplikasi web Transfer Family.

Anda harus menentukan hibah akses Amazon S3 untuk propagasi identitas. Hibah akses Amazon S3 menyimpan data yang harus diakses pengguna akhir Anda. Saat pengguna akhir masuk ke aplikasi web Transfer Family, S3 Access Grants meneruskan identitas pengguna ke aplikasi tepercaya. Bagian ini menjelaskan cara menambahkan dan mengonfigurasi instans hibah akses Amazon S3 dan kemudian hibah akses untuk bucket Amazon S3.

 Note

Siapkan [ARN instance IAM Identity Center](#) dan ID pengguna atau grup Anda, karena Anda membutuhkannya untuk menyelesaikan pengaturan hibah akses Anda.

Untuk membuat hibah menggunakan Amazon S3 Access Grants

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Buat bucket, atau catat bucket yang sudah ada untuk digunakan dengan aplikasi web Anda. Untuk informasi tentang cara membuat bucket, lihat Panduan Pengguna [Amazon S3](#).
3. Dari panel navigasi kiri, pilih Access Grants.
4. Pilih instance Create S3 Access Grants dan berikan informasi berikut.
 - Pilih Add IAM Identity Center instance di **your-Region** mana Anda **your-Region** Wilayah AWS berada. Biarkan kotak ini tetap bersih jika Anda tidak menggunakan IAM Identity Center sebagai penyedia identitas Anda.
 - Tempel di ARN Instance Pusat Identitas IAM Anda.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
● **Create S3 Access Grants instance**
- Step 2
○ Register S3 Buckets or prefixes as locations
- Step 3
○ Create grant
- Step 4
○ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - *optional*

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoins-

Format: arn:aws:sso::instance/<instanceidentifier>

Pilih Next untuk melanjutkan.

- Daftarkan Bucket atau awalan S3 sebagai lokasi. Kami menyarankan Anda mendaftarkan lokasi defaults3://, dan memetakannya ke peran IAM. Lokasi di jalur default ini mencakup akses ke semua bucket Amazon S3 Anda di akun Anda Wilayah AWS. Saat membuat hibah akses, Anda dapat mempersempit cakupan ke bucket, awalan, atau objek di dalam lokasi default.

Berikan informasi berikut.

- Untuk Lingkup, telusuri bucket atau masukkan nama bucket Anda, dan secara opsional awalan.
- Untuk peran IAM, pilih Buat peran baru agar layanan membuat peran.

Atau, Anda dapat membuat peran sendiri, seperti yang dijelaskan dalam [Konfigurasi peran IAM untuk aplikasi web Transfer Family](#), dan kemudian masukkan ARN-nya di sini.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
Format for bucket: s3://<bucket>
Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

[To ensure the role has proper permissions to access the location scope, consult the \[list of permissions\]\(#\).](#)

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role

☐ Choose from existing IAM roles

☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Pilih Next untuk melanjutkan.

6. Di layar Create Grant, berikan detail berikut.

- Untuk Izin, pilih Baca dan Tulis. Izin pemberian akses dapat berupa read-only atau read & write, tetapi write-only tidak didukung.
- Untuk jenis Penerima Hibah, pilih Identitas direktori dari IAM Identity Center.
- Untuk jenis identitas Direktori, pilih Pengguna atau Grup, tergantung pada jenis yang ingin Anda daftarkan sekarang.
- Di user/group ID Pusat Identitas IAM, tempel ID untuk pengguna atau grup Anda. ID ini tersedia di konsol Pusat Identitas IAM dan di aplikasi web Transfer Family Anda di tabel pengguna dan grup Anda.

Create Grant [Info](#)**Grant** [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)**IAM role** [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Pilih Berikutnya.

7. Tinjau pengaturan di layar. Jika semuanya benar, pilih Selesai untuk membuat hibah akses. Atau, Anda dapat memilih Batal atau Sebelumnya untuk membuat perubahan.

- Step 1
● Create S3 Access Grants instance
- Step 2
● Register S3 Buckets or prefixes as locations
- Step 3
● Create grant
- Step 4
● **Review and finish**

Review and finish [Info](#)

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional [Info](#)

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

arn:aws:sso:::application/ssoins-:/apl-

Successfully created S3 Access Grants instance

Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the [Resource Access Management console](#).

Step 2 - Register S3 buckets or prefixes as locations

Location [Info](#)

Location scope

s3://

IAM role [Info](#)

[web-app-beta-access-grants](#)

Successfully registered location

Location ID:

Step 3 - Create grants

Grant [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

s3:///*

IAM role [Info](#)

[web-app-beta-access-grants](#)

Location ID

Permissions and access

Access Type

READWRITE

Grantee type

Directory identity user

Grantee ID

Application - optional

Successfully created grant

Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

[Create another grant](#)

[Cancel](#)

[Previous](#)

[Finish](#)

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)

arn:aws:s3:us-east-2:account-id:access-grants/default

Creation date

October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

account-id

IAM Identity Center

DeregisterAdd

IAM Identity Center instance ARN

arn:aws:sso:us-east-2:account-id:application/ssoins-instance-id/apl-application-id

GrantsLocations

Grants (1)

DeleteCreate Grant

Find by grant scope or grantee

Grant scope	Grant ID	Permission	Grantee type	Grantee ID	Creation date	Location ID	Application ARN
s3://bucket-name/*	grant-id	Read, Write	Directory identity user	grantee-id	October 25, 2024, 11:57:30 (UTC-04:00)	location-id	ALL

Ini menyelesaikan penyiapan untuk aplikasi web Anda. Pengguna dan grup yang telah Anda konfigurasi dapat mengunjungi aplikasi web di titik akses, masuk, dan mengunggah dan mengunduh file.

Perbarui titik akhir akses Anda dengan URL khusus

Titik akhir akses default yang dibuat dengan aplikasi web Anda berisi pengenalan yang dihasilkan layanan. Untuk memberikan pengalaman bermerek, Anda mungkin ingin memberikan URL khusus bagi pengguna Anda untuk mengakses aplikasi web Transfer Family Anda. Topik ini menjelaskan cara memperbarui titik akhir akses Anda dengan URL khusus.

Note

Titik akhir akses tidak dapat disesuaikan untuk titik akhir VPC. Untuk menambahkan URL kustom, gunakan titik akhir publik.

Note

Prosedur berikut bergantung pada Anda menggunakan [template CloudFormation tumpukan](#) yang direkomendasikan. Anda tidak perlu menggunakan template: Anda dapat membuat distribusi dengan menggunakan [CloudFront konsol](#) secara langsung.

Gunakan URL khusus

312

Namun, template yang disediakan menyederhanakan proses, dan membuatnya lebih mudah untuk menghindari kesalahan konfigurasi. Jika Anda tidak menggunakan CloudFormation template, pastikan untuk mengikuti panduan ini:

- [Kebijakan permintaan Origin](#) harus meneruskan string kueri dan cookie ke asal, dan tidak boleh meneruskan Host header ke asal.
- [Kebijakan Cache](#) tidak boleh menyertakan Host header dalam kunci cache.

Untuk menyesuaikan URL aplikasi web Anda

1. Buat CloudFront distribusi dengan menggunakan template yang disediakan Transfer Family, AWS CloudFormation [template CloudFormation stack](#).
 - a. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
 - b. Pilih Buat tumpukan dan tentukan yang berikut ini.
 - Di bagian Prasyarat - Siapkan templat, pilih Pilih templat yang ada.
 - Di bagian Tentukan templat, pilih Unggah file templat.
 - Simpan file [template CloudFormation tumpukan](#), lalu unggah di sini.
 - c. Pilih Berikutnya dan berikan informasi berikut.
 - WebAppEndpoint: salin nilai dari aplikasi web Anda
 - AccessEndpoint: berikan nama domain khusus yang ingin Anda gunakan
 - AcmCertificateArn: menyediakan ARN untuk SSL/TLS sertifikat publik atau swasta yang disimpan di AWS Certificate Manager
 - d. Selesaikan CloudFormation wizard sampai tumpukan baru Anda dibuat.
2. Di aplikasi web Anda, edit titik akhir Access, perbarui URL Kustom ke URL yang ingin Anda gunakan.

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

`https://my-custom-url`

[Create a new distribution](#)

3. Buat catatan DNS untuk merutekan lalu lintas untuk nama domain kustom Anda ke CloudFront distribusi. Jika Anda menggunakan Route 53 untuk zona tersebut, Anda dapat membuat catatan Alias atau CNAME ke nama CloudFront distribusi (misalnya, xxxx.cloudfront.net). Untuk informasi tentang menggunakan Amazon Route 53 dengan CloudFront, lihat [Mengonfigurasi Amazon Route 53 untuk merutekan lalu lintas ke CloudFront distribusi](#).
4. Perbarui kebijakan berbagi sumber daya lintas asal Anda dengan mengganti titik akhir akses default dengan baris berikut di blok AllowedOrigins kode:

```
"https://custom-url"
```

Anda perlu membuat perubahan ini untuk setiap bucket yang digunakan oleh aplikasi web Anda.

Setelah Anda melakukan pembaruan, AllowedOrigins bagian kebijakan CORS Anda akan terlihat seperti berikut:

```
"AllowedOrigins": [
  "https://custom-url",
```

Anda hanya perlu satu AllowedOrigins entri untuk setiap aplikasi web Transfer Family.

Lihat [Mengatur berbagi Cross-origin sumber daya \(CORS\) untuk prosedur bucket Amazon S3](#) untuk detail selengkapnya.

Anda sekarang dapat mengunjungi titik akhir akses kustom Anda, dan membagikan tautan ini dengan pengguna akhir Anda.

CloudTrail log untuk aplikasi web Transfer Family

CloudTrail adalah Layanan AWS yang membuat catatan tindakan yang diambil dalam diri Anda Akun AWS. Ini terus memantau dan merekam operasi API untuk aktivitas seperti login konsol, AWS Command Line Interface perintah, dan SDK/API operasi. Ini memungkinkan Anda untuk menyimpan log siapa yang mengambil tindakan apa, kapan, dan dari mana. CloudTrail membantu audit, manajemen akses, dan kepatuhan terhadap peraturan dengan memberikan riwayat semua aktivitas di AWS lingkungan Anda.

Untuk aplikasi web Transfer Family, Anda dapat melacak peristiwa autentikasi dan operasi akses data yang dilakukan oleh pengguna. Untuk mengaktifkan pencatatan komprehensif, Anda perlu:

1. Konfigurasi CloudTrail untuk mencatat peristiwa manajemen untuk melacak aktivitas otentikasi.
2. Aktifkan peristiwa data Amazon S3 untuk melacak operasi file yang dilakukan melalui aplikasi web Anda.

Lihat juga

- [CloudTrail kasus penggunaan untuk Pusat Identitas IAM](#)
- [Memahami peristiwa masuk Pusat Identitas IAM](#)
- [CloudTrail Elemen UserIdentity](#)
- [Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3](#)
- [Acara Amazon S3 CloudTrail](#)

Mengaktifkan peristiwa data Amazon S3

Untuk melacak operasi file yang dilakukan melalui aplikasi web Transfer Family di bucket Amazon S3, Anda harus mengaktifkan peristiwa data untuk bucket tersebut. Peristiwa data menyediakan

aktivitas API tingkat objek dan sangat berguna untuk melacak unggahan file, unduhan, dan operasi lain yang dilakukan oleh pengguna aplikasi web.

Untuk mengaktifkan peristiwa data Amazon S3 untuk aplikasi web Transfer Family Anda:

1. Buka CloudTrail konsol di <https://console.aws.amazon.com/cloudtrail/>.
2. Di panel navigasi, pilih Jalur, lalu pilih jejak yang ada atau buat yang baru.
3. Di bawah Penyeleksi acara lanjutan, pilih Edit.
4. Pilih Tambahkan pemilih acara lanjutan.
5. Untuk pemilih bidang pertama:
 - Setel Bidang ke `eventCategory`
 - Setel Operator ke `Equals`
 - Tetapkan Nilai ke `Data`
6. Pilih Tambah bidang dan untuk pemilih bidang kedua:
 - Setel Bidang ke `resources.type`
 - Setel Operator ke `Equals`
 - Tetapkan Nilai ke `AWS::S3::Object`
7. (Opsional) Untuk mencatat peristiwa hanya untuk bucket tertentu, pilih Tambah bidang dan tambahkan:
 - Setel Bidang ke `resources.ARN`
 - Atur Operator ke Mulai dengan
 - Tetapkan Nilai ke `arn:aws:s3:::your-bucket-name/`
8. Pilih Simpan perubahan.

Atau, Anda dapat menggunakan konfigurasi peristiwa data lama:

1. Di bawah Peristiwa data, pilih Edit.
2. Untuk jenis peristiwa Data, pilih bucket S3 dan peristiwa objek.
3. Pilih bucket Amazon S3 untuk mencatat peristiwa data. Anda dapat memilih Semua bucket S3 saat ini dan masa depan atau menentukan masing-masing bucket.
4. Pilih apakah akan mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.
5. Pilih Simpan perubahan.

Setelah mengaktifkan peristiwa data, Anda dapat mengakses log ini di bucket Amazon S3 yang dikonfigurasi untuk CloudTrail Log mencakup detail seperti pengguna yang melakukan tindakan, stempel waktu tindakan, objek tertentu yang terpengaruh, dan onBehalfOf bidang yang membantu melacak tindakan yang dilakukan melalui aplikasi web Transfer Family. `userId`

Menemukan dan melihat log Anda

Ada beberapa cara untuk menemukan dan melihat CloudTrail log untuk aplikasi web Transfer Family Anda:

Menggunakan CloudTrail konsol

Cara tercepat untuk melihat peristiwa terbaru:

1. Buka CloudTrail konsol di <https://console.aws.amazon.com/cloudtrail/>.
2. Pilih Riwayat acara.
3. Filter acara berdasarkan:
 - Sumber acara: `signin.amazonaws.com` untuk acara aplikasi web
 - Sumber acara: `s3.amazonaws.com` untuk operasi file
4. Klik acara apa pun untuk melihat informasi terperinci.

Mengakses log di Amazon S3

Untuk mengakses file log lengkap yang disimpan di Amazon S3:

1. Identifikasi CloudTrail bucket Amazon S3 jejak Anda:

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Arahkan ke file log di Amazon S3:

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Unduh dan cari file log untuk ID aplikasi web Anda:

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
```

```
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Menggunakan AWS CLI untuk mencari acara

Cari acara aplikasi web tertentu menggunakan AWS CLI:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

Atau cari acara otentikasi:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Contoh log otentikasi

CloudTrail mencatat peristiwa autentikasi untuk aplikasi web Transfer Family, yang dapat membantu Anda melacak upaya login yang berhasil dan gagal. Log ini sangat berguna untuk pemantauan keamanan dan tujuan kepatuhan.

Topik

- [Contoh entri log untuk verifikasi kredensi](#)
- [Contoh entri log untuk otentikasi masuk](#)
- [Contoh entri log untuk ListCallerAccessGrants](#)
- [Contoh entri log untuk GetDataAccess acara](#)

Contoh entri log untuk verifikasi kredensi

Contoh berikut menunjukkan entri CloudTrail log untuk peristiwa verifikasi kredensi yang terjadi selama proses otentikasi.

```
{
```

```

    "eventVersion": "1.09",
    "userIdentity": {
      "type": "Unknown",
      "principalId": "123456789012",
      "arn": "",
      "accountId": "123456789012",
      "accessKeyId": "",
      "userName": "demo-user-2",
      "onBehalfOf": {
        "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
      },
      "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
    },
    "eventTime": "2025-08-08T15:29:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.224",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
      "CredentialType": "PASSWORD"
    },
    "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
    "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
      "CredentialVerification": "Success"
    },
    "eventCategory": "Management"
  }
}

```

Peristiwa ini memberikan detail tambahan tentang langkah verifikasi kredensi dalam proses otentikasi, yang menunjukkan ID kredensial tertentu dan ID alur kerja otentikasi yang digunakan.

Contoh entri log untuk otentikasi masuk

Contoh berikut menunjukkan entri CloudTrail log untuk peristiwa otentikasi pengguna yang berhasil selama proses masuk aplikasi web menggunakan IAM Identity Center.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  },
  "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
  "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "UserAuthentication": "Success"
  }
}
```

```

    },
    "eventCategory": "Management"
  }

```

Dalam contoh ini, perhatikan bidang-bidang penting berikut:

- `eventSource`: Menampilkan “signin.amazonaws.com”, menunjukkan ini adalah peristiwa otentikasi Pusat Identitas IAM.
- `userIdentity.onBehalfOf`: Berisi ID pengguna dan ARN penyimpanan identitas untuk pengguna aplikasi web.
- `additionalEventData.LoginTo`: Menunjukkan URL aplikasi IAM Identity Center yang sedang diakses.
- `additionalEventData.CredentialType`: Menunjukkan metode otentikasi yang digunakan (PASSWORD).
- `serviceEventDetails`: Menunjukkan hasil otentikasi (Sukses).

Contoh entri log untuk ListCallerAccessGrants

Contoh berikut menunjukkan entri CloudTrail log untuk suatu ListCallerAccessGrants peristiwa, yang terjadi saat aplikasi web Transfer Family menanyakan hibah akses yang tersedia untuk pengguna.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
        "accountId": "123456789012",
        "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
      },
      "attributes": {

```

```

        "creationDate": "2025-08-08T15:29:34Z",
        "mfaAuthenticated": "false"
    },
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
        "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    },
    "eventTime": "2025-08-08T15:29:35Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "ListCallerAccessGrants",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
        "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
        "allowedByApplication": "true",
        "maxResults": "100"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "1g34AaAELn/fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
        "bytesTransferredOut": 462
    },
    "requestID": "48485MTZEDWT0ANT",
    "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS:S3::AccessGrantsInstance",
            "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
        }
    ],
    "eventType": "AWS ApiCall",
    "managementEvent": true,

```

```

    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
  }

```

Dalam contoh ini, perhatikan bidang-bidang penting berikut:

- `eventName`: Menunjukkan ini adalah `ListCallerAccessGrants` acara, yang menanyakan hibah akses S3 yang tersedia.
- `requestParameters.allowedByApplication`: Menunjukkan kueri disaring ke hibah yang diizinkan oleh aplikasi.
- `requestParameters.maxResults`: Menunjukkan jumlah maksimum hibah untuk dikembalikan dalam tanggapan.
- `userIdentity.onBehalfOf`: Menautkan permintaan ke pengguna aplikasi web tertentu.

Acara ini membantu melacak kapan aplikasi web Transfer Family menanyakan sumber daya S3 yang dapat diakses pengguna, memberikan visibilitas ke dalam operasi penemuan hibah akses.

Contoh entri log untuk GetDataAccess acara

Contoh berikut menunjukkan entri CloudTrail log untuk suatu GetDataAccess peristiwa, yang terjadi saat aplikasi web Transfer Family meminta izin akses untuk sumber daya S3 atas nama pengguna.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },

```

```

      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      },
      "invokedBy": "transfer.amazonaws.com",
      "onBehalfOf": {
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9667b0da7a",
        "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
      }
    },
    "eventTime": "2025-05-08T16:10:25Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetDataAccess",
    "awsRegion": "ap-southeast-1",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
      "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
      "durationSeconds": 900,
      "permission": "READWRITE",
      "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
    },
    "responseElements": null,
    "additionalEventData": {
      "AuthenticationMethod": "AuthHeader",
      "CipherSuite": "TLS_AES_128_GCM_SHA256",
      "SignatureVersion": "SigV4",
      "bytesTransferredIn": 0,
      "bytesTransferredOut": 2244,
      "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagya
+cs0NjYl8FgEw4FGpE8DARi90aNC0RFWlTYNE7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
    },
    "requestID": "BXGSKKQXCWS5RAHB",
    "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
    "readOnly": true,
    "resources": [
      {
        "type": "AWS:S3::AccessGrantsInstance",
        "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
        "accountId": "123456789012"
      }
    ]
  ],

```



```
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

Dalam contoh ini, perhatikan bidang-bidang penting berikut:

- `eventName`: Menunjukkan ini adalah `GetDataAccess` peristiwa, yang terjadi ketika Transfer Family meminta izin akses untuk sumber daya S3.
- `userIdentity.onBehalfOf`: Berisi ARN penyimpanan identitas dan ID pengguna, yang menautkan permintaan akses ke pengguna aplikasi web tertentu.
- `requestParameters.target`: Menunjukkan pola jalur S3 yang aksesnya diminta.
- `requestParameters.permission`: Menunjukkan jenis akses yang diminta (`READWRITE`, `READ`, atau `WRITE`).
- `requestParameters.durationSeconds`: Menunjukkan berapa lama hibah akses valid (biasanya 900 seconds/15 menit).
- `sourceIPAddressdanuserAgent`: Keduanya menampilkan “`transfer.amazonaws.com`”, yang menunjukkan ini adalah permintaan layanan internal.

`GetDataAccess` event sangat berguna untuk melacak ketika pengguna aplikasi web Transfer Family diberikan akses ke sumber daya S3 tertentu, membantu Anda memantau pola akses dan memastikan otorisasi yang tepat.

Melihat entri CloudTrail log

Ada beberapa cara untuk melihat dan menganalisis entri CloudTrail log untuk aplikasi web Transfer Family Anda:

Menggunakan CloudTrail konsol

CloudTrail Konsol menyediakan antarmuka yang ramah pengguna untuk melihat dan memfilter entri log:

1. Buka CloudTrail konsol di <https://console.aws.amazon.com/cloudtrail/>.
2. Pada panel navigasi, pilih Riwayat peristiwa.
3. Gunakan opsi filter untuk mempersempit peristiwa:

- Setel sumber Acara `transfer.amazonaws.com` untuk hanya melihat acara Transfer Family.
 - Filter berdasarkan nama Acara untuk melihat operasi tertentu seperti `UserAuthentication`.
 - Gunakan rentang waktu untuk fokus pada peristiwa dalam periode tertentu.
4. Klik pada acara apa pun untuk melihat informasi detailnya.

Mengakses log di Amazon S3

Jika Anda telah mengonfigurasi CloudTrail jejak untuk mengirimkan log ke bucket Amazon S3, Anda dapat mengakses file log mentah secara langsung:

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Arahkan ke bucket dan awalan tempat CloudTrail log Anda disimpan.
3. Log diatur berdasarkan tahun, bulan, hari, dan wilayah. Arahkan ke direktori yang sesuai.
4. Unduh dan buka file log, yang dalam format JSON.

Memecahkan masalah aplikasi web Anda

Note

Kiat pemecahan masalah ini ditujukan untuk administrator aplikasi web dan bukan pengguna akhir. Untuk pengguna akhir, jika Anda mengalami masalah, hubungi administrator aplikasi web Anda. Semua contoh Anda dalam paragraf berikut merujuk ke admin aplikasi web.

Memecahkan masalah kesalahan jaringan

Deskripsi

Pengguna akhir Anda melihat spanduk jaringan Network Error saat memuat titik akhir aplikasi web.

Menyebabkan

Masalah yang paling umum adalah sebagai berikut:

- Admin tidak menetapkan pengguna yang mencoba masuk ke aplikasi baru.
- Admin tidak menambahkan tindakan yang diperlukan ke peran IAM Anda.

- Anda melihat daftar Hibah Akses S3 yang ditetapkan untuk pengguna Anda, tetapi CORS tidak dikonfigurasi dengan benar untuk bucket atau bucket Amazon S3 Anda.

Solusi

- Di IAM Identity Center, pastikan untuk menetapkan pengguna ke aplikasi yang benar. Atau, jika Anda memiliki grup yang ditetapkan, pastikan bahwa pengguna yang mencoba masuk termasuk dalam grup yang benar. Ini dijelaskan dalam [Menetapkan atau menambahkan pengguna atau grup ke aplikasi web Transfer Family](#).
- Periksa apakah peran Anda berisi tindakan yang diperlukan dalam kebijakan kepercayaan khusus untuk keduanya `sts:AssumeRole` dan `sts:SetContext` tindakan. Ini dijelaskan dalam [Konfigurasi peran IAM untuk aplikasi web Transfer Family](#).
- Periksa kebijakan CORS untuk semua bucket yang digunakan oleh aplikasi web Anda. Hal ini dijelaskan dalam [Mengatur berbagi Cross-origin sumber daya \(CORS\) untuk bucket Amazon S3 Anda](#).

Memecahkan masalah bucket yang dikonfigurasi tidak muncul

Deskripsi

Semuanya tampaknya dikonfigurasi dengan benar, tetapi bucket Amazon S3 tidak muncul di aplikasi web.

Menyebabkan

Salah satu kemungkinan penyebabnya adalah bucket Amazon S3 tidak berada di akun yang sama dengan aplikasi web.

Solusi

Pastikan bucket Amazon S3 berada di akun yang sama dengan aplikasi web. Cross-account bucket saat ini tidak didukung.

Memecahkan masalah kesalahan URL kustom

Deskripsi

Saat pengguna akhir Anda masuk ke aplikasi web, mereka menerima pesan kesalahan Otorisasi gagal: kode otorisasi hilang.

Menyebabkan

Jika Anda menggunakan CloudFront secara langsung, bukan CloudFormation templat yang disediakan, kemungkinan besar Anda salah mengonfigurasi kebijakan permintaan asal agar tidak meneruskan string kueri.

Solusi

Perbarui kebijakan permintaan asal Anda untuk meneruskan string kueri dan cookie ke asal.

Deskripsi

Saat pengguna akhir Anda mencoba mengakses aplikasi web Transfer Family, mereka menerima respons 404.

Menyebabkan

Jika Anda menggunakan CloudFront secara langsung, bukan CloudFormation templat yang disediakan, Anda mungkin salah mengonfigurasi kebijakan cache untuk menyertakan Host header dalam kunci cache atau salah konfigurasi kebijakan permintaan asal untuk meneruskan header.

Host

Solusi

- Pastikan kebijakan cache Anda tidak menyertakan Host header dalam kunci cache
- Pastikan kebijakan permintaan asal Anda tidak meneruskan Host header.

Memecahkan masalah kesalahan lain-lain

Deskripsi

Pengguna akhir Anda tidak dapat masuk, atau tidak dapat melihat ember atau file apa pun, atau Anda menerima kesalahan lain.

Menyebabkan

Salah satu kemungkinan penyebabnya adalah ARN instance IAM Identity Center tidak cocok dengan nilai ARN hibah Anda atau ARN instance IAM Identity Center aplikasi web Anda.

Solusi

Periksa item berikut untuk melihat apakah mereka cocok.

- Di Pusat Identitas IAM, navigasikan ke Pengaturan dan lihat ARN Instance.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- Di Amazon S3, navigasikan ke Access Grants dan lihat ARN instance IAM Identity Center Anda.

```
arn:aws:sso::account-id:application/ssoins-instance-identifier/ap1-1234567890abcdef0
```

- Di Transfer Family, buka halaman detail aplikasi web Anda dan lihat ARN Instance.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

instance-identifier Nilainya harus sama di ketiga tempat ini.

Bucket S3 duplikat muncul di aplikasi web

Deskripsi

Pengguna melihat bucket S3 yang sama terdaftar beberapa kali di antarmuka aplikasi web Transfer Family.

Menyebabkan

Hal ini terjadi ketika pengguna merupakan bagian dari beberapa grup Active Directory yang memiliki hibah duplikat ke bucket S3 yang sama. Aplikasi web mencantumkan semua hibah tingkat atas yang terkait dengan pengguna (UID atau GID) terlepas dari apakah pengguna memiliki beberapa hibah yang ditetapkan ke lokasi bucket yang sama.

Solusi

Untuk mengatasi masalah ini, administrator harus menghapus duplikasi hibah sehingga setiap pengguna hanya memiliki satu hibah untuk setiap lokasi S3. Tinjau konfigurasi S3 Access Grants Anda dan konsolidasikan hibah duplikat untuk bucket yang sama di berbagai grup Active Directory.

Instruksi pengguna akhir untuk aplikasi web Transfer Family

Note

Dalam topik ini, informasi dimaksudkan untuk pengguna akhir yang berinteraksi dengan aplikasi web. Semua contoh Anda dalam topik ini merujuk ke pengguna akhir.

Topik ini menjelaskan cara mengakses aplikasi AWS Transfer Family web yang diizinkan untuk digunakan, dan menjelaskan bagaimana Anda dapat berinteraksi dengannya.

Kuota aplikasi web

Perhatikan batasan berikut saat menggunakan aplikasi web.

- Jumlah maksimum hasil pencarian per kueri: 10.000
- Bucket Amazon S3 yang digunakan oleh aplikasi web Transfer Family harus berada di akun yang sama dengan aplikasi web itu sendiri. Cross-account bucket saat ini tidak didukung.
- Luas pencarian maksimum per kueri: 10.000 file yang dicari
- Ukuran unggahan maksimal per file: 160 GB (149 GiB)
- Ukuran file maksimal untuk disalin: 5,36 GB (5 GiB)
- Nama folder yang dimulai atau diakhiri dengan titik (.) tidak didukung

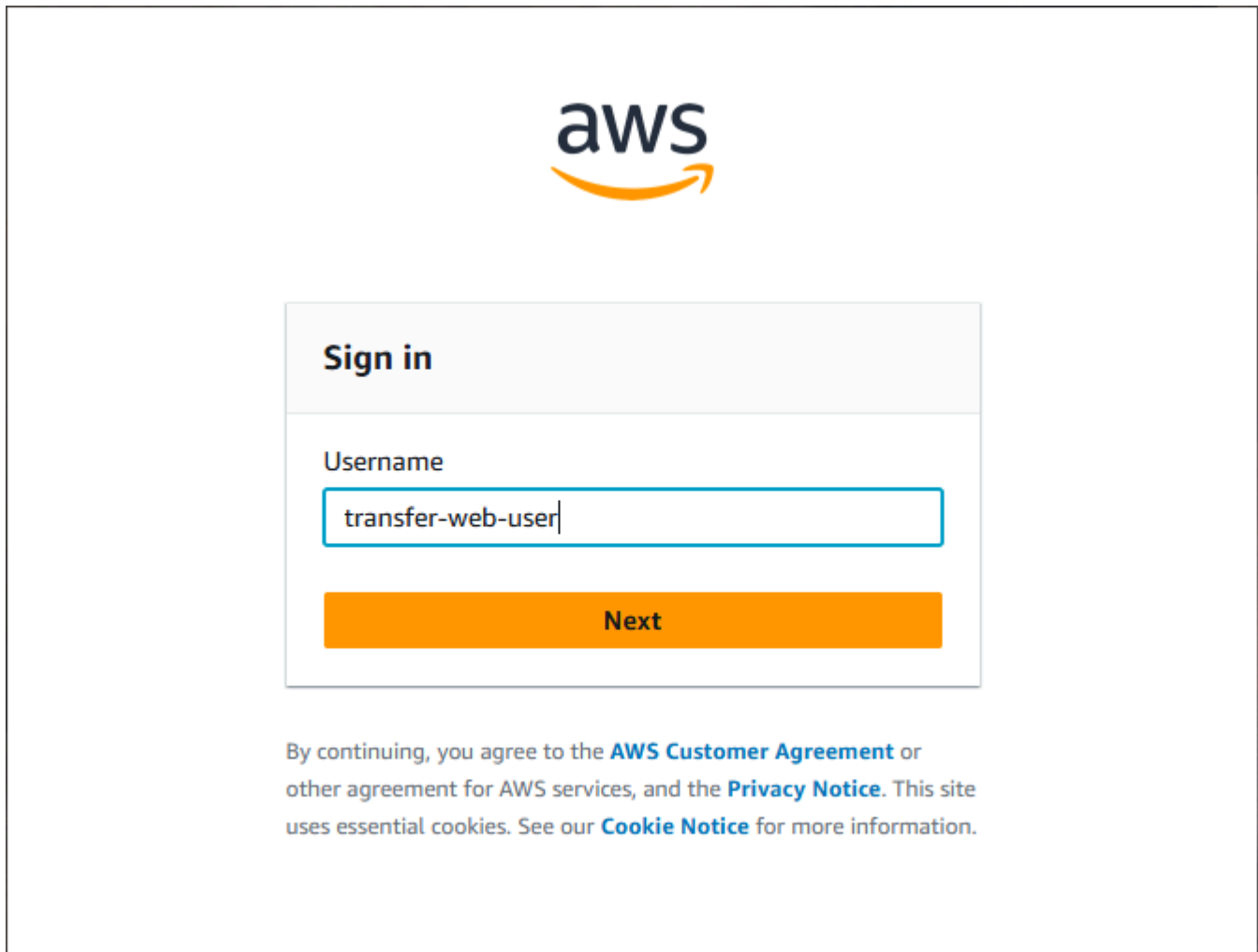
Pengalaman pengguna untuk pengguna IAM Identity Center

Bagian ini menjelaskan pengalaman pengguna jika organisasi Anda menggunakan IAM Identity Center untuk mengonfigurasi penggunaannya.

Untuk mengakses aplikasi web Transfer Family

1. Anda harus menerima email dari `no-reply@login.awsapps.com` berjudul “Undangan untuk bergabung AWS IAM Identity Center.” Terima undangan untuk mengaktifkan akun pengguna Anda.
2. Dalam pesan, pilih URL di bawah URL portal AWS akses Anda.

Ini membawa Anda ke layar AWS masuk.



aws

Sign in

Username

transfer-web-user

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

3. Masukkan kredensial Anda dan pilih Masuk.

Ini membawa Anda ke Portal akses AWS, yang menunjukkan daftar aplikasi Anda yang tersedia.

4. Pilih aplikasi untuk aplikasi web Transfer Family Anda.

Pengalaman pengguna untuk pengguna penyedia identitas pihak ketiga

Jika organisasi Anda tidak menggunakannya AWS IAM Identity Center untuk mengonfigurasi penggunanya, pengalaman orientasi Anda akan bergantung pada aplikasi penyedia identitas yang mereka gunakan untuk mengonfigurasi pengguna akhir mereka. Setelah Anda mengautentikasi dan masuk, antarmuka aplikasi web Anda sama dengan yang dijelaskan di bagian berikutnya.

Note

Jika pengguna termasuk dalam beberapa grup Direktori Aktif yang memiliki hibah ke bucket Amazon S3 yang sama, bucket akan muncul beberapa kali di antarmuka aplikasi web. Hal ini terjadi karena aplikasi web mencantumkan semua hibah tingkat atas yang terkait dengan UID atau GID pengguna, termasuk hibah duplikat ke bucket yang sama. Untuk mencegah daftar duplikat, administrator dapat menggabungkan beberapa hibah sehingga setiap pengguna hanya memiliki satu hibah per lokasi Amazon S3.

Antarmuka pengguna akhir Transfer Family

Setelah Anda mengautentikasi dan masuk, Anda dapat berinteraksi dengan aplikasi web.

Ada empat pandangan utama.

- Halaman rumah: Halaman beranda Anda mencantumkan lokasi S3, yang dapat Anda akses, serta izin untuk masing-masing lokasi. Lokasi S3 adalah bucket atau awalan S3, yang dapat Anda tentukan saat menggunakan S3 Access Grants. Ini adalah tampilan awal untuk pengguna yang menunjukkan sumber daya S3 tingkat root yang dapat diakses oleh pengguna akhir Anda dan izin untuk setiap lokasi S3.

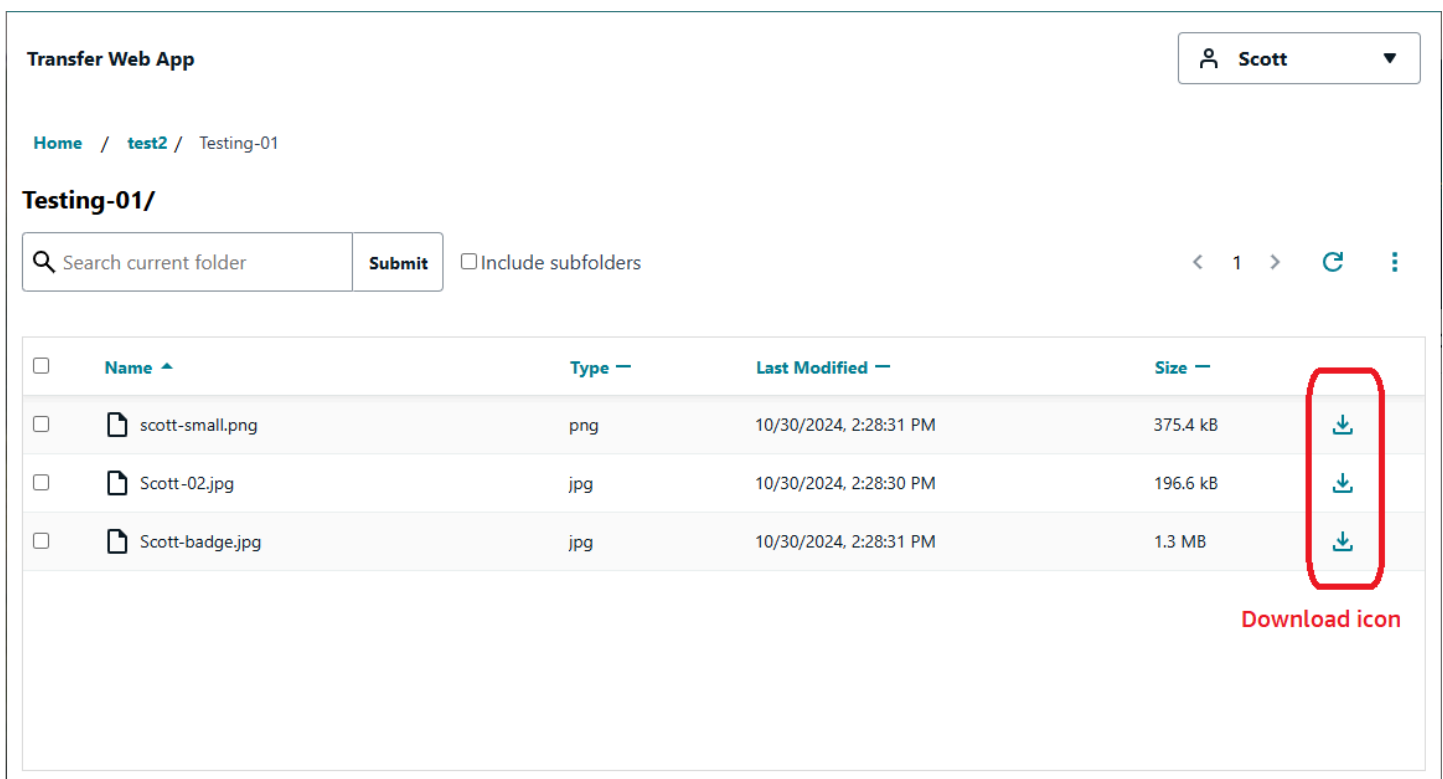
The screenshot shows the Amazon Transfer Family Home page. At the top left is the Amazon logo. At the top right is a user profile dropdown menu. Below the logo is the heading "Home". Under "Home" is a search bar with the placeholder text "Filter folders and files" and a "Submit" button. To the right of the search bar are navigation controls: "< 1 >" and a refresh icon. Below the search bar is a table with three columns: "Folder", "Bucket", and "Permission". The "Folder" column has a dropdown arrow and contains the text "test". The "Bucket" column contains the text "test" and is highlighted with a green box. The "Permission" column contains the text "READWRITE" and is highlighted with a red box. Below the "Bucket" column is the text "Buckets the web app can access". Below the "Permission" column is the text "Permissions for the bucket".

Folder	Bucket	Permission
test	test	READWRITE

- Detail lokasi: Tampilan ini memungkinkan pengguna untuk menelusuri file dan folder di S3, dan mengunggah atau mengunduh file.
- Tindakan lokasi: Setelah Anda memilih tindakan (seperti Unggah), tindakan tersebut akan membuka tampilan lain dari lokasi file.
- Elipsis vertikal: Ikon elipsis vertikal membuka menu Tindakan.

Tindakan yang tersedia

Sebagian besar tindakan tersedia dari menu Tindakan. Untuk tindakan utama lainnya, mengunduh file, Anda menggunakan ikon unduhan setelah Anda memilih file (saat ini, Anda hanya dapat mengunduh satu file pada satu waktu).



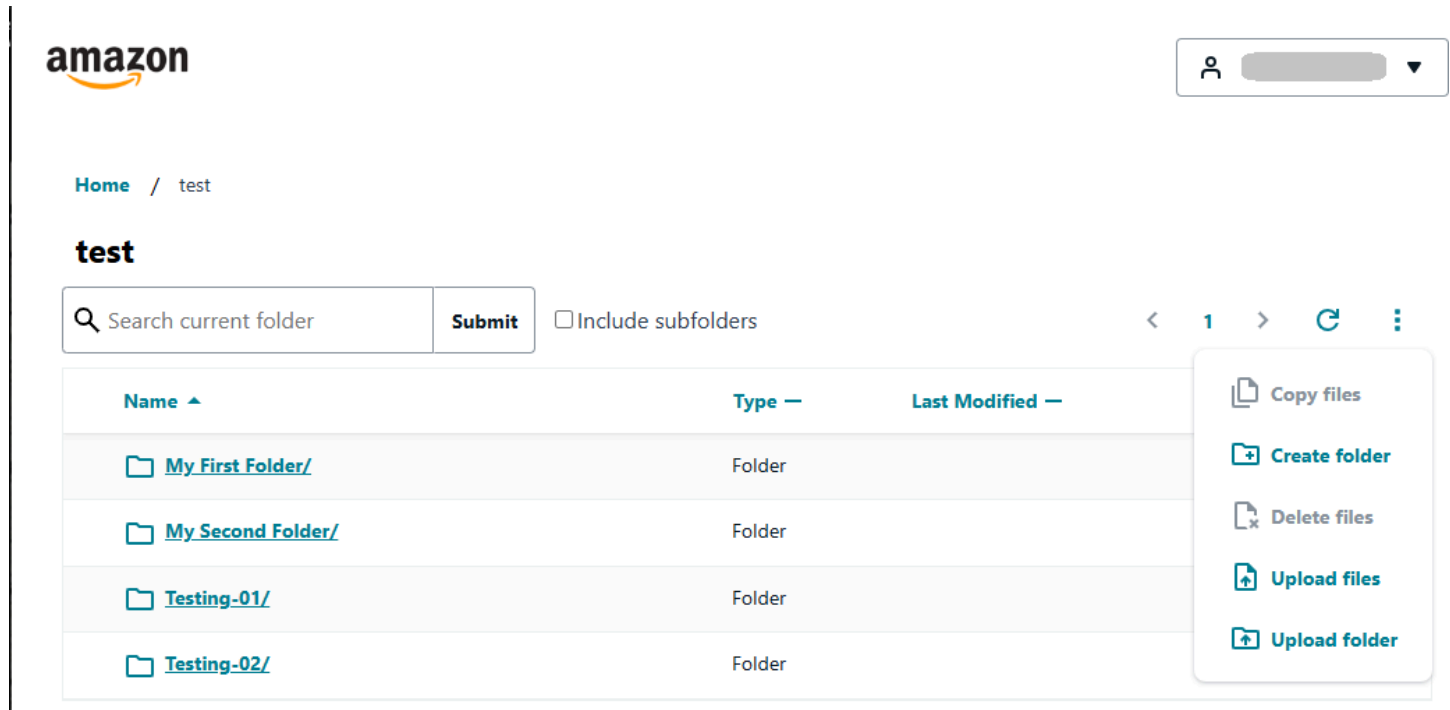
The screenshot shows the AWS Transfer Web App interface. At the top, it says "Transfer Web App" and "Scott" is logged in. The breadcrumb trail is "Home / test2 / Testing-01". The current view is "Testing-01/". There is a search bar "Search current folder" and a "Submit" button. A checkbox "Include subfolders" is also present. The file list has columns: Name, Type, Last Modified, and Size. Three files are listed: "scott-small.png", "Scott-02.jpg", and "Scott-badge.jpg". Each file has a download icon (a blue arrow pointing down) in the rightmost column. These download icons are highlighted with a red rectangle. Below the table, the text "Download icon" is written in red.

☐	Name ^	Type —	Last Modified —	Size —	
☐	scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	Download icon
☐	Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	Download icon
☐	Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	Download icon

Dari folder, gunakan menu Tindakan untuk melakukan salah satu tugas berikut:

- Salin satu atau beberapa file ke lokasi lain.
- Buat folder.
- Hapus satu atau lebih file.
- Unggah satu atau lebih file.
- Unggah seluruh folder (termasuk subfolder jika ada).

- Pilih folder dan arahkan ke sana. Anda kemudian dapat melakukan salah satu tindakan yang terdaftar sebelumnya.
- Urutkan berdasarkan halaman.
- Filter berdasarkan nama file atau folder per folder dan subfolder.



The screenshot shows the Amazon S3 console interface. At the top left is the Amazon logo. To the right is a user profile dropdown. Below the logo is a breadcrumb trail: [Home](#) / [test](#). The main heading is **test**. Below this is a search bar with the placeholder text "Search current folder" and a "Submit" button. To the right of the search bar is a checkbox labeled "Include subfolders". Further right are navigation icons: a left arrow, the number "1", a right arrow, a refresh icon, and a three-dot menu icon. The main content area displays a table of folders:

Name ▲	Type —	Last Modified —
 My First Folder/	Folder	
 My Second Folder/	Folder	
 Testing-01/	Folder	
 Testing-02/	Folder	

A context menu is open over the "Testing-01/" folder, displaying the following actions:

-  Copy files
-  Create folder
-  Delete files
-  Upload files
-  Upload folder

AWS Transfer Family Konektor SFTP

Konektor AWS Transfer Family SFTP membuat koneksi dengan server SFTP jarak jauh untuk mentransfer file antara penyimpanan Amazon dan server jarak jauh, menggunakan protokol SFTP. Anda dapat mengirim file dari Amazon S3 ke server SFTP eksternal milik mitra, mengambil file dari server SFTP mitra ke Amazon S3 atau mencantumkan, menghapus, mengganti nama, atau memindahkan file di server jarak jauh. Konektor SFTP mendukung dua jenis jalan keluar: layanan yang dikelola (menggunakan AWS infrastruktur terkelola) dan VPC (perutean melalui VPC Anda menggunakan Amazon VPC Lattice). Dengan menggunakan konektor SFTP, Anda dapat membuat alur kerja transfer file otomatis yang digerakkan oleh peristiwa. AWS

Lihat konektor [AWS Transfer Family SFTP untuk pengenalan singkat tentang konektor SFTP](#) Transfer Family.

Topik

- [Membuat konektor SFTP](#)
- [Konektivitas VPC untuk konektor SFTP](#)
- [Menggunakan konektor SFTP](#)
- [Memantau konektor SFTP](#)
- [Mengelola konektor SFTP](#)
- [Penskalaan dan kuota untuk konektor SFTP](#)
- [Arsitektur referensi menggunakan konektor SFTP](#)

Membuat konektor SFTP

Topik ini menjelaskan cara membuat konektor SFTP. Setiap konektor menyediakan kemampuan untuk terhubung dengan satu server SFTP jarak jauh. Anda melakukan tugas tingkat tinggi berikut untuk mengonfigurasi konektor SFTP.

Note

Untuk VPC-based konektor yang merutekan lalu lintas melalui Virtual Private Cloud Anda, lihat [Buat konektor SFTP dengan jalan keluar VPC-based](#).

1. Simpan kredensi otentikasi untuk konektor di AWS Secrets Manager
2. Buat konektor, dengan menentukan ARN rahasia, URL server jarak jauh atau ARN Konfigurasi Sumber Daya, kebijakan keamanan yang berisi algoritme yang akan didukung oleh konektor, dan pengaturan konfigurasi lainnya.
3. Setelah Anda membuat konektor, Anda dapat mengujinya untuk memastikan bahwa itu dapat membuat koneksi dengan server SFTP jarak jauh.

Memilih jenis jalan keluar konektor SFTP

Saat Anda membuat konektor SFTP, Anda memilih Jenis Jalan Keluar antara “Layanan dikelola” dan “Kisi VPC”.

- **Layanan dikelola (default):** Konektor menggunakan gateway NAT dan alamat IP yang dimiliki oleh AWS Transfer Family untuk merutekan koneksi melalui internet publik. Layanan ini menyediakan 3 alamat IP statis untuk konektor Anda yang perlu diizinkan terdaftar di server jarak jauh untuk membuat koneksi.
- **Kisi VPC:** Konektor merutekan lalu lintas melalui lingkungan VPC Anda menggunakan Amazon VPC Lattice. Gunakan konektivitas VPC untuk konektor SFTP dalam skenario berikut:
 - **Server SFTP pribadi:** Connect ke server SFTP yang hanya dapat diakses dari VPC Anda
 - **On-premises konektivitas:** Connect ke server SFTP lokal melalui atau koneksi AWS Direct Connect AWS Virtual Private Network
 - **Alamat IP khusus:** Sajikan gateway NAT Anda sendiri dan alamat IP Elastis ke server jarak jauh
 - **Kontrol keamanan terpusat:** Rutekan transfer file melalui kontrol pusat ingress/egress organisasi Anda

Matriks berikut membantu Anda memilih jenis konektor yang tepat untuk kasus penggunaan Anda.

Matriks Tipe Jalan Keluar Konektor SFTP

Kemampuan	Egress Type = Layanan dikelola	Jenis Jalan Keluar = Kisi VPC
Konektivitas ke server SFTP yang dihosting secara publik (dapat diakses internet)	Didukung	Didukung ¹

Kemampuan	Egress Type = Layanan dikelola	Jenis Jalan Keluar = Kisi VPC
Konektivitas ke server SFTP yang dihosting secara pribadi (lokal)	Tidak didukung	Didukung ²
Konektivitas ke server SFTP yang di-host secara pribadi (dalam VPC)	Tidak didukung	Didukung
Alamat IP statis disajikan ke server SFTP jarak jauh	Didukung melalui layanan yang disediakan alamat IP statis	Didukung melalui alamat IP statis milik pelanggan
Bandwidth tersedia	50 MBPS per akun	Bandwidth yang lebih tinggi, tersedia dari Resource Gateway dan NAT Gateway milik pelanggan
Perutean lalu lintas ke internet melalui Gateway NAT dan Firewall Jaringan milik pelanggan	Tidak didukung. NAT Gateways dimiliki dan dikelola oleh layanan Transfer Family.	Didukung

¹ Dengan Egress Type = VPC Lattice, konektivitas ke server yang dihosting secara publik didukung menggunakan pengaturan infrastruktur jalan keluar (NAT Gateways) di VPC keluar Anda.

² Dengan Egress Type = VPC Lattice, konektivitas ke server yang dihosting secara pribadi didukung menggunakan jaringan yang ada di VPC Anda, seperti atau VPN. AWS Direct Connect

Memilih mode pengalamatan IP

Saat Anda membuat konektor SFTP dengan jalan keluar yang dikelola layanan, Anda dapat memilih di antara dua mode pengalamatan IP:

- Hanya IPv4 (default): Konektor menggunakan alamat IPv4 secara eksklusif untuk terhubung ke server SFTP jarak jauh. Ini adalah mode default saat membuat konektor melalui konsol, AWS CLI, atau API.
- Dual-stack: Konektor mendukung alamat IPv6 dan IPv4. Dalam mode dual-stack, konektor lebih memilih IPv6 ketika resolusi DNS mengembalikan hasil IPv6, dan menggunakan IPv4 ketika hanya hasil DNS IPv4 yang dikembalikan.

Note

Mode pengalamatan IP hanya berlaku untuk konektor dengan tipe jalan keluar yang dikelola layanan. Konektor yang menggunakan jalan keluar VPC Lattice tidak mendukung pengaturan ini.

Topik

- [Simpan kredensi otentikasi untuk konektor SFTP di Secrets Manager](#)
- [Buat konektor SFTP dengan jalan keluar yang dikelola layanan](#)
- [Buat konektor SFTP dengan jalan keluar VPC-based](#)
- [Uji konektor SFTP](#)

Simpan kredensi otentikasi untuk konektor SFTP di Secrets Manager

Anda dapat menggunakan Secrets Manager untuk menyimpan kredensi pengguna untuk konektor SFTP Anda. Ketika Anda membuat rahasia Anda, Anda harus memberikan nama pengguna. Selain itu, Anda dapat memberikan kata sandi, kunci pribadi, atau keduanya. Lihat perinciannya di [Kuota untuk konektor SFTP](#).

Note

Ketika Anda menyimpan rahasia di Secrets Manager, Anda Akun AWS dikenakan biaya. Untuk informasi tentang harga, lihat [AWS Secrets Manager Harga](#).

Untuk menyimpan kredensi pengguna di Secrets Manager untuk konektor SFTP

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pada panel navigasi kiri, pilih Rahasia.
3. Pada halaman Rahasia, pilih Simpan rahasia baru.
4. Pada halaman Pilih jenis rahasia, untuk tipe Rahasia, pilih Jenis rahasia lainnya.
5. Berikan key/value informasi untuk rahasia Anda: Anda perlu memberikan nama pengguna, dan kunci pribadi atau kata sandi.
 - a. Di bagian Key/value pasangan, pilih Key/valuetab.
 - Kunci — Masukkan **Username**.
 - nilai — Masukkan nama pengguna yang berwenang untuk terhubung ke server mitra.
 - b. Jika Anda ingin memberikan key pair, pilih Add row, dan di bagian Key/value pairs, pilih Key/valuetab.
 - Kunci — Masukkan **PrivateKey**.
 - nilai — tempel di kunci pribadi Anda.

Tip: Data kunci pribadi yang Anda masukkan harus sesuai dengan kunci publik yang disimpan untuk pengguna ini di server SFTP jarak jauh.

 Note

Tidak mungkin menggunakan kunci pribadi yang dilindungi frasa sandi untuk otentikasi dengan konektor SFTP. AWS Transfer Family

Untuk detail tentang cara menghasilkan public/private key pair, lihat [Membuat kunci SSH di macOS, Linux, atau Unix](#).

- c. Jika Anda ingin memberikan kata sandi, pilih Tambah baris, dan di bagian Key/value pasangan, pilih Key/valuetab.
 - Kunci — Masukkan **Password**.
 - nilai — Masukkan kata sandi untuk pengguna.

6. Pilih Berikutnya.
7. Pada halaman Konfigurasi rahasia, masukkan nama dan deskripsi untuk rahasia Anda. Kami menyarankan Anda menggunakan awalan **aws/transfer/** untuk nama tersebut. Misalnya, Anda bisa menyebutkan rahasia Anda **aws/transfer/connector-1**.
8. Pilih Berikutnya, dan kemudian terima default pada halaman Konfigurasi rotasi. Lalu pilih Selanjutnya.
9. Pada halaman Review, pilih Store untuk membuat dan menyimpan rahasia.

Buat konektor SFTP dengan jalan keluar yang dikelola layanan

Prosedur ini menjelaskan cara membuat konektor SFTP dengan menggunakan AWS Transfer Family konsol atau AWS CLI

Console

Untuk membuat konektor SFTP

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor SFTP, lalu pilih Buat konektor SFTP.
3. Di bagian Konfigurasi konektor, untuk tipe Egress, pilih Service managed. Opsi ini menggunakan infrastruktur AWS Transfer Family jalan keluar terkelola. Layanan Transfer Family menyediakan dan mengelola alamat IP statis untuk setiap konektor SFTP.
4. Di bagian Konfigurasi konektor, berikan informasi berikut:

Connector configuration

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

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

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

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

URL of the remote (target) SFTP server

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

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

- Untuk URL, masukkan URL untuk server SFTP jarak jauh. URL ini harus diformat sebagai `sftp://partner-SFTP-server-url`, misalnya `sftp://AnyCompany.com`.

 Note

Secara opsional, Anda dapat memberikan nomor port di URL Anda. Formatnya adalah `sftp://partner-SFTP-server-url:port-number`. Nomor port default (bila tidak ada port yang ditentukan) adalah port 22.

- Untuk peran Access, pilih Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang akan digunakan.
- Pastikan bahwa peran ini menyediakan akses baca dan tulis ke direktori induk dari lokasi file yang digunakan dalam `StartFileTransfer` permintaan.
- Pastikan bahwa peran ini memberikan izin `secretsmanager:GetSecretValue` untuk mengakses rahasia.

 Note

Dalam kebijakan, Anda harus menentukan ARN untuk rahasianya. ARN berisi nama rahasia, tetapi menambahkan nama dengan enam, acak, karakter alfanumerik. ARN untuk rahasia memiliki format berikut.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Pastikan peran ini berisi hubungan kepercayaan yang memungkinkan konektor mengakses sumber daya Anda saat melayani permintaan transfer pengguna Anda. Untuk detail tentang membangun hubungan kepercayaan, lihat [Untuk membangun hubungan kepercayaan](#).

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

```

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

```

Note

Untuk peran akses, contoh memberikan akses ke satu rahasia. Namun, Anda dapat menggunakan karakter wildcard, yang dapat menyimpan pekerjaan jika Anda ingin menggunakan kembali peran IAM yang sama untuk beberapa pengguna dan rahasia. Misalnya, pernyataan sumber daya berikut memberikan izin untuk semua rahasia yang memiliki nama yang dimulai dengan. `aws/transfer`

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Anda juga dapat menyimpan rahasia yang berisi kredensi SFTP Anda di tempat lain. Akun AWS Untuk detail tentang mengaktifkan akses rahasia lintas akun, lihat [Izin untuk AWS Secrets Manager rahasia bagi pengguna di](#) akun lain.

5. Lengkapi konfigurasi konektor:

- (Opsional) Untuk peran Logging, pilih peran IAM untuk konektor yang akan digunakan untuk mendorong peristiwa ke CloudWatch log Anda. Contoh kebijakan berikut mencantumkan izin yang diperlukan untuk mencatat peristiwa untuk konektor SFTP.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

6. Di bagian Konfigurasi SFTP, berikan informasi berikut:

SFTP configuration [Info](#)

Connector credentials [Info](#)
Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1 ▼

↻

Store a new secret ↗

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

📘

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

ssh-rsa AAAAF

Remove

Add trusted host key

Maximum concurrent connections [Info](#)
Select the maximum number of concurrent connections that your connector can create to the remote server

5 ▼

- Untuk kredensi Connector, dari daftar dropdown, pilih nama rahasia AWS Secrets Manager yang berisi kunci pribadi atau kata sandi pengguna SFTP. Anda harus membuat rahasia dan menyimpannya dengan cara tertentu. Lihat perinciannya di [Simpan kredensi otentikasi untuk konektor SFTP di Secrets Manager](#).
- (Opsional) Anda memiliki opsi untuk membuat konektor sambil membiarkan TrustedHostKeys parameter kosong. Namun, konektor Anda tidak akan dapat mentransfer file dengan server jarak jauh sampai Anda memberikan parameter ini dalam konfigurasi konektor Anda. Anda dapat memasukkan kunci host Tepercaya pada saat membuat konektor, atau memperbarui konektor Anda nanti dengan menggunakan informasi kunci host yang dikembalikan oleh tindakan TestConnection konsol atau perintah API. Artinya, untuk kotak teks kunci host tepercaya, Anda dapat melakukan salah satu hal berikut:
 - Berikan Kunci Host Tepercaya pada saat membuat konektor Anda. Tempel di bagian publik dari kunci host yang digunakan untuk mengidentifikasi server eksternal. Anda dapat menambahkan lebih dari satu kunci, dengan memilih Tambahkan kunci host tepercaya untuk menambahkan kunci tambahan. Anda dapat menggunakan ssh-keyscan perintah terhadap server SFTP untuk mengambil kunci yang diperlukan. Untuk detail tentang format dan jenis kunci host tepercaya yang didukung Transfer Family, lihat [SFTPConnectorConfig](#).
 - Biarkan kotak teks Trusted Host Key kosong saat membuat konektor Anda dan perbarui konektor Anda di lain waktu dengan informasi ini. Jika Anda tidak memiliki

informasi kunci host pada saat membuat konektor Anda, Anda dapat membiarkan parameter ini kosong untuk saat ini dan melanjutkan dengan membuat konektor Anda. Setelah konektor dibuat, gunakan ID konektor baru untuk menjalankan `TestConnection` perintah, baik di AWS CLI atau dari halaman detail konektor. Jika berhasil, `TestConnection` akan mengembalikan informasi kunci host yang diperlukan. Anda kemudian dapat mengedit konektor menggunakan konsol (atau dengan menjalankan `UpdateConnector` AWS CLI perintah) dan menambahkan informasi kunci host yang dikembalikan saat Anda menjalankan `TestConnection`.

 Important

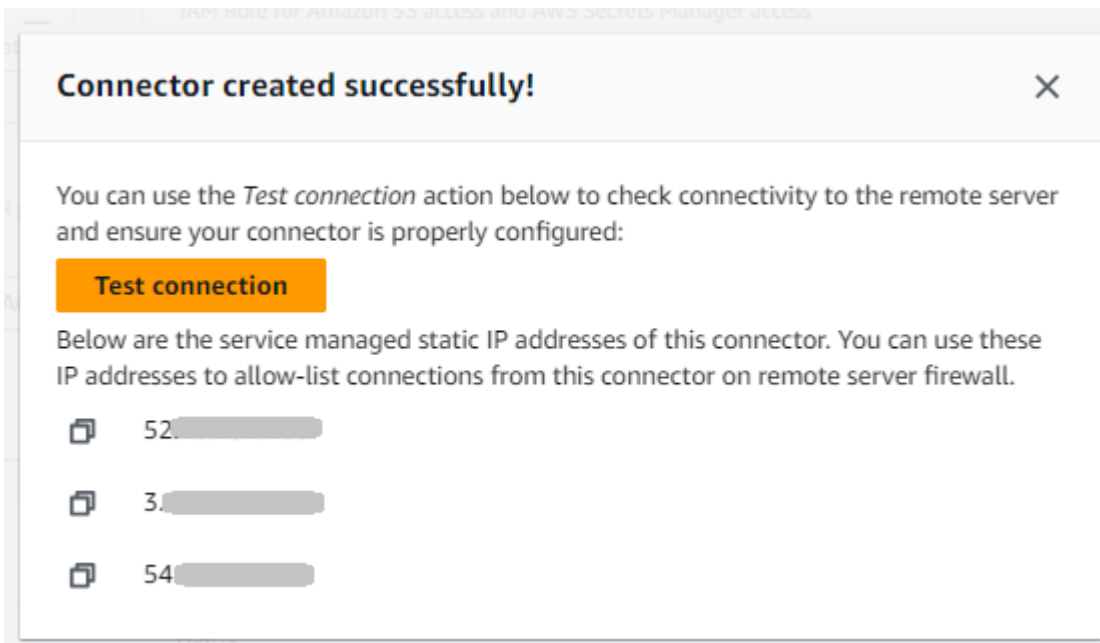
Jika Anda mengambil kunci host server jarak jauh dengan menjalankan `TestConnection`, pastikan Anda melakukan validasi out-of-band pada kunci yang dikembalikan.

Anda harus menerima kunci baru sebagai tepercaya, atau memverifikasi sidik jari yang disajikan dengan sidik jari yang diketahui sebelumnya yang telah Anda terima dari pemilik server SFTP jarak jauh yang Anda sambungkan.

- (Opsional) Untuk Koneksi bersamaan maksimum, dari daftar tarik-turun, pilih jumlah koneksi bersamaan yang dibuat konektor Anda ke server jarak jauh. Pilihan default pada konsol adalah 5.

Pengaturan ini menentukan jumlah koneksi aktif yang dapat dibuat konektor Anda dengan server jarak jauh secara bersamaan. Membuat koneksi bersamaan dapat meningkatkan kinerja konektor dengan mengaktifkan operasi paralel.

7. Di bagian Opsi algoritma kriptografi, pilih kebijakan keamanan dari daftar dropdown di bidang Kebijakan Keamanan. Kebijakan keamanan memungkinkan Anda untuk memilih algoritma kriptografi yang didukung konektor Anda. Untuk detail tentang kebijakan dan algoritme keamanan yang tersedia, lihat [Kebijakan keamanan untuk AWS Transfer Family Konektor SFTP](#).
8. (Opsional) Di bagian Tag, untuk Kunci dan Nilai, masukkan satu atau beberapa tag sebagai pasangan nilai kunci.
9. Setelah Anda mengkonfirmasi semua pengaturan Anda, pilih Buat konektor SFTP untuk membuat konektor SFTP. Jika konektor berhasil dibuat, layar muncul dengan daftar alamat IP statis yang ditetapkan dan tombol koneksi Uji. Gunakan tombol untuk menguji konfigurasi konektor baru Anda.



Halaman Konektor muncul, dengan ID konektor SFTP baru Anda ditambahkan ke daftar. Untuk melihat detail konektor Anda, lihat [Lihat detail konektor SFTP](#).

CLI

Anda menggunakan [create-connector](#) perintah untuk membuat konektor. Untuk menggunakan perintah ini untuk membuat konektor SFTP, Anda harus memberikan informasi berikut.

- URL untuk server SFTP jarak jauh. URL ini harus diformat sebagai `ftp://partner-SFTP-server-url`, misalnya `ftp://AnyCompany.com`.
- Peran akses. Pilih Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang akan digunakan.
 - Pastikan bahwa peran ini menyediakan akses baca dan tulis ke direktori induk dari lokasi file yang digunakan dalam `StartFileTransfer` permintaan.
 - Pastikan bahwa peran ini memberikan izin `secretsmanager:GetSecretValue` untuk mengakses rahasia.

Note

Dalam kebijakan, Anda harus menentukan ARN untuk rahasianya. ARN berisi nama rahasia, tetapi menambahkan nama dengan enam, acak, karakter alfanumerik. ARN untuk rahasia memiliki format berikut.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Pastikan peran ini berisi hubungan kepercayaan yang memungkinkan konektor mengakses sumber daya Anda saat melayani permintaan transfer pengguna Anda. Untuk detail tentang membangun hubungan kepercayaan, lihat [Untuk membangun hubungan kepercayaan](#).

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

```

    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/
transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

Untuk peran akses, contoh memberikan akses ke satu rahasia. Namun, Anda dapat menggunakan karakter wildcard, yang dapat menyimpan pekerjaan jika Anda ingin menggunakan kembali peran IAM yang sama untuk beberapa pengguna dan rahasia. Misalnya, pernyataan sumber daya berikut memberikan izin untuk semua rahasia yang memiliki nama yang dimulai dengan `aws/transfer`

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"

```

Anda juga dapat menyimpan rahasia yang berisi kredensi SFTP Anda di tempat lain. Akun AWS Untuk detail tentang mengaktifkan akses rahasia lintas akun, lihat [Izin untuk AWS Secrets Manager rahasia bagi pengguna di](#) akun lain.

- (Opsional) Pilih peran IAM untuk konektor yang akan digunakan untuk mendorong peristiwa ke CloudWatch log Anda. Contoh kebijakan berikut mencantumkan izin yang diperlukan untuk mencatat peristiwa untuk konektor SFTP.

```

{
  "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/*"
    }
  ]
}

```


}

- Berikan informasi konfigurasi SFTP berikut.
 - ARN rahasia AWS Secrets Manager yang berisi kunci pribadi atau kata sandi pengguna SFTP.
 - Bagian publik dari kunci host yang digunakan untuk mengidentifikasi server eksternal. Anda dapat memberikan beberapa kunci host tepercaya jika Anda mau.

Cara termudah untuk memberikan informasi SFTP adalah dengan menyimpannya ke file. Misalnya, salin contoh teks berikut ke file bernama `testSFTPConfig.json`.

```
// Listing for testSFTPConfig.json
{
  "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
  "TrustedHostKeys": [
    "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
  ]
}
```

- Tentukan kebijakan keamanan untuk konektor Anda, masukkan nama kebijakan keamanan.

Note

SecretId dapat berupa seluruh ARN atau nama rahasia (*example-username-key* dalam daftar sebelumnya).

Kemudian jalankan perintah berikut untuk membuat konektor:

```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5
```

Saat Anda menjelaskan konektor tipe jalan keluar VPC, responsnya mencakup bidang baru:

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/connector-secret"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Perhatikan bahwa `ServiceManagedEgressIpAddresses` nol untuk konektor tipe jalan keluar VPC karena rute lalu lintas melalui VPC Anda alih-alih infrastruktur terkelola. AWS

Buat konektor SFTP dengan jalan keluar VPC-based

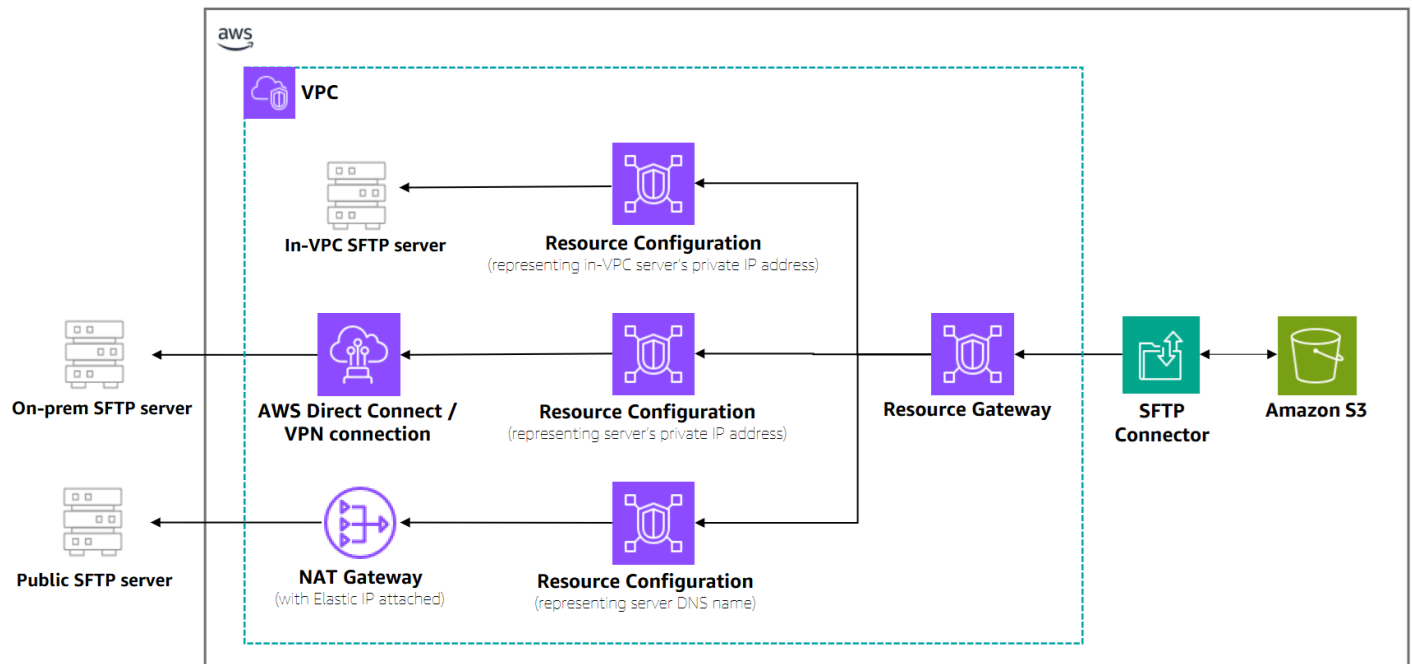
Topik ini memberikan petunjuk langkah demi langkah untuk membuat konektor SFTP dengan konektivitas VPC. LATTICE-enabled Konektor VPC_ menggunakan Amazon VPC Lattice untuk merutekan lalu lintas melalui Virtual Private Cloud Anda, memungkinkan koneksi aman ke titik akhir pribadi atau menggunakan gateway NAT Anda sendiri untuk akses internet.

Kapan menggunakan konektivitas VPC

Gunakan konektivitas VPC untuk konektor SFTP dalam skenario berikut:

- Server SFTP pribadi: Connect ke server SFTP yang hanya dapat diakses dari VPC Anda.
- On-premises konektivitas: Connect ke server SFTP lokal melalui AWS koneksi Direct Connect atau AWS Site-to-Site VPN.

- Alamat IP khusus: Gunakan gateway NAT dan alamat IP Elastis Anda sendiri, termasuk skenario BYOIP.
- Kontrol keamanan terpusat: Rutekan transfer file melalui ingress/egress kontrol pusat organisasi Anda.



Prasyarat untuk konektor VPC_ SFTP LATTICE-enabled

Sebelum membuat konektor VPC_ LATTICE-enabled SFTP, Anda harus menyelesaikan prasyarat berikut:

Cara kerja VPC-based konektivitas

VPC Lattice memungkinkan Anda berbagi sumber daya VPC dengan aman dengan layanan lain. AWS AWS Transfer Family menggunakan jaringan layanan untuk menyederhanakan proses berbagi sumber daya. Komponen kuncinya adalah:

- **Resource Gateway:** Berfungsi sebagai titik akses ke VPC Anda. Anda membuat ini di VPC Anda dengan minimal dua Availability Zone.
- **Konfigurasi Sumber Daya:** Berisi alamat IP pribadi atau nama DNS publik dari server SFTP yang ingin Anda sambungkan.

Saat Anda membuat LATTICE-enabled konektor VPC_, AWS Transfer Family gunakan Forward Access Session (FAS) untuk sementara mendapatkan kredensi Anda dan mengaitkan Konfigurasi Sumber Daya Anda dengan jaringan layanan kami.

Langkah-langkah penyiapan yang diperlukan

1. Infrastruktur VPC: Pastikan Anda memiliki VPC yang dikonfigurasi dengan benar dengan subnet, tabel rute, dan grup keamanan yang diperlukan untuk persyaratan konektivitas server SFTP Anda.
2. Resource Gateway: Buat Resource Gateway di VPC Anda menggunakan perintah VPC Lattice. `create-resource-gateway` Resource Gateway harus dikaitkan dengan subnet di setidaknya dua Availability Zone. Untuk informasi selengkapnya, lihat [Gateway sumber daya](#) di Panduan Pengguna Amazon VPC Lattice.
3. Konfigurasi Sumber Daya: Buat Konfigurasi Sumber Daya yang mewakili server SFTP target menggunakan perintah VPC Lattice. `create-resource-configuration` Anda dapat menentukan:
 - Alamat IP pribadi untuk titik akhir pribadi
 - Nama DNS publik untuk titik akhir publik (alamat IP tidak didukung untuk titik akhir publik)
4. Kredensi otentikasi: Simpan kredensial pengguna SFTP seperti yang dijelaskan dalam. AWS Secrets Manager [Simpan kredensi otentikasi untuk konektor SFTP di Secrets Manager](#)

 Important

Resource Gateway dan Resource Configuration harus dibuat di AWS akun yang sama. Saat membuat Konfigurasi Sumber Daya, Anda harus terlebih dahulu memiliki Resource Gateway di tempatnya.

Untuk informasi selengkapnya tentang konfigurasi sumber daya VPC, lihat [Konfigurasi sumber daya di Panduan Pengguna](#) Amazon VPC Lattice.

 Note

Konektivitas VPC untuk konektor SFTP tersedia di tempat sumber daya Wilayah AWS Amazon VPC Lattice tersedia. Untuk informasi selengkapnya, lihat [FAQ VPC Lattice](#). Dukungan Availability Zone bervariasi menurut wilayah, dan Resource Gateways memerlukan minimal dua Availability Zone.

Buat konektor VPC_ LATTICE-enabled SFTP

Setelah menyelesaikan prasyarat, Anda dapat membuat konektor SFTP dengan konektivitas VPC menggunakan AWS CLI, Management Console, atau SDK. AWS AWS

Console

Untuk membuat konektor VPC_ LATTICE-enabled SFTP

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor SFTP, lalu pilih Buat konektor SFTP.
3. Di bagian Konfigurasi konektor, untuk tipe Egress, pilih VPC Lattice.

Opsi ini merutekan lalu lintas melalui VPC Anda menggunakan Amazon VPC Lattice untuk akses sumber daya lintas VPC. Anda dapat menggunakan opsi ini untuk terhubung ke titik akhir server yang dihosting secara pribadi, merutekan lalu lintas melalui kontrol keamanan VPC Anda, atau menggunakan gateway NAT dan alamat IP Elastis Anda sendiri. Alamat server SFTP jarak jauh direpresentasikan sebagai Konfigurasi Sumber Daya di VPC Anda. Untuk informasi selengkapnya tentang Konfigurasi Sumber Daya, lihat [Konfigurasi sumber daya untuk sumber daya VPC di Panduan Pengguna](#) Amazon VPC Lattice.

4. Lengkapi konfigurasi konektor:
 - Untuk peran Access, pilih Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang akan digunakan.
 - Pastikan bahwa peran ini menyediakan akses baca dan tulis ke direktori induk dari lokasi file yang digunakan dalam `StartFileTransfer` permintaan.
 - Pastikan bahwa peran ini memberikan izin `secretsmanager:GetSecretValue` untuk mengakses rahasia.

Note

Dalam kebijakan, Anda harus menentukan ARN untuk rahasianya. ARN berisi nama rahasia, tetapi menambahkan nama dengan enam, acak, karakter alfanumerik. ARN untuk rahasia memiliki format berikut.

```
arn:aws:secretsmanager:region:account-id:secret:aws/  
transfer/SecretName-6RandomCharacters
```

- Pastikan peran ini berisi hubungan kepercayaan yang memungkinkan konektor mengakses sumber daya Anda saat melayani permintaan transfer pengguna Anda. Untuk detail tentang membangun hubungan kepercayaan, lihat [Untuk membangun hubungan kepercayaan](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-  
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

```
]
}
```

Note

Untuk peran akses, contoh memberikan akses ke satu rahasia. Namun, Anda dapat menggunakan karakter wildcard, yang dapat menyimpan pekerjaan jika Anda ingin menggunakan kembali peran IAM yang sama untuk beberapa pengguna dan rahasia. Misalnya, pernyataan sumber daya berikut memberikan izin untuk semua rahasia yang memiliki nama yang dimulai dengan `aws/transfer`

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Anda juga dapat menyimpan rahasia yang berisi kredensi SFTP Anda di tempat lain. Akun AWS Untuk detail tentang mengaktifkan akses rahasia lintas akun, lihat [Izin untuk AWS Secrets Manager rahasia bagi pengguna di](#) akun lain.

- Untuk ARN Konfigurasi Sumber Daya, masukkan ARN Konfigurasi Sumber Daya Kisi VPC yang mengarah ke server SFTP Anda:

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (Opsional) Untuk peran Logging, pilih peran IAM untuk konektor yang akan digunakan untuk mendorong peristiwa ke CloudWatch log Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

```
]
}
```

5. Di bagian Konfigurasi SFTP, berikan informasi berikut:

- Untuk kredensi Konektor, pilih nama rahasia AWS Secrets Manager yang berisi kunci pribadi atau kata sandi pengguna SFTP.
- Untuk kunci host Tepercaya, tempel di bagian publik dari kunci host yang digunakan untuk mengidentifikasi server eksternal, atau biarkan kosong untuk mengkonfigurasi nanti menggunakan `TestConnection` perintah.

Karena kunci host ini untuk konektor VPC_LATTICE, hapus nama host di kunci

- (Opsional) Untuk koneksi bersamaan maksimum, pilih jumlah koneksi bersamaan yang dibuat konektor Anda ke server jarak jauh (defaultnya adalah 5).
6. Di bagian Opsi algoritma kriptografi, pilih kebijakan keamanan dari daftar dropdown.
7. (Opsional) Di bagian Tag, tambahkan tag sebagai pasangan nilai kunci.
8. Pilih Buat konektor SFTP untuk membuat konektor LATTICE-enabled VPC_ SFTP.

Konektor akan dibuat dengan status PENDING sementara asosiasi sumber daya sedang disediakan, yang biasanya memakan waktu beberapa menit. Setelah status berubah ACTIVE, konektor siap digunakan.

CLI

Gunakan perintah berikut untuk membuat konektor VPC_ LATTICE-enabled SFTP:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

Parameter kunci untuk konektivitas VPC adalah `--egress-config`, yang menentukan ARN Konfigurasi Sumber Daya yang menentukan target server SFTP Anda.

Memantau status konektor VPC

LATTICE-enabled Konektor VPC_ memiliki proses pengaturan asinkron. Setelah pembuatan, pantau status konektor:

- **PENDING:** Konektor sedang disediakan. Penyediaan jaringan layanan sedang berlangsung, yang biasanya memakan waktu beberapa menit.
- **AKTIF:** Konektor siap digunakan dan dapat mentransfer file.
- **ERRORED:** Konektor gagal disediakan. Periksa detail kesalahan untuk informasi pemecahan masalah.

Periksa status konektor menggunakan `describe-connector` perintah:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Selama status **PENDING**, `test-connection` API akan mengembalikan “Konektor tidak tersedia” hingga penyediaan selesai.

Pertimbangan dan batasan

- **Titik akhir publik:** Saat menghubungkan ke titik akhir publik melalui VPC, Anda harus memberikan nama DNS di Konfigurasi Sumber Daya. Alamat IP publik tidak didukung.
- **Ketersediaan regional:** Konektivitas VPC tersedia di pilih. Wilayah AWS Cross-region berbagi sumber daya tidak didukung.
- **Persyaratan Availability Zone:** Resource Gateway harus dikaitkan dengan subnet di setidaknya dua Availability Zone. Tidak semua Availability Zone mendukung VPC Lattice di setiap wilayah.
- **Batas koneksi:** Maksimum 350 koneksi per sumber daya dengan batas waktu idle 350 detik untuk koneksi TCP.

Pertimbangan Biaya

Tidak ada biaya tambahan dari AWS Transfer Family luar biaya layanan reguler. Namun, pelanggan dapat dikenakan biaya tambahan dari Amazon VPC Lattice yang terkait dengan berbagi sumber daya Amazon Virtual Private Cloud mereka, dan biaya gateway NAT jika mereka menggunakan gateway NAT mereka sendiri untuk keluar ke internet.

Untuk informasi AWS Transfer Family harga lengkap, lihat [halaman AWS Transfer Family harga](#).

Contoh konektivitas VPC untuk konektor SFTP

Bagian ini memberikan contoh pembuatan konektor SFTP dengan konektivitas VPC untuk berbagai skenario. Sebelum menggunakan contoh ini, pastikan Anda telah menyelesaikan penyiapan infrastruktur VPC seperti yang dijelaskan dalam dokumentasi konektivitas VPC.

Contoh: Koneksi titik akhir pribadi

Contoh ini menunjukkan cara membuat konektor SFTP yang terhubung ke server SFTP pribadi yang hanya dapat diakses dari VPC Anda.

Prasyarat

1. Buat Resource Gateway di VPC Anda:

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifier vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Buat Konfigurasi Sumber Daya untuk server SFTP pribadi Anda:

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
  --port-ranges 22
```

Buat konektor VPC_ LATTICE-enabled

1. Buat konektor SFTP dengan konektivitas VPC:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Pantau status konektor hingga menjadi ACTIVE:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Server SFTP jarak jauh akan melihat koneksi yang berasal dari alamat IP Resource Gateway dalam rentang CIDR VPC Anda.

Contoh: Titik akhir publik melalui VPC

Contoh ini menunjukkan cara merutekan koneksi ke server SFTP publik melalui VPC Anda untuk memanfaatkan kontrol keamanan terpusat dan menggunakan alamat IP NAT Gateway Anda sendiri.

Prasyarat

1. Buat Resource Gateway di VPC Anda (sama seperti contoh endpoint pribadi).
2. Buat Konfigurasi Sumber Daya untuk server SFTP publik menggunakan nama DNS-nya:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Untuk titik akhir publik, Anda harus menggunakan nama DNS, bukan alamat IP.

Buat konektor

- Buat konektor SFTP:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

Lalu lintas akan mengalir dari konektor ke Resource Gateway Anda, kemudian melalui NAT Gateway Anda untuk mencapai server SFTP publik. Server jarak jauh akan melihat alamat IP Elastis NAT Gateway Anda sebagai sumbernya.

Contoh: titik akhir Cross-account pribadi

Contoh ini menunjukkan cara menghubungkan ke server SFTP pribadi di AWS akun yang berbeda dengan menggunakan berbagi sumber daya.

Note

Jika Anda sudah mengaktifkan berbagi sumber daya lintas VPC melalui mekanisme lain, seperti AWS Transit Gateway, Anda tidak perlu mengonfigurasi pembagian sumber daya yang dijelaskan di sini. Mekanisme routing yang ada, seperti tabel rute Transit Gateway, secara otomatis digunakan oleh konektor SFTP. Anda hanya perlu membuat Konfigurasi Sumber Daya di akun yang sama tempat Anda membuat konektor SFTP.

Akun A (Penyedia Sumber Daya) - Bagikan Konfigurasi Sumber Daya

1. Buat Resource Gateway dan Resource Configuration di Akun A (sama seperti contoh sebelumnya).
2. Bagikan Konfigurasi Sumber Daya dengan Akun B menggunakan AWS Resource Access Manager:

```
aws ram create-resource-share \
  --name cross-account-sftp-share \
  --resource-arns arn:aws:vpc-lattice:us-
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \
  --principals 222222222222
```

Akun B (Konsumen Sumber Daya) - Terima dan Gunakan Saham

1. Terima undangan berbagi sumber daya:

```
aws ram accept-resource-share-invitation \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/invitation-id
```

2. Buat konektor SFTP di Akun B:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \  
  --sftp-config UserSecretId=cross-account-server-  
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

Konektor di Akun B sekarang dapat mengakses server SFTP pribadi di Akun A melalui Konfigurasi Sumber Daya bersama.

Skenario pemecahan masalah umum

Berikut adalah solusi untuk masalah umum saat membuat konektor VPC_LATTICE-enabled :

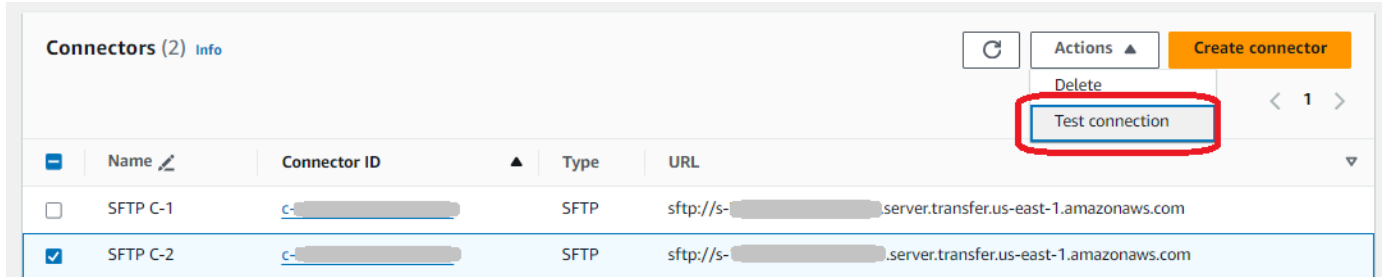
- Konektor terjebak dalam status PENDING: Periksa apakah Resource Gateway Anda AKTIF dan memiliki subnet di Availability Zone yang didukung. Jika konektor masih macet dengan status PENDING, panggil UpdateConnector menggunakan parameter konfigurasi yang sama yang Anda gunakan pada awalnya. Ini memicu peristiwa status baru yang mungkin menyelesaikan masalah.
- Batas waktu koneksi: Verifikasi aturan grup keamanan mengizinkan lalu lintas di port 22 dan perutean VPC Anda benar.
- Masalah resolusi DNS: Untuk titik akhir publik, pastikan VPC Anda memiliki konektivitas internet melalui NAT Gateway atau Internet Gateway.
- Cross-account akses ditolak: Verifikasi pembagian sumber daya diterima dan ARN Konfigurasi Sumber Daya sudah benar. Jika kebijakan izin yang tepat dilampirkan ke konfigurasi sumber daya saat akun asal membuat pembagian sumber daya, izin ini diperlukan: vpc-lattice:AssociateViaAWSService,, vpc-lattice:AssociateViaAWSService-EventsAndStates vpc-lattice:CreateServiceNetworkResourceAssociation, vpc-lattice:GetResourceConfiguration.

Uji konektor SFTP

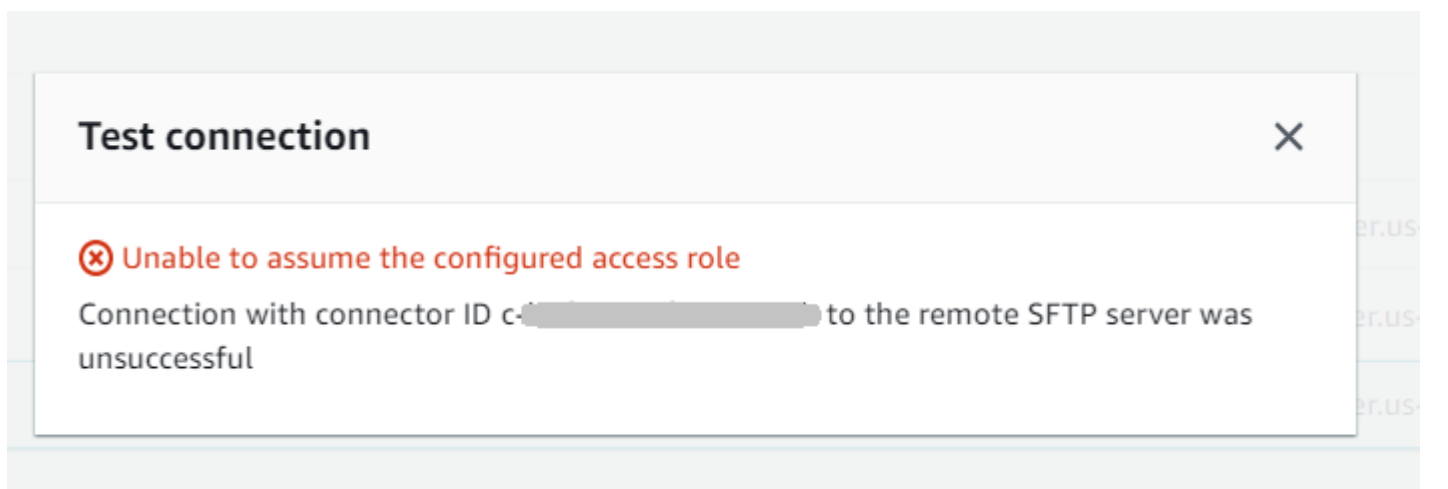
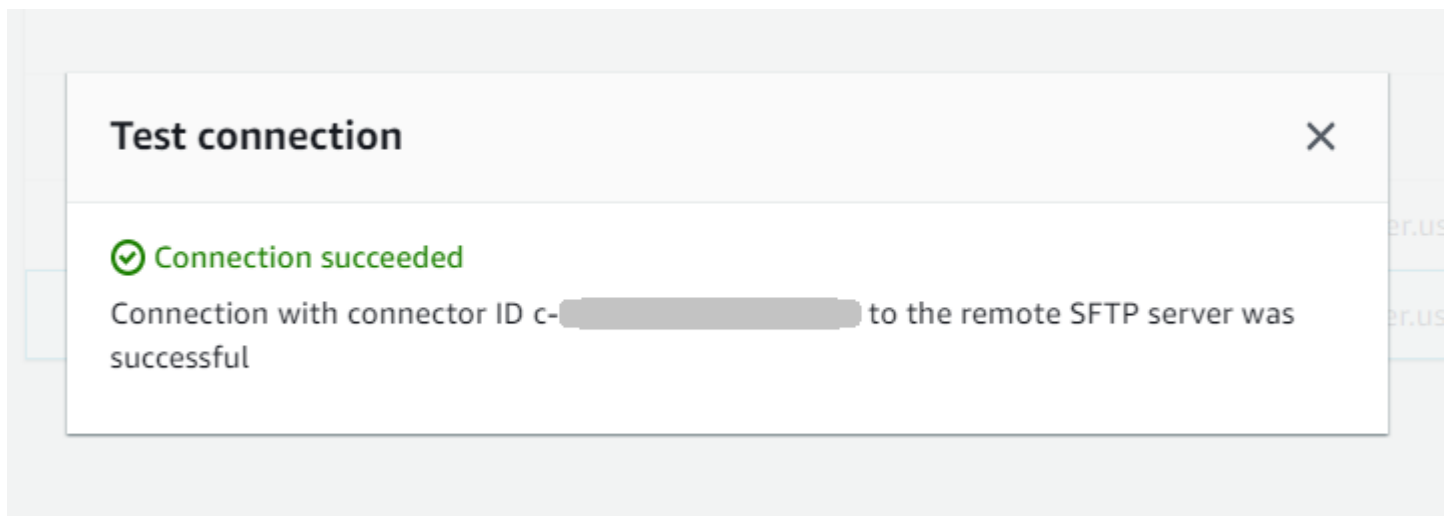
Setelah Anda membuat konektor SFTP, kami sarankan Anda mengujinya sebelum mencoba mentransfer file apa pun menggunakan konektor baru Anda.

Untuk menguji konektor SFTP

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor SFTP, dan pilih konektor.
3. Dari menu Tindakan, pilih Uji koneksi.



Sistem mengembalikan pesan, menunjukkan apakah tes lulus atau gagal. Jika tes gagal, sistem memberikan pesan kesalahan berdasarkan alasan pengujian gagal.



 Note

Untuk menggunakan API untuk menguji konektor Anda, lihat dokumentasi [TestConnectionAPI](#).

Konektivitas VPC untuk konektor SFTP

AWS Transfer Family Konektor SFTP mendukung konektivitas ke server SFTP jarak jauh melalui lingkungan VPC Anda menggunakan Amazon VPC Lattice. Ini memungkinkan Anda untuk terhubung dengan server SFTP yang dihosting secara pribadi atau merutekan lalu lintas internet melalui kontrol keamanan VPC Anda, dan menggunakan gateway NAT dan alamat IP Elastis Anda sendiri.

Jenis jalan keluar

Konektor SFTP dapat menggunakan salah satu dari dua jenis jalan keluar:

- Layanan Dikelola (default): Konektor menggunakan gateway NAT dan alamat IP yang dimiliki oleh AWS Transfer Family untuk merutekan koneksi melalui internet publik.
- VPC_LATTICE: Konektor merutekan lalu lintas melalui lingkungan VPC Anda menggunakan Resource Access. Cross-VPC

Kapan menggunakan konektivitas VPC

Gunakan konektivitas VPC untuk konektor SFTP dalam skenario berikut:

- Server SFTP pribadi: Connect ke server SFTP yang hanya dapat diakses dari VPC Anda.
- On-premises konektivitas: Connect ke server SFTP lokal melalui AWS koneksi Direct Connect atau AWS Site-to-Site VPN.
- Alamat IP khusus: Gunakan gateway NAT dan alamat IP Elastis Anda sendiri, termasuk skenario BYOIP.
- Kontrol keamanan terpusat: Rutekan transfer file melalui ingress/egress kontrol pusat organisasi Anda.

Persyaratan

Sebelum membuat konektor VPC_ LATTICE-enabled SFTP, Anda perlu:

- VPC dan infrastruktur terkait (subnet, tabel rute, grup keamanan)
- Resource Gateway di VPC Anda (minimal dua Availability Zone)
- Konfigurasi Sumber Daya yang menentukan server SFTP target

Untuk petunjuk penyiapan terperinci, lihat [Buat konektor VPC_LATTICE-enabled SFTP](#). Dan, sebagai contoh, lihat [Contoh konektivitas VPC untuk konektor SFTP](#).

Menggunakan konektor SFTP

Topik ini menjelaskan cara melakukan operasi file yang didukung menggunakan konektor SFTP Anda. Anda juga dapat menemukan contoh perintah untuk melakukan operasi ini dengan memilih detail konektor Anda di AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.

Setelah Anda membuat konektor SFTP, Anda dapat menggunakannya untuk melakukan operasi file berikut di server SFTP jarak jauh yang terkait dengannya.

- Kirim file dari Amazon S3 ke server SFTP jarak jauh.
- Ambil file dari server SFTP jarak jauh ke Amazon S3.
- Daftar file dan sub-folder dari direktori di server SFTP jarak jauh.
- Hapus, ganti nama, atau pindahkan file dan direktori di server SFTP jarak jauh.

Untuk detail tentang membuat konektor, lihat [Membuat konektor SFTP](#).

Topik

- [Transfer file](#)
- [Daftar isi direktori jarak jauh](#)
- [Memindahkan, mengganti nama, atau menghapus file atau direktori di server jarak jauh](#)

Transfer file

Topik

- [Mengirim dan mengambil file dengan menggunakan konektor SFTP](#)

Mengirim dan mengambil file dengan menggunakan konektor SFTP

Untuk mengirim dan mengambil file menggunakan konektor SFTP, Anda menggunakan operasi [StartFileTransfer](#) API dan menentukan parameter berikut, tergantung apakah Anda mengirim file (transfer keluar) atau menerima file (transfer masuk). Perhatikan bahwa setiap `StartFileTransfer` permintaan dapat berisi 10 jalur berbeda.

Note

Secara default, konektor SFTP memproses satu file pada satu waktu, mentransfer file secara berurutan. Anda memiliki opsi untuk mempercepat kinerja transfer dengan meminta konektor Anda membuat sesi bersamaan dengan server jarak jauh yang mendukung sesi bersamaan dari pengguna yang sama, dan memproses hingga 5 file secara paralel.

Untuk mengaktifkan koneksi bersamaan untuk konektor apa pun, Anda dapat mengedit pengaturan Koneksi konkuren maksimum saat membuat atau memperbarui konektor. Lihat perinciannya di [Buat konektor SFTP dengan jalan keluar yang dikelola layanan](#).

- Transfer keluar
 - `send-file-paths` berisi dari satu hingga sepuluh jalur file sumber, untuk file yang akan ditransfer ke server SFTP mitra.
 - `remote-directory-path` adalah jalur jarak jauh untuk mengirim file ke server SFTP pelanggan.
- Transfer masuk
 - `retrieve-file-paths` berisi dari satu hingga sepuluh jalur jarak jauh. Setiap jalur menentukan lokasi untuk mentransfer file dari server SFTP mitra ke server Transfer Family Anda.
 - `local-directory-path` adalah lokasi Amazon S3 (bucket dan awalan opsional) tempat file Anda disimpan.

Untuk mengirim file, Anda menentukan `remote-directory-path` parameter `send-file-paths` dan. Anda dapat menentukan hingga 10 file untuk `send-file-paths` parameter. Contoh perintah berikut mengirimkan file bernama `/amzn-s3-demo-source-bucket/file1.txt` dan `/amzn-s3-demo-source-bucket/file2.txt`, terletak di penyimpanan Amazon S3, ke `/tmp` direktori di server SFTP mitra Anda. Untuk menggunakan perintah contoh ini, ganti *amzn-s3-demo-source-bucket* dengan bucket Anda sendiri.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Untuk mengambil file, Anda menentukan `local-directory-path` parameter `retrieve-file-paths` dan. Contoh berikut mengambil file `/my/remote/file1.txt` dan `/my/remote/file2.txt` di server SFTP mitra, dan menempatkannya di lokasi Amazon S3 `/amzn-s3-demo-bucket/`. *prefix* Untuk menggunakan perintah contoh ini, ganti *user input placeholders* dengan informasi Anda sendiri.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/
remote/file2.txt \
  --local-directory-path /amzn-s3-demo-bucket/prefix --connector-id
c-2222BBBB3333CCCC4 --region us-east-2
```

Contoh sebelumnya menentukan jalur absolut pada server SFTP. Anda juga dapat menggunakan jalur relatif: yaitu jalur yang relatif terhadap direktori home pengguna SFTP. Misalnya, jika pengguna SFTP `marymajor` dan direktori home mereka di server SFTP adalah `/users/marymajor/`, perintah berikut dikirim ke `/amzn-s3-demo-source-bucket/file1.txt` `/users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

Daftar isi direktori jarak jauh

Sebelum Anda mengambil file dari server SFTP jarak jauh, Anda dapat mengambil konten direktori di server SFTP jarak jauh. Untuk melakukan ini, Anda menggunakan operasi [StartDirectoryListingAPI](#).

Contoh berikut mencantumkan isi home folder pada server SFTP jarak jauh, yang ditentukan dalam konfigurasi konektor. Hasilnya ditempatkan ke lokasi Amazon S3 `/amzn-s3-demo-bucket/connector-files`, dan ke dalam file bernama `c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`

```
aws transfer start-directory-listing \
  --connector-id c-AAAA1111BBBB2222C \
```

```
--output-directory-path /amzn-s3-demo-bucket/example/connector-files \
--remote-directory-path /home
```

AWS CLI Perintah ini mengembalikan ID daftar dan nama file yang berisi hasil.

```
{
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
  "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

 Note

Konvensi penamaan untuk file output adalah *connector-ID-listing-ID.json*.

File JSON berisi informasi berikut:

- **filePath**: jalur lengkap file jarak jauh, relatif terhadap direktori permintaan daftar untuk konektor SFTP Anda di server jarak jauh.
- **modifiedTimestamp**: terakhir kali file diubah, dalam hitungan detik, format Coordinated Universal Time (UTC). Bidang ini bersifat opsional. Jika atribut file jarak jauh tidak berisi stempel waktu, atribut tersebut dihilangkan dari daftar file.
- **size**: ukuran file, dalam byte. Bidang ini bersifat opsional. Jika atribut file jarak jauh tidak berisi ukuran file, itu dihilangkan dari daftar file.
- **path**: jalur lengkap direktori jarak jauh, relatif terhadap direktori permintaan daftar untuk konektor SFTP Anda di server jarak jauh.
- **truncated**: bendera yang menunjukkan apakah output daftar berisi semua item yang terkandung dalam direktori jarak jauh atau tidak. Jika nilai **truncated** output Anda benar, Anda dapat meningkatkan nilai yang disediakan dalam atribut **max-items** input opsional untuk dapat mencantumkan lebih banyak item (hingga ukuran daftar maksimum yang diizinkan 200.000 item).

Berikut ini adalah contoh isi dari file output (c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json), di mana direktori remote berisi dua file dan dua sub-direktori (path).

```
{
  "files": [
    {
```

```
    "filePath": "/home/what.txt",
    "modifiedTimestamp": "2024-01-30T20:34:54Z",
    "size" : 2323
  },
  {
    "filePath": "/home/how.pgp",
    "modifiedTimestamp": "2024-01-30T20:34:54Z",
    "size" : 4691
  }
],
"paths": [
  {
    "path": "/home/magic"
  },
  {
    "path": "/home/aws"
  },
],
"truncated": "false"
}
```

Memindahkan, mengganti nama, atau menghapus file atau direktori di server jarak jauh

Topik

- [Memindahkan atau mengganti nama file atau direktori di server SFTP jarak jauh](#)
- [Hapus file atau direktori di server SFTP jarak jauh](#)

Memindahkan atau mengganti nama file atau direktori di server SFTP jarak jauh

Anda dapat menggunakan konektor SFTP untuk memindahkan atau mengganti nama file dan direktori pada server SFTP jarak jauh. Perhatikan bahwa server jarak jauh perlu mendukung operasi ini agar pemrosesan berhasil menggunakan konektor.

Beberapa kasus penggunaan umum adalah sebagai berikut.

- Server jarak jauh menghasilkan atau menerima file baru setiap jam, dengan nama file yang sama tetapi stempel waktu yang berbeda. Untuk menjaga agar folder utama tetap up to date (sehingga hanya berisi file terbaru), Anda dapat menggunakan konektor untuk memindahkan file lama ke folder yang diarsipkan.

- Anda menggunakan konektor untuk mencantumkan semua file di direktori jarak jauh, lalu mentransfer semua file ke penyimpanan lokal Anda. Anda kemudian dapat menggunakan konektor untuk memindahkan file ke folder yang diarsipkan di server jarak jauh.

Anda harus menggunakan `StartRemoteMove` panggilan untuk setiap file atau direktori yang ingin Anda proses, karena perintah mengambil satu sumber dan file tujuan atau direktori sebagai argumen. Namun, Anda dapat mempercepat kinerja dengan meminta konektor membuat sesi bersamaan dengan server jarak jauh yang mendukung sesi bersamaan dari pengguna yang sama, dan `move/rename` hingga 5 file secara paralel.

Contoh berikut memindahkan file di server SFTP jarak jauh dari `/source/folder/sourceFile` ke `/destination/targetFile`, dan mengembalikan pengenal unik untuk operasi.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
--source-path /source/folder/sourceFile --target-path /destination/targetFile
```

Note

Untuk `move/rename` operasi, Transfer Family menggunakan SFTP `SSH_FXP_RENAME` perintah standar untuk melakukan `move/rename` operasi.

Hapus file atau direktori di server SFTP jarak jauh

Anda dapat menggunakan konektor SFTP untuk menghapus file atau direktori di server SFTP jarak jauh. Perhatikan bahwa server jarak jauh perlu mendukung operasi ini agar pemrosesan berhasil menggunakan konektor.

Note

Hapus operasi untuk direktori jarak jauh hanya didukung untuk direktori kosong.

Beberapa kasus penggunaan umum adalah sebagai berikut.

- Anda menggunakan konektor untuk mengambil file dari server SFTP jarak jauh, menyimpannya di bucket Amazon S3 Anda, lalu mengenkripsinya. Terakhir, Anda dapat menggunakan konektor untuk menghapus file yang tidak terenkripsi di server jarak jauh.

- Anda menggunakan konektor untuk mencantumkan semua file di direktori jarak jauh, lalu mentransfer semua file ke penyimpanan lokal Anda. Anda kemudian dapat menggunakan konektor untuk menghapus semua file yang Anda transfer. Anda juga dapat menghapus direktori jarak jauh jika Anda mau.

Anda harus menggunakan `StartRemoteDelete` panggilan untuk setiap file atau direktori yang ingin Anda hapus, karena perintah mengambil satu file atau direktori sebagai argumen. Namun, Anda dapat mempercepat kinerja dengan meminta konektor membuat sesi bersamaan dengan server jarak jauh yang mendukung sesi bersamaan dari pengguna yang sama, dan menghapus hingga 5 files/directories secara paralel.

Contoh berikut menghapus file di server SFTP jarak jauh di jalur `/delete/folder/deleteFile`, dan mengembalikan pengenalan unik untuk operasi.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \
--delete-path /delete/folder/deleteFile
```

Note

Untuk operasi hapus, Transfer Family menggunakan `SSH_FXP_REMOVE` perintah standar untuk menghapus file, dan `SSH_FXP_RMDIR` untuk menghapus direktori.

Memantau konektor SFTP

Anda dapat memantau status operasi konektor Anda menggunakan salah satu cara berikut. Pilih pendekatan yang memenuhi kebutuhan Anda.

Gunakan API konektor untuk menanyakan status permintaan transfer file

Untuk melacak kemajuan operasi transfer file, Anda menggunakan operasi [ListFileTransferResults](#) API, yang mengembalikan pembaruan real-time dan informasi terperinci tentang status setiap file individu yang ditransfer dalam operasi transfer file tertentu. Anda menentukan transfer file dengan memberikan ID Konektor dan ID TransfERNYA. Contoh berikut mengembalikan daftar file untuk ID konektor `a-11112222333344444` dan `aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111` Transfer-ID.

```
aws transfer list-file-transfer-results --connector-id a-1111222233334444 --transfer-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

Hasil transfer file tersedia hingga 7 hari setelah Anda memanggil operasi `ListFileTransferResults` API.

Anda juga dapat melihat log dan peristiwa untuk permintaan transfer file Anda yang menggunakan konektor SFTP. EventBridge Acara Amazon untuk Transfer Family dijelaskan dalam [Acara konektor SFTP](#). Untuk melihat entri CloudWatch log Transfer Family, lihat [Melihat aliran log Transfer Family](#).

Lihat acara konektor SFTP di Amazon EventBridge

Untuk setiap operasi yang dilakukan oleh konektor SFTP, Transfer Family secara otomatis menghasilkan dan mengirim acara ke bus acara default di akun Amazon EventBridge Anda. Peristiwa berisi metadata terperinci tentang operasi, termasuk status operasi. Anda dapat berlangganan acara ini EventBridge, menerapkan filter pada kriteria peristiwa tertentu seperti status operasi, dan secara otomatis memicu tindakan hilir berdasarkan status. Untuk detail tentang peristiwa yang dihasilkan oleh operasi konektor SFTP, lihat [Acara konektor SFTP](#).

Lihat log konektor SFTP di Amazon CloudWatch

Semua operasi konektor SFTP menghasilkan log masuk terperinci. CloudWatch Misalnya entri log yang dihasilkan oleh konektor SFTP, lihat [Contoh entri log untuk konektor SFTP](#).

Memantau konektor tipe jalan keluar VPC

Konektor tipe jalan keluar VPC memberikan kemampuan pemantauan dan pertimbangan tambahan di luar konektor terkelola layanan standar:

Pemantauan status konektor

Konektor `VPC_LATTICE` menyertakan informasi tambahan untuk membantu Anda memantau status penyediaan dan operasional:

- `EgressType` bidang: Pertunjukan VPC untuk konektor tipe jalan keluar `VPC_LATTICE`

- EgressConfig bidang: Berisi Konfigurasi Sumber Daya ARN dan informasi port

Memantau status konektor menggunakan `describe-connector` API:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Pemantauan biaya VPC Lattice

Konektor tipe jalan keluar VPC dikenakan biaya Kisi VPC tambahan yang harus Anda pantau:

- Biaya penyedia sumber daya: Anda ditagih \$0. 006/GB untuk pemrosesan data sebagai penyedia sumber daya (ditagih langsung oleh VPC Lattice)
- Biaya konsumen sumber daya: AWS Transfer Family menyerap \$0. 01/GB biaya konsumen sumber daya (1 PB pertama)
- Biaya NAT Gateway: Untuk titik akhir publik yang diakses melalui VPC, tambahan NAT Gateway dan biaya transfer data mungkin berlaku
- Biaya Transfer Family: Standar \$0. 40/GB Biaya pemrosesan data masih berlaku

Pantau penggunaan dan biaya VPC Lattice melalui konsol AWS Cost and Billing, penyaringan oleh layanan VPC Lattice.

Pemantauan jaringan untuk konektor VPC

Pantau aktivitas dan kinerja jaringan untuk konektor tipe jalan keluar VPC:

- VPC Flow Logs: Aktifkan VPC Flow Logs untuk memantau pola lalu lintas jaringan antara Resource Gateways dan server SFTP
- Log akses VPC Lattice: VPC Lattice menyediakan log akses yang menunjukkan alamat source/destination IP, waktu koneksi, dan volume transfer data
- Pemantauan grup keamanan: Pantau aturan grup keamanan dan pola lalu lintas untuk memastikan kontrol akses jaringan yang tepat
- Pemantauan resolusi DNS: Memantau waktu resolusi DNS dan kegagalan untuk titik akhir jaringan layanan

Contoh entri log akses VPC Lattice:

```
{
```



```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
  "gatewayIpPort": "10.0.1.150:1769",
  "resourceIpPort": "10.0.2.200:22"
}
```

Pemecahan masalah melalui pemantauan

Gunakan data pemantauan untuk memecahkan masalah umum konektor VPC:

- Status TERTUNDA: Pantau kemajuan resolusi DNS dan tunggu status AKTIF sebelum mencoba transfer
- Batas waktu koneksi: Periksa Log Aliran VPC dan aturan grup keamanan untuk lalu lintas yang diblokir di port 22
- Kegagalan transfer: Tinjau CloudWatch log untuk pesan kesalahan terperinci dan log akses VPC Lattice untuk masalah tingkat jaringan
- Masalah kinerja: Pantau log akses VPC Lattice untuk pengaturan waktu koneksi dan metrik throughput

Mengelola konektor SFTP

Topik ini menjelaskan cara melihat dan memperbarui konektor SFTP.

Note

Setiap konektor secara otomatis diberi alamat IP statis yang tetap tidak berubah selama masa pakai konektor. Ini memungkinkan Anda untuk terhubung dengan server SFTP jarak jauh yang hanya menerima koneksi masuk dari alamat IP yang diketahui. Konektor Anda diberi satu set alamat IP statis yang dibagikan oleh semua konektor menggunakan protokol yang sama (SFTP atau AS2) di konektor Anda. Akun AWS Alamat ini tidak didedikasikan khusus untuk akun Anda.

Jika Anda membutuhkan alamat IP khusus yang dapat diprediksi, konfigurasi konektor Anda dengan jalan VPC-based keluar. Untuk informasi selengkapnya, lihat [the section called “Buat konektor SFTP dengan jalan keluar VPC-based”](#).

Perbarui konektor SFTP

Untuk mengubah nilai parameter yang ada untuk konektor Anda, Anda dapat menjalankan `update-connector` perintah. Perintah berikut memperbarui rahasia untuk konektor `connector-id`, di Wilayah `region-id` ke `secret-ARN`. Untuk menggunakan perintah contoh ini, ganti `user input placeholders` dengan informasi Anda sendiri.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
--connector-id connector-id --region region-id
```

Memperbarui pengaturan konektivitas VPC

Anda dapat memperbarui pengaturan konektivitas VPC untuk konektor yang ada, termasuk beralih antara jenis jalan keluar yang dikelola layanan dan VPC atau mengubah ARN Konfigurasi Sumber Daya.

Untuk mengganti konektor dari yang dikelola layanan ke jalan keluar VPC:

```
aws transfer update-connector \
--connector-id connector-id \
--egress-type VPC \
--egress-config ResourceConfigurationArn=resource-configuration-arn
```

Untuk memperbarui ARN Konfigurasi Sumber Daya untuk konektor LATTICE-enabled VPC_:

```
aws transfer update-connector \
--connector-id connector-id \
--egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Saat memperbarui pengaturan konektivitas VPC, status konektor akan berubah menjadi PENDING selama proses konfigurasi ulang. Pantau status konektor menggunakan `describe-connector` perintah.

Lihat detail konektor SFTP

Anda dapat menemukan daftar detail dan properti untuk konektor SFTP di konsol. AWS Transfer Family

Untuk melihat detail konektor

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor.
3. Pilih pengenal di kolom Connector ID untuk melihat halaman detail untuk konektor yang dipilih.

Anda dapat mengubah properti untuk konektor SFTP dengan memilih Edit pada halaman detail konektor.

Memantau status konektor VPC

LATTICE-enabled Konektor VPC_ menyertakan informasi status tambahan untuk membantu Anda memantau proses penyediaan:

- Status: Pertunjukan PENDING, ACTIVE, atau ERROR
- EgressType: Pertunjukan VPC atau SERVICE_MANAGED
- EgressConfig: Berisi ARN Konfigurasi Sumber Daya untuk konektor VPC
- Kesalahan: Memberikan informasi kesalahan terperinci jika konektor dalam ERROR keadaan

Untuk konektor VPC, ServiceManagedEgressIpAddresses bidang akan menjadi nol karena lalu lintas menggunakan alamat IP VPC Anda sebagai gantinya.

Note

Anda bisa mendapatkan banyak informasi ini, meskipun dalam format yang berbeda, dengan menjalankan perintah AWS Command Line Interface (AWS CLI) berikut. Untuk menggunakan perintah contoh ini, ganti *user input placeholders* dengan informasi Anda sendiri.

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

Untuk informasi selengkapnya, lihat [DescribeConnector](#) di referensi API.

Penskalaan dan kuota untuk konektor SFTP

Topik

- [Kuota untuk konektor SFTP](#)
- [Menskalakan konektor SFTP Anda](#)

Kuota untuk konektor SFTP

Kuota berikut tersedia untuk konektor SFTP.

Note

Lebih banyak kuota layanan untuk konektor SFTP tercantum dalam [AWS Transfer Family titik akhir dan](#) kuota di. Referensi Umum Amazon Web

Kuota konektor SFTP

Nama	Default	Dapat disesuaikan
Transaksi koneksi uji maksimum per detik (TPS)	1 permintaan per detik, per akun	Tidak
Ukuran antrian maksimum untuk transfer file yang tertunda	1000	Tidak
Ukuran maksimum file	150 gibibyte (GiB)	Tidak
Waktu transfer maksimum per file	12 jam	Tidak
Waktu tunggu permintaan maksimum per file	12 jam	Tidak
Bandwidth maksimum untuk konektor per akun (konektor	50 MBps	Tidak

Nama	Default	Dapat disesuaikan
SFTP dan AS2 berkontribusi pada nilai ini)		
Jumlah maksimum item untuk operasi daftar direktori	200.000	Tidak

Note

Secara default, konektor SFTP memproses satu file pada satu waktu, mentransfer file secara berurutan. Anda memiliki opsi untuk mempercepat kinerja transfer dengan meminta konektor Anda membuat sesi bersamaan dengan server jarak jauh yang mendukung sesi bersamaan dari pengguna yang sama, dan memproses hingga 5 file secara paralel.

Untuk mengaktifkan koneksi bersamaan untuk konektor apa pun, Anda dapat mengedit pengaturan Koneksi konkuren maksimum saat membuat atau memperbarui konektor. Lihat perinciannya di [Buat konektor SFTP dengan jalan keluar yang dikelola layanan](#).

Untuk menyimpan kredensial untuk konektor SFTP, ada kuota yang terkait dengan setiap rahasia Secrets Manager. Jika Anda menggunakan rahasia yang sama untuk menyimpan beberapa jenis kunci, untuk berbagai tujuan, Anda mungkin menemukan kuota ini.

- Total panjang untuk satu rahasia: 12.000 karakter
- Panjang maksimum **Password** string: 1024 karakter
- Panjang maksimum **PrivateKey** string: 8192 karakter
- Panjang maksimum **Username** string: 100 karakter

Menskalakan konektor SFTP Anda

Bagian ini menjelaskan pertimbangan tentang cara menskalakan beban kerja konektor AWS Transfer Family SFTP Anda. Anda perlu memperhitungkan tiga kuota berikut yang berlaku saat Anda ingin menskalakan beban kerja Anda dengan konektor SFTP.

- Ukuran antrian maksimum. Ini mengacu pada jumlah maksimum operasi yang tertunda dalam antrian konektor yang telah diminta. Operasi yang tertunda mengacu pada permintaan transfer yang diajukan sebelumnya yang belum selesai, baik berhasil atau tidak berhasil.

Kedalaman antrian maksimum untuk permintaan tertunda saat ini ditetapkan pada 1.000 per konektor (seperti yang didefinisikan dalam [kuota AWS Transfer Family layanan](#)). Beban kerja Anda mungkin melebihi batas layanan ini ketika Anda meminta ribuan operasi transfer dalam durasi singkat, dan Anda akan menerima pesan `ThrottlingException` dengan pesan `Melebihi permintaan tertunda maksimum`. Jika beban kerja Anda tunduk pada kuota ini, hubungi tim layanan Transfer Family melalui AWS Dukungan atau tim akun Anda untuk mendiskusikan persyaratan skalabilitas Anda.

Anda juga dapat mengambil salah satu atau kedua tindakan berikut.

- Mendistribusikan volume file Anda di beberapa konektor.
- Mintalah konektor Anda membuat sesi bersamaan dengan server jarak jauh untuk memproses beberapa permintaan dari antrian secara paralel.
- Jumlah sesi bersamaan. Secara default, konektor SFTP mentransfer satu file pada satu waktu, mentransfer file secara berurutan dari antreannya.

Anda memiliki opsi untuk mempercepat kinerja transfer dengan meminta konektor Anda mentransfer banyak file secara paralel. Anda dapat membuat sesi bersamaan dengan server jarak jauh yang mendukung sesi bersamaan dari pengguna yang sama, dan memproses hingga 5 file secara paralel. Saat Anda membuat konektor SFTP, pilih nilai hingga 5 untuk pengaturan Koneksi bersamaan maksimum saat Anda membuat atau memperbarui konektor. Lihat perinciannya di [Buat konektor SFTP dengan jalan keluar yang dikelola layanan](#).

- Tingkat **StartFileTransfer** permintaan. Anda dapat meminta hingga 100 jalur file per detik untuk transfer dengan setiap konektor SFTP. Jalur file yang diminta ditambahkan ke antrian konektor Anda untuk diproses. Anda dapat menggunakan `StartFileTransfer` perintah secara rekursif untuk meminta hingga 100 jalur file per detik per konektor, terlepas dari jumlah file yang disediakan dalam perintah `individualStartFileTransfer`.

Arsitektur referensi menggunakan konektor SFTP

Bagian ini mencantumkan bahan referensi yang tersedia untuk mengonfigurasi alur kerja transfer file otomatis menggunakan konektor SFTP. Anda dapat mendesain arsitektur berbasis peristiwa Anda

sendiri dengan menggunakan peristiwa konektor SFTP di Amazon EventBridge, untuk mengatur antara tindakan transfer file Anda dan tindakan sebelum dan sesudah pemrosesan di AWS

Unggahan blog

Posting blog berikut menyediakan arsitektur referensi untuk membangun alur kerja MFT menggunakan konektor SFTP, termasuk enkripsi file menggunakan PGP sebelum mengirimnya ke server SFTP jarak jauh menggunakan konektor SFTP: [Merancang transfer file terkelola yang aman dan sesuai dengan konektor SFTP dan](#) enkripsi PGP. AWS Transfer Family

Lokakarya

- Lokakarya berikut menyediakan lab langsung untuk mengonfigurasi konektor SFTP dan menggunakan konektor Anda untuk mengirim atau mengambil file dari server SFTP jarak jauh: Transfer [Family](#) - bengkel SFTP.
- [Lokakarya berikut menyediakan laboratorium langsung untuk membangun alur kerja yang sepenuhnya otomatis dan digerakkan oleh peristiwa yang melibatkan transfer file ke atau dari server SFTP eksternal ke Amazon S3, dan pra dan pasca pemrosesan umum dari file-file tersebut: lokakarya MFT. Event-driven](#)

Video ini memberikan jalan-jalan melalui lokakarya ini.

Solusi

AWS Transfer Family memberikan solusi berikut:

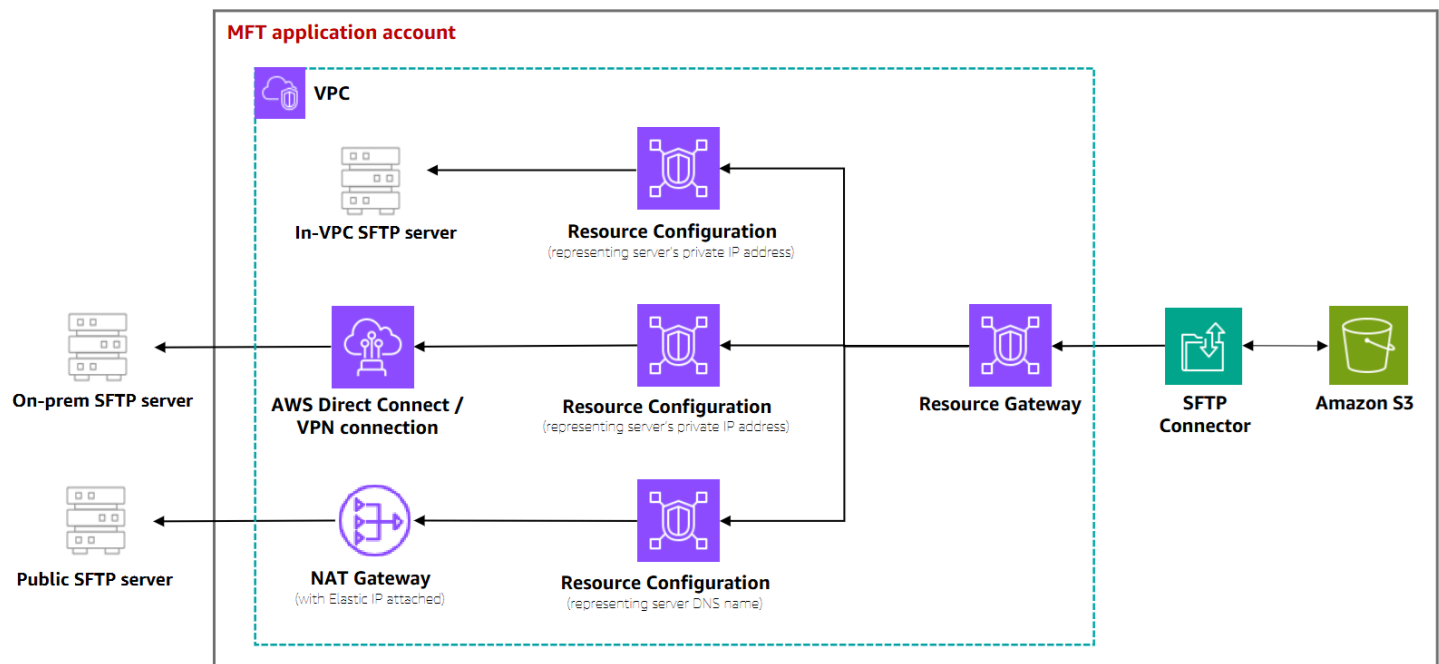
- [Solusi sinkronisasi transfer file](#) menyediakan arsitektur referensi untuk mengotomatiskan proses sinkronisasi direktori SFTP jarak jauh—termasuk seluruh struktur folder—dengan bucket Amazon S3 lokal Anda menggunakan konektor SFTP. Ini mengatur proses daftar direktori jarak jauh, mendeteksi perubahan, dan mentransfer file baru atau yang dimodifikasi.
- [Serverlessland - Transfer file selektif antara server SFTP jarak jauh & S3; menggunakan AWS Transfer Family](#) menyediakan pola sampel untuk mencantumkan file yang disimpan di lokasi SFTP jarak jauh, dan mentransfer file selektif ke Amazon S3.

Arsitektur referensi VPC

Arsitektur referensi berikut menunjukkan pola umum untuk menerapkan konektor LATTICE-enabled VPC_SFTP. Contoh-contoh ini membantu Anda memahami di mana sumber daya VPC Lattice perlu dibuat dalam keseluruhan arsitektur Anda. AWS

Akun tunggal dengan infrastruktur jalan keluar bersama

Dalam arsitektur ini, infrastruktur jalan keluar (NAT Gateway, VPN tunnel, atau Direct Connect) dikonfigurasi dalam VPC dalam akun yang sama dengan konektor SFTP Anda. Semua konektor dapat berbagi Resource Gateway dan NAT Gateway yang sama.

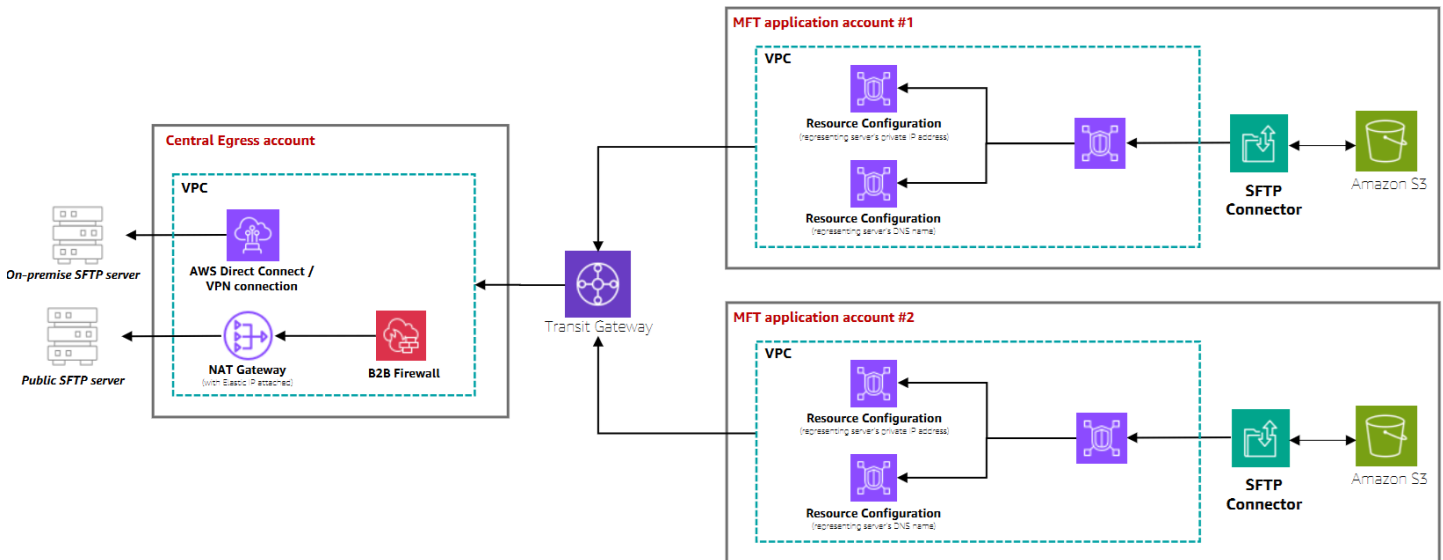


Pola ini sangat ideal ketika:

- Semua konektor SFTP dikelola dalam satu Akun AWS
- Infrastruktur jalan keluar diatur dalam VPC dalam akun yang sama dengan konektor SFTP Anda

Cross-account dengan infrastruktur jalan keluar terpusat

Dalam arsitektur ini, infrastruktur jalan keluar (NAT Gateway, VPN tunnel, Direct Connect, atau B2B Firewalls) dikonfigurasi dalam akun Egress pusat yang dikelola oleh tim jaringan. Konektor SFTP dibuat di akun Aplikasi MFT yang dikelola oleh tim admin MFT. Cross-account jaringan dibuat menggunakan Transit Gateway untuk menghormati aturan jaringan yang ada.



Pola ini sangat ideal ketika:

- Infrastruktur jaringan dikelola oleh tim terpisah di akun khusus
- Anda memiliki rute yang ada (seperti AWS Transit Gateway) antara akun tempat konektor SFTP dibuat dan akun tempat infrastruktur Egress diatur. Konektor SFTP akan dapat memanfaatkan rute Anda yang ada yang menghubungkan kedua akun.
- Kontrol keamanan terpusat dan firewall B2B diperlukan
- Anda perlu mempertahankan pemisahan tugas antara jaringan dan tim aplikasi

AWS Transfer Family untuk AS2

Applicability Statement 2 (AS2) adalah spesifikasi RFC-defined transmisi file yang mencakup perlindungan pesan yang kuat dan mekanisme verifikasi. Melindungi muatan AS2 dalam perjalanan menggunakan Cryptographic Message Syntax (CMS) dengan enkripsi dan tanda tangan digital untuk memberikan perlindungan data dan otentikasi rekan. Payload respons Pemberitahuan Disposisi Pesan (MDN) yang ditandatangani memberikan verifikasi (non-penolakan) bahwa pesan diterima dan berhasil didekripsi.

Protokol AS2 sangat penting untuk alur kerja dengan persyaratan kepatuhan yang bergantung pada perlindungan data dan fitur keamanan yang dibangun ke dalam protokol. AWS Transfer Family Titik akhir AS2 [bersertifikat Drummond](#), memungkinkan pelanggan di industri seperti ritel, ilmu hayati, manufaktur, layanan keuangan, dan utilitas untuk bertransaksi dengan aman dengan mitra bisnis mereka.

Saat Anda menggunakan AS2 dengan Transfer Family, data yang ditransaksikan dapat diakses secara native untuk: AWS

- Pemrosesan, analisis, dan pembelajaran mesin
- Integrasi dengan sistem perencanaan sumber daya perusahaan (ERP)
- Integrasi dengan sistem manajemen hubungan pelanggan (CRM)

Untuk bertukar file dengan mitra yang memiliki AS2-enabled server, Anda harus:

- Menghasilkan key pair public-private untuk enkripsi
- Menghasilkan key pair public-private untuk penandatanganan
- Tukarkan kunci publik dengan pasangan Anda

Important

Titik akhir server HTTPS AS2 saat ini tidak didukung. Anda bertanggung jawab atas penghentian TLS.

Transfer Family menyediakan lokakarya yang dapat Anda hadiri, di mana Anda dapat mengonfigurasi titik akhir Transfer Family dengan AS2 diaktifkan, dan konektor Transfer Family AS2. Anda dapat melihat detail untuk lokakarya ini [di sini](#).

Untuk petunjuk langkah demi langkah untuk mengkonfigurasi AS2 di Transfer Family, lihat berikut ini:

1. [Impor sertifikat AS2](#)
2. [Buat profil AS2](#)
3. [Buat server AS2](#)
4. [Buat perjanjian AS2](#)
5. [Konfigurasi konektor AS2](#)

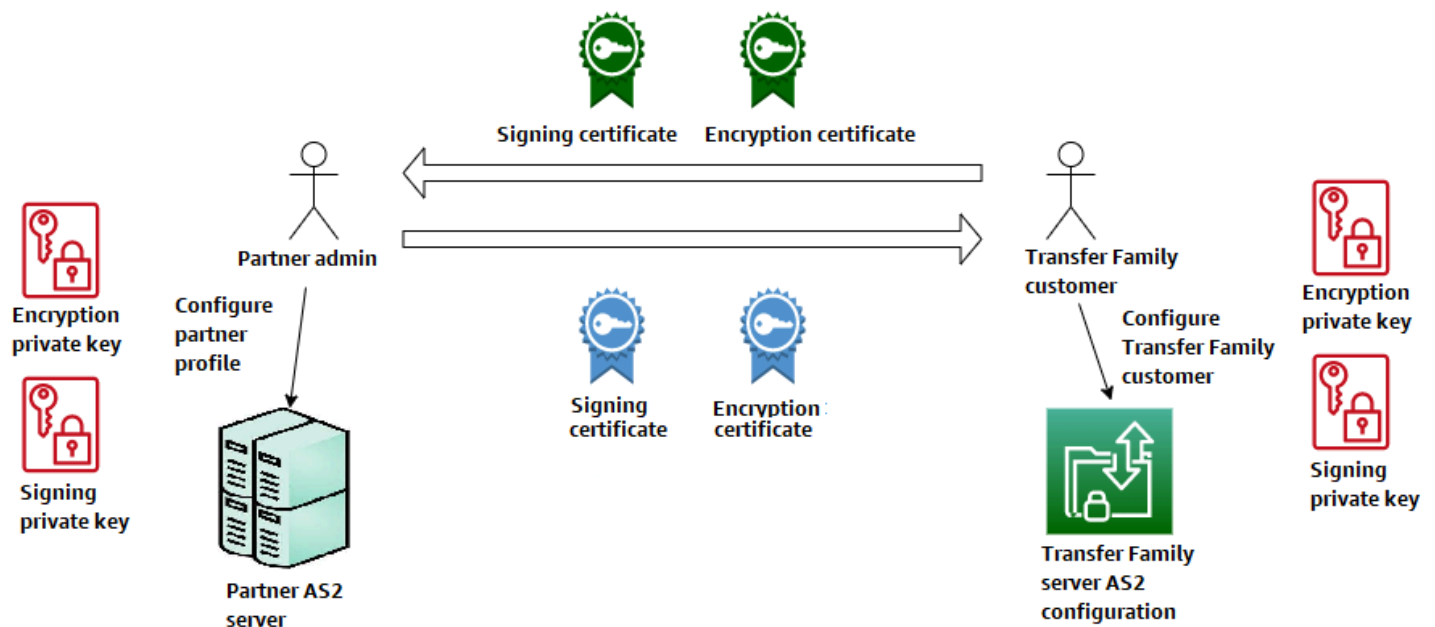
Untuk contoh lengkapnya, lihat [Menyiapkan konfigurasi AS2](#).

 Note

Untuk menunjukkan dukungan untuk template AS2 Terraform, tambahkan reaksi jempol (#) ke permintaan fitur template [Transfer Family Terraform](#). Anda juga dapat menambahkan komentar yang menjelaskan kasus penggunaan Anda.

Kasus penggunaan AS2

Jika Anda adalah AWS Transfer Family pelanggan yang ingin bertukar file dengan mitra yang memiliki AS2-enabled server, bagian paling kompleks dari pengaturan melibatkan menghasilkan satu public-private key pair untuk enkripsi dan satu lagi untuk menandatangani dan bertukar kunci publik dengan mitra.



Pertimbangkan variasi berikut untuk digunakan AWS Transfer Family dengan AS2.

Note

Mitra dagang adalah mitra yang terkait dengan profil mitra tersebut.
Semua penyebutan MDN dalam tabel berikut mengasumsikan mDNS ditandatangani.

Kasus penggunaan AS2

Inbound-only kasus penggunaan

- Transfer pesan AS2 terenkripsi dari mitra dagang ke server Transfer Family.

Dalam kasus ini, lakukan hal berikut:

1. Buat profil untuk mitra dagang Anda dan diri Anda sendiri.
2. Buat server Transfer Family yang menggunakan protokol AS2.
3. Buat perjanjian dan tambahkan ke server Anda.
4. Impor sertifikat dengan kunci pribadi dan tambahkan ke profil Anda, lalu impor kunci publik ke profil mitra Anda untuk enkripsi.
5. Setelah Anda memiliki barang-barang ini, kirimkan kunci publik untuk sertifikat Anda ke mitra dagang Anda.

Sekarang pasangan Anda dapat mengirimi Anda pesan terenkripsi dan Anda dapat mendekripsi dan menyimpannya di ember Amazon S3 Anda.

- Transfer pesan AS2 terenkripsi dari mitra dagang ke server Transfer Family dan tambahkan penandatanganan.

Dalam skenario ini, Anda masih hanya melakukan transfer masuk, tetapi sekarang Anda ingin pasangan Anda menandatangani pesan yang mereka kirim. Dalam hal ini, impor kunci publik penandatanganan mitra dagang (sebagai sertifikat penandatanganan yang ditambahkan ke profil mitra Anda).

- Transfer pesan AS2 terenkripsi dari mitra dagang ke server Transfer Family dan tambahkan penandatanganan dan pengiriman respons MDN.

Dalam skenario ini, Anda masih hanya melakukan transfer masuk, tetapi sekarang, selain menerima muatan yang ditandatangani, mitra dagang Anda ingin menerima tanggapan MDN yang ditandatangani.

1. Impor kunci penandatanganan publik dan pribadi Anda (sebagai sertifikat penandatanganan ke profil Anda).
2. Kirim kunci penandatanganan publik ke mitra dagang Anda.

Outbound-only kasus penggunaan

- Transfer pesan AS2 terenkripsi dari server Transfer Family ke mitra dagang.

Kasus ini mirip dengan kasus penggunaan transfer inbound-only, kecuali bahwa alih-alih menambahkan perjanjian ke server AS2 Anda, Anda membuat konektor. Dalam hal ini, Anda mengimpor kunci publik mitra dagang Anda ke profil mereka.

- Transfer pesan AS2 terenkripsi dari server Transfer Family ke mitra dagang dan tambahkan penandatanganan.

Anda masih hanya melakukan transfer keluar, tetapi sekarang mitra dagang Anda ingin Anda menandatangani pesan yang Anda kirim kepada mereka.

1. Impor kunci pribadi penandatanganan Anda (sebagai sertifikat penandatanganan yang ditambahkan ke profil Anda).
 2. Kirimkan kunci publik kepada mitra dagang Anda.
- Transfer pesan AS2 terenkripsi dari server Transfer Family ke mitra dagang dan tambahkan penandatanganan dan kirim tanggapan MDN.

Anda masih hanya melakukan transfer keluar, tetapi sekarang, selain mengirim muatan yang ditandatangani, Anda ingin menerima tanggapan MDN yang ditandatangani dari mitra dagang Anda.

1. Mitra dagang Anda mengirimkan Anda kunci penandatanganan publik mereka.
2. Impor kunci publik mitra dagang Anda (sebagai sertifikat penandatanganan yang ditambahkan ke profil mitra Anda).

Kasus penggunaan masuk dan keluar

- Transfer pesan AS2 terenkripsi di kedua arah antara server Transfer Family dan mitra dagang.

Dalam kasus ini, lakukan hal berikut:

1. Buat profil untuk mitra dagang Anda dan diri Anda sendiri.
2. Buat server Transfer Family yang menggunakan protokol AS2.
3. Buat perjanjian dan tambahkan ke server Anda.
4. Buat konektor.
5. Impor sertifikat dengan kunci pribadi dan tambahkan ke profil Anda, lalu impor kunci publik ke profil mitra Anda untuk enkripsi.
6. Terima kunci publik dari mitra dagang Anda dan tambahkan ke profil mereka untuk enkripsi.
7. Setelah Anda memiliki barang-barang ini, kirimkan kunci publik untuk sertifikat Anda ke mitra dagang Anda.

Sekarang Anda dan mitra dagang Anda dapat bertukar pesan terenkripsi, dan Anda berdua dapat mendekripsi mereka. Anda dapat menyimpan pesan yang Anda terima di bucket Amazon S3 Anda, dan pasangan Anda dapat mendekripsi dan menyimpan pesan yang Anda kirim kepada mereka.

- Transfer pesan AS2 terenkripsi di kedua arah antara server Transfer Family dan mitra dagang dan tambahkan penandatanganan.

Sekarang Anda dan pasangan Anda ingin pesan yang ditandatangani.

1. Impor kunci pribadi penandatanganan Anda (sebagai sertifikat penandatanganan yang ditambahkan ke profil Anda).
 2. Kirimkan kunci publik kepada mitra dagang Anda.
 3. Impor kunci publik penandatanganan mitra dagang Anda dan tambahkan ke profil mereka.
- Transfer pesan AS2 terenkripsi di kedua arah antara server Transfer Family dan mitra dagang dan tambahkan penandatanganan dan kirim respons MDN.

Sekarang, Anda ingin menukar muatan yang ditandatangani, dan Anda dan mitra dagang Anda menginginkan tanggapan MDN.

1. Mitra dagang Anda mengirimi Anda kunci penandatanganan publik mereka.
2. Impor kunci publik mitra dagang Anda (sebagai sertifikat penandatanganan ke profil mitra Anda).

3. Kirim kunci publik Anda ke mitra dagang Anda.

Template AS2 CloudFormation

Topik ini memberikan informasi tentang AWS CloudFormation template yang dapat Anda gunakan untuk menyebarkan server dan konfigurasi AS2 dengan cepat. AWS Transfer Family Template ini mengotomatiskan proses penyiapan dan membantu Anda menerapkan praktik terbaik untuk transfer file AS2.

- Template AS2 dasar dijelaskan dalam [Gunakan template untuk membuat demo Transfer Family AS2 stack](#)
- Template AS2 untuk menyesuaikan header HTTP dijelaskan dalam. [Sesuaikan header HTTP untuk pesan AS2](#)

Menyesuaikan Templat AS2

Anda dapat menyesuaikan templat yang disediakan untuk memenuhi persyaratan spesifik Anda:

1. Unduh template dari URL S3.
2. Ubah kode YAMAL untuk menyesuaikan konfigurasi seperti:
 - Pengaturan keamanan dan konfigurasi sertifikat
 - Arsitektur jaringan dan pengaturan VPC
 - Opsi penyimpanan dan penanganan file
 - Preferensi pemantauan dan pemberitahuan
3. Unggah template Anda yang dimodifikasi ke bucket S3 Anda sendiri.
4. Terapkan templat yang disesuaikan menggunakan CloudFormation konsol atau AWS CLI.

Important

Saat menyesuaikan template, pastikan Anda mempertahankan dependensi antar sumber daya dan mengikuti praktik terbaik keamanan.

Menguji penerapan AS2 Anda

Setelah menerapkan server AS2 menggunakan template, Anda dapat menguji konfigurasi:

1. Periksa output CloudFormation tumpukan untuk perintah sampel dan informasi titik akhir.
2. Gunakan AWS CLI untuk mengirim file pengujian:

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt
aws transfer start-file-transfer --connector-id your-connector-id --send-file-
paths /your-bucket-name/test.txt
```

3. Verifikasi pengiriman file di bucket S3 tujuan.
4. Periksa CloudWatch log untuk pemrosesan yang berhasil dan tanggapan MDN.

Untuk pengujian yang lebih komprehensif, pertimbangkan untuk menggunakan klien AS2 pihak ketiga untuk mengirim file ke server Transfer Family AS2 Anda.

Praktik terbaik untuk penerapan template AS2

Ikuti praktik terbaik ini saat menggunakan CloudFormation templat AS2:

Keamanan

Gunakan sertifikat yang kuat dan putar secara teratur.

Menerapkan kebijakan IAM dengan hak istimewa paling sedikit.

Batasi akses jaringan menggunakan grup keamanan.

Keandalan

Terapkan di beberapa Availability Zone.

Menerapkan pemantauan dan peringatan untuk transfer yang gagal.

Siapkan percobaan ulang otomatis untuk transfer yang gagal.

Performa

Pilih jenis instans yang sesuai untuk volume transfer Anda.

Menerapkan kebijakan siklus hidup S3 untuk manajemen file yang efisien.

Memantau dan mengoptimalkan konfigurasi jaringan.

Pengoptimalan Biaya

Gunakan auto-scaling untuk beban kerja variabel.

Menerapkan kelas penyimpanan S3 untuk file yang lebih lama.

Pantau dan sesuaikan sumber daya berdasarkan penggunaan aktual.

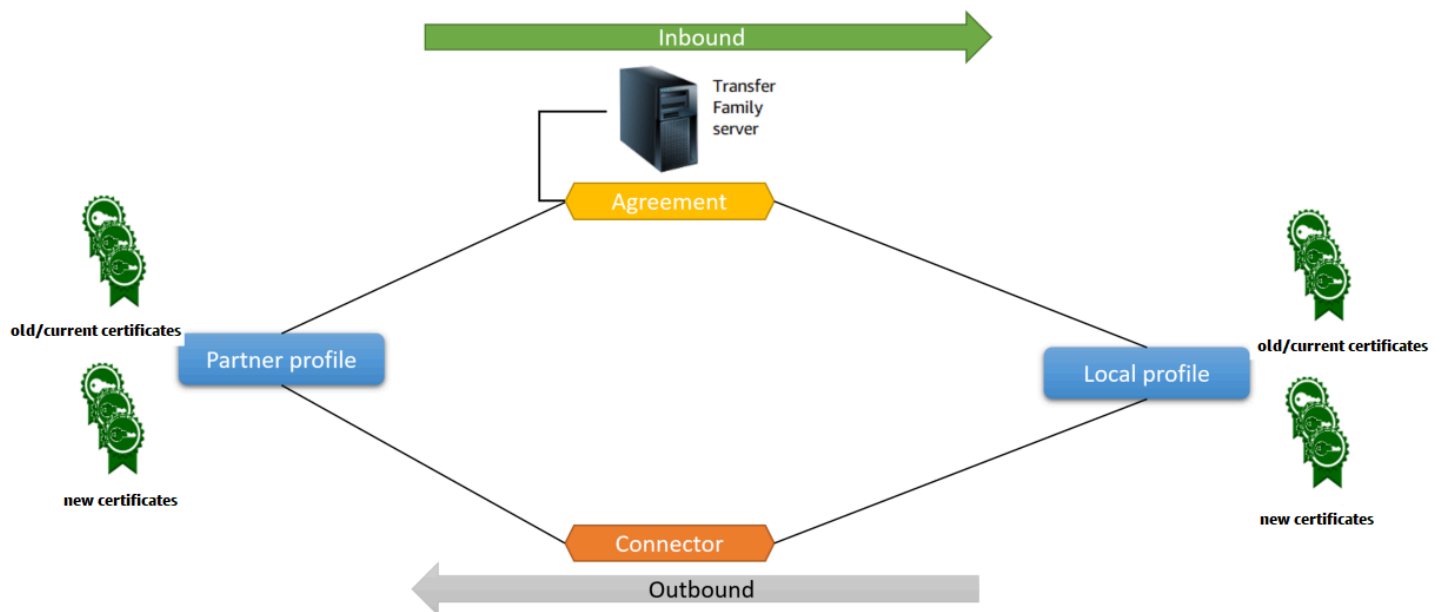
Mengkonfigurasi AS2

Untuk membuat AS2-enabled server, Anda juga harus menentukan komponen berikut:

- **Perjanjian** — Perjanjian mitra dagang bilateral, atau kemitraan, menentukan hubungan antara kedua pihak yang bertukar pesan (file). Untuk menentukan perjanjian, Transfer Family menggabungkan server, profil lokal, profil mitra, dan informasi sertifikat. AS2-inbound Proses Transfer Family menggunakan perjanjian.
- **Sertifikat** — Sertifikat kunci publik (X.509) digunakan dalam komunikasi AS2 untuk enkripsi dan verifikasi pesan. Sertifikat juga digunakan untuk titik akhir konektor.
- **Profil lokal dan profil mitra** — Profil lokal mendefinisikan organisasi lokal (AS2-enabled Transfer Family server) atau “pesta”. Demikian pula, profil mitra mendefinisikan organisasi mitra jarak jauh, eksternal untuk Transfer Family.

Meskipun tidak diperlukan untuk semua AS2-enabled server, untuk transfer keluar, Anda memerlukan konektor. Konektor menangkap parameter untuk koneksi keluar. Konektor diperlukan untuk mengirim file ke eksternal pelanggan, non AWS server.

Diagram berikut menunjukkan hubungan antara objek AS2 yang terlibat dalam proses masuk dan keluar.



Untuk contoh konfigurasi AS2 end-to-end, lihat. [Menyiapkan konfigurasi AS2](#)

Topik

- [Konfigurasi AS2](#)
- [Kuota dan batasan AS2](#)
- [Fitur dan kemampuan AS2](#)

Konfigurasi AS2

Topik ini menjelaskan konfigurasi, fitur, dan kemampuan yang didukung untuk transfer yang menggunakan protokol Applicability Statement 2 (AS2), termasuk cipher dan digest yang diterima.

Penandatanganan, enkripsi, kompresi, MDN

Untuk transfer masuk dan keluar, item berikut wajib atau opsional:

- Enkripsi — Diperlukan (untuk transportasi HTTP, yang merupakan satu-satunya metode transport yang saat ini didukung). Pesan yang tidak terenkripsi hanya diterima jika diteruskan oleh TLS-terminating proxy seperti Application Load Balancer (ALB) dan header ada. X-Forwarded-Proto: https
- Penandatanganan - Opsional
- Kompresi - Opsional (satu-satunya algoritma kompresi yang didukung saat ini adalah ZLIB)

- Pemberitahuan Disposisi Pesan (MDN) — Opsional

Cipher

Cipher berikut didukung untuk transfer masuk dan keluar:

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES (hanya untuk kompatibilitas mundur)

Intisari

Intisari berikut didukung:

- Penandatanganan masuk dan MDN - SHA1, SHA256, SHA384, SHA512
- Penandatanganan keluar dan MDN - SHA1, SHA256, SHA384, SHA512

MDN

Untuk tanggapan MDN, jenis tertentu didukung, sebagai berikut:

- Transfer masuk — Sinkron dan asinkron
- Transfer keluar — Sinkron dan asinkron
- Protokol Transfer Surat Sederhana (SMTP) (email MDN) - Tidak didukung

Transportasi

- Transfer masuk - HTTP adalah satu-satunya transportasi yang didukung saat ini, dan Anda harus menentukannya secara eksplisit.

Note

Jika Anda perlu menggunakan HTTPS untuk transfer masuk, Anda dapat menghentikan TLS pada Application Load Balancer atau Network Load Balancer. Ini dijelaskan dalam [Terima pesan AS2 melalui HTTPS](#).

- Transfer keluar — Jika Anda memberikan URL HTTP, Anda juga harus menentukan algoritma enkripsi. Jika Anda memberikan URL HTTPS, Anda memiliki opsi untuk menentukan NONE untuk algoritma enkripsi Anda.

Kuota dan batasan AS2

Bagian ini membahas kuota dan batasan untuk AS2

Topik

- [Kuota AS2](#)
- [Kuota untuk menangani rahasia](#)
- [Keterbatasan yang Sudah Diketahui](#)

Kuota AS2

Kuota berikut tersedia untuk transfer file AS2. Untuk meminta kenaikan kuota yang dapat disesuaikan, lihat [Layanan AWS kuota](#) di. Referensi Umum AWS

Kuota AS2

Nama	Default	Dapat disesuaikan
Jumlah maksimum file per permintaan keluar	10	Tidak
Jumlah maksimum permintaan keluar per detik	100	Tidak
Jumlah maksimum permintaan masuk per detik	100	Tidak
Bandwidth keluar maksimum per akun (permintaan SFTP keluar dan AS2 keduanya berkontribusi pada nilai ini)	50 MB per detik	Tidak

Kuota untuk menangani rahasia

AWS Transfer Family melakukan panggilan ke AWS Secrets Manager atas nama pelanggan AS2 yang menggunakan otentikasi Dasar. Selain itu Secrets Manager membuat panggilan ke AWS KMS.

Note

Kuota ini tidak spesifik untuk penggunaan rahasia Anda untuk Transfer Family: kuota ini dibagikan di antara semua layanan di Akun AWS.

Untuk Secrets Manager `GetSecretValue`, kuota yang berlaku adalah Combined rate of `DescribeSecret` dan permintaan `GetSecretValue` API, seperti yang dijelaskan dalam [AWS Secrets Manager kuota](#).

Secrets Manager **GetSecretValue**

Nama	Nilai	Deskripsi
Tingkat gabungan permintaan <code>DescribeSecret</code> dan <code>GetSecretValue</code> API	Setiap Wilayah yang didukung: 10.000 per detik	Transaksi maksimum per detik untuk <code>DescribeSecret</code> dan operasi <code>GetSecretValue</code> API digabungkan.

Untuk AWS KMS, kuota berikut berlaku untuk `Decrypt`. Untuk detailnya, lihat [Meminta kuota untuk setiap operasi AWS KMS API](#)

AWS KMS **Decrypt**

Nama kuota	Nilai default (permintaan per detik)
Tingkat permintaan operasi kriptografi (simetris)	Kuota bersama ini bervariasi dengan Wilayah AWS dan jenis AWS KMS kunci yang digunakan dalam permintaan. Setiap kuota dihitung secara terpisah. • 5.500 (bersama) • 10.000 (bersama) di Wilayah berikut:

Nama kuota	Nilai default (permintaan per detik)
	• US East (Ohio) us-east-2 • Asia Pacific (Singapore) ap-southeast-1 • Asia Pacific (Sydney), ap-southeast-2 • Asia Pacific (Tokyo), ap-northeast-1 • Europe (Frankfurt), eu-central-1 • Europe (London), eu-west-2 • 50.000 (bersama) di Wilayah berikut: • US East (N. Virginia), us-east-1 • US West (Oregon), us-west-2 • Europe (Ireland), eu-west-1
Kuota permintaan toko kunci kustom  Note Kuota ini hanya berlaku jika Anda menggunakan toko kunci eksternal.	Kuota permintaan toko kunci khusus dihitung secara terpisah untuk setiap toko kunci khusus. • 1.800 (dibagikan) untuk setiap toko AWS CloudHSM kunci • 1.800 (dibagikan) untuk setiap toko kunci eksternal

Keterbatasan yang Sudah Diketahui

- Server-side TCP keep-alive tidak didukung. Waktu koneksi habis setelah 350 detik tidak aktif kecuali klien mengirim paket keep-alive.
- Agar perjanjian aktif diterima oleh layanan dan muncul di CloudWatch log Amazon, pesan harus berisi header AS2 yang valid.
- [Server yang menerima pesan dari AWS Transfer Family AS2 harus mendukung atribut perlindungan algoritma Cryptographic Message Syntax \(CMS\) untuk memvalidasi tanda tangan pesan, seperti yang didefinisikan dalam RFC 6211.](#) Atribut ini tidak didukung di beberapa produk IBM Sterling yang lebih lama.
- ID pesan duplikat menghasilkan processed/Warning: pesan dokumen duplikat.
- Panjang kunci untuk sertifikat AS2 harus minimal 2048 bit, dan paling banyak 4096.

- Saat mengirim pesan AS2 atau mDNS asinkron ke titik akhir HTTPS mitra dagang, pesan atau mDNS harus menggunakan sertifikat SSL yang valid yang ditandatangani oleh otoritas sertifikat tepercaya publik (CA). Self-signed sertifikat saat ini hanya didukung untuk transfer keluar.
- Titik akhir harus mendukung protokol TLS versi 1.2 dan algoritma kriptografi yang diizinkan oleh kebijakan keamanan (seperti yang dijelaskan dalam). [Kebijakan keamanan untuk AWS Transfer Family server](#)
- Beberapa lampiran dan pesan pertukaran sertifikat (CEM) dari AS2 versi 1.2 saat ini tidak didukung.
- Otentikasi dasar saat ini hanya didukung untuk pesan keluar.
- Anda dapat melampirkan alur kerja pemrosesan file ke server Transfer Family yang menggunakan protokol AS2: namun, pesan AS2 tidak menjalankan alur kerja yang dilampirkan ke server.

Fitur dan kemampuan AS2

Tabel berikut mencantumkan fitur dan kemampuan yang tersedia untuk sumber daya Transfer Family yang menggunakan AS2.

Fitur AS2

Transfer Family menawarkan fitur-fitur berikut untuk AS2.

Fitur	Didukung oleh AWS Transfer Family
Sertifikasi Drummond	Ya
AWS CloudFormation dukungan	Ya
CloudWatchMetrik Amazon	Ya
SHA-2 algoritma kriptografi	Ya
Support untuk Amazon S3	Ya
Dukungan untuk Amazon EFS	Tidak
Pesan Terjadwal	Ya ¹
AWS Transfer Family Alur Kerja Terkelola	Tidak

Fitur	Didukung oleh AWS Transfer Family
Pesan Pertukaran Sertifikat (CEM)	Tidak
TLS Bersama (mTLS)	Tidak
Support untuk sertifikat yang ditandatangani sendiri	Ya

1. Pesan Terjadwal Keluar tersedia dengan [menjadwalkan AWS Lambda fungsi menggunakan Amazon EventBridge](#)

AS2 mengirim dan menerima kemampuan

Tabel berikut menyediakan daftar kemampuan mengirim dan menerima AWS Transfer Family AS2.

Kemampuan	Inbound: Menerima dengan server	Keluar: Mengirim dengan konektor
Transportasi Terenkripsi TLS (HTTPS)	Ya ¹	Ya
Non-TLS Transportasi (HTTP)	Ya	Ya ²
MDN sinkron	Ya	Ya
Kompresi Pesan	Ya	Ya
MDN asinkron	Ya	Ya
Alamat IP Statis	Ya	Ya
Bawa Alamat IP Anda Sendiri	Ya	Tidak
Beberapa Lampiran File	Tidak	Tidak
Otentikasi Dasar	Tidak	Ya
AS2 Mulai Ulang	Tidak berlaku	Tidak

Kemampuan	Inbound: Menerima dengan server	Keluar: Mengirim dengan konektor
Keandalan AS2	Tidak	Tidak
Subjek Kustom per Pesan	Tidak berlaku	Tidak

1. Transportasi Terenkripsi TLS Masuk tersedia dengan Network Load Balancer (NLB) atau Application Load Balancer (ALB)
2. Transportasi Non-TLS Outbound hanya tersedia saat enkripsi diaktifkan

Kelola sertifikat AS2

Topik ini membahas cara mengimpor dan mengelola sertifikat AS2. Mengimpor sertifikat adalah langkah pertama dalam proses AS2 untuk Transfer Family.

1. Impor sertifikat
2. [Buat profil AS2](#)
3. [Buat server AS2](#)
4. [Buat perjanjian AS2](#)
5. [Konfigurasi konektor AS2](#)

Impor sertifikat AS2

Proses Transfer Family AS2 menggunakan kunci sertifikat untuk enkripsi dan penandatanganan informasi yang ditransfer. Mitra dapat menggunakan kunci yang sama untuk kedua tujuan, atau kunci terpisah untuk masing-masing. Jika Anda memiliki kunci enkripsi umum yang disimpan di escrow oleh pihak ketiga tepercaya sehingga data dapat didekripsi jika terjadi bencana atau pelanggaran keamanan, sebaiknya Anda memiliki kunci penandatanganan terpisah. Dengan menggunakan kunci penandatanganan terpisah (yang tidak Anda escrow), Anda tidak mengkompromikan fitur non-penolakan tanda tangan digital Anda.

Note

Panjang kunci untuk sertifikat AS2 harus minimal 2048 bit, dan paling banyak 4096.

Poin-poin berikut merinci bagaimana sertifikat AS2 digunakan selama proses berlangsung.

- AS2 masuk
 - Mitra dagang mengirimkan kunci publik mereka untuk sertifikat penandatanganan, dan kunci ini diimpor ke profil mitra.
 - Pihak lokal mengirimkan kunci publik untuk enkripsi dan sertifikat penandatanganan mereka. Mitra kemudian mengimpor kunci pribadi atau kunci. Pihak lokal dapat mengirim kunci sertifikat terpisah untuk penandatanganan dan enkripsi, atau dapat memilih untuk menggunakan kunci yang sama untuk kedua tujuan tersebut.
- AS2 Keluar
 - Mitra mengirimkan kunci publik untuk sertifikat enkripsi mereka, dan kunci ini diimpor ke profil mitra.
 - Pihak lokal mengirimkan kunci publik untuk sertifikat untuk ditandatangani, dan mengimpor kunci pribadi sertifikat untuk ditandatangani.
 - Jika Anda menggunakan HTTPS, Anda dapat mengimpor sertifikat Transport Layer Security (TLS) yang ditandatangani sendiri.

Untuk detail tentang cara membuat sertifikat, lihat [the section called “Langkah 1: Buat sertifikat untuk AS2”](#).

Prosedur ini menjelaskan cara mengimpor sertifikat dengan menggunakan konsol Transfer Family. Jika Anda ingin menggunakan AWS CLI sebagai gantinya, lihat [the section called “Langkah 2: Impor sertifikat sebagai sumber sertifikat Transfer Family”](#).

Untuk menentukan AS2-enabled sertifikat

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, di bawah Mitra Dagang AS2, pilih Sertifikat.
3. Pilih Impor sertifikat.
4. Di bagian konfigurasi Sertifikat, untuk deskripsi Sertifikat, masukkan nama yang mudah diidentifikasi untuk sertifikat. Pastikan Anda dapat mengidentifikasi tujuan sertifikat dengan deskripsinya. Selain itu, pilih peran untuk sertifikat.
5. Di bagian Penggunaan sertifikat, pilih tujuan untuk sertifikat ini. Ini dapat digunakan untuk enkripsi, penandatanganan, atau keduanya.

Tip: Jika Anda memilih Enkripsi dan menandatangani untuk penggunaan, Transfer Family akan membuat dua sertifikat identik (masing-masing memiliki ID sendiri): satu dengan nilai penggunaan ENCRYPTION dan satu dengan nilai penggunaan SIGNING.

6. Di bagian Konten Sertifikat, berikan sertifikat publik dari mitra dagang, atau kunci publik dan pribadi untuk sertifikat lokal.

Isi bagian Isi sertifikat dengan detail yang sesuai.

- Jika Anda memilih Self-signed sertifikat, Anda tidak memberikan rantai sertifikat.
 - Tempelkan teks sertifikat dan rantainya ke bidang rantai Sertifikat dan Sertifikat.
 - Jika sertifikat ini adalah sertifikat lokal, tempel di kunci pribadinya.
7. Pilih Impor sertifikat untuk menyelesaikan proses dan menyimpan rincian untuk sertifikat yang diimpor.

Note

Sertifikat TLS hanya dapat diimpor sebagai sertifikat publik mitra. Jika Anda memilih sertifikat Publik dari mitra, lalu pilih Transport Layer Security (TLS) untuk penggunaan, Anda akan menerima peringatan. Selain itu, sertifikat TLS harus ditandatangani sendiri (yaitu, Anda harus memilih Self Signed Certificate untuk mengimpor sertifikat TLS).

Rotasi sertifikat AS2

Seringkali, sertifikat berlaku untuk jangka waktu enam bulan hingga satu tahun. Anda mungkin telah menyiapkan profil yang ingin Anda pertahankan untuk durasi yang lebih lama. Untuk memfasilitasi hal ini, Transfer Family menyediakan rotasi sertifikat. Anda dapat menentukan beberapa sertifikat untuk profil, memungkinkan Anda untuk tetap menggunakan profil selama beberapa tahun. Transfer Family menggunakan sertifikat untuk penandatanganan (opsional) dan enkripsi (wajib). Anda dapat menentukan satu sertifikat untuk kedua tujuan, jika Anda mau.

Rotasi sertifikat adalah proses penggantian sertifikat lama yang kedaluwarsa dengan sertifikat yang lebih baru. Transisi adalah transisi bertahap untuk menghindari gangguan transfer di mana mitra dalam perjanjian belum mengonfigurasi sertifikat baru untuk transfer keluar atau mungkin mengirim muatan yang ditandatangani atau dienkripsi dengan sertifikat lama selama periode ketika sertifikat

yang lebih baru mungkin juga digunakan. Periode menengah di mana sertifikat lama dan baru valid disebut sebagai masa tenggang.

X.509 sertifikat memiliki `Not Before` dan `Not After` tanggal. Namun, parameter ini mungkin tidak memberikan kontrol yang cukup untuk administrator. `Transfer Family Inactive Date` menyediakan `Active Date` dan mengatur untuk mengontrol sertifikat mana yang digunakan untuk muatan keluar dan mana yang diterima untuk muatan masuk.

Pemantauan kedaluwarsa sertifikat

Transfer Family menerbitkan CloudWatch metrik `Amazon DaysUntilExpiry` setelah mengimpor sertifikat. Metrik memancarkan jumlah hari antara tanggal saat ini dan tanggal yang ditentukan sebagai `InactiveDate` pada Sertifikat. Metrik ditemukan di bawah `Transfer AWS` namespace di dasbor CloudWatch metrik.

Metrik ini akan selalu memiliki dimensi metrik untuk `CertificateId` dan secara opsional akan menyertakan dimensi `Deskripsi` jika disediakan oleh pelanggan pada sertifikat. Untuk informasi selengkapnya tentang dimensi CloudWatch metrik, lihat [Dimensi](#) di Referensi CloudWatch API.

Note

Diperlukan waktu hingga satu hari penuh setelah mengimpor Sertifikat untuk Transfer Family untuk memancarkan metrik ini ke akun pelanggan.

Anda dapat menggunakan metrik ini untuk membuat CloudWatch alarm yang memberi tahu Anda saat sertifikat mendekati kedaluwarsa.

Pemilihan sertifikat keluar menggunakan nilai maksimum yang sebelum tanggal transfer sebagai `Inactive Date`. Proses masuk menerima sertifikat dalam kisaran `Not Before` dan `Not After` dan dalam kisaran `Active Date` dan `Inactive Date`.

Contoh rotasi sertifikat

Tabel berikut menjelaskan satu cara yang mungkin untuk mengkonfigurasi dua sertifikat untuk satu profil.

Dua sertifikat dalam rotasi

Nama	NOT BEFORE(di kendalikan oleh otoritas sertifikat)	ACTIVE DATE(diatur oleh Transfer Family)	INACTIVE DATE(diatur oleh Transfer Family)	NOT AFTER(ditetapkan oleh otoritas sertifikat)
Cert1 (sertifikat lama)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
Cert2 (sertifikat yang lebih baru)	01/11/2020	2020-06-01	2021-06-01	2025-01-01

Perhatikan hal-hal berikut:

- Saat Anda menentukan Active Date dan Inactive Date untuk sertifikat, rentang harus berada di dalam rentang antara Not Before dan Not After.
- Kami menyarankan Anda mengonfigurasi beberapa sertifikat untuk setiap profil, memastikan bahwa rentang tanggal aktif untuk semua sertifikat yang digabungkan mencakup jumlah waktu yang ingin Anda gunakan profil.
- Kami menyarankan Anda menentukan waktu tenggang antara saat sertifikat lama Anda menjadi tidak aktif dan ketika sertifikat Anda yang lebih baru menjadi aktif. Dalam contoh sebelumnya, sertifikat pertama tidak menjadi tidak aktif hingga 2020-12-31, sedangkan sertifikat kedua menjadi aktif pada 2020-06-01, memberikan masa tenggang 6 bulan. Selama periode 2020-06-01 hingga 2020-12-31, kedua sertifikat aktif.

Buat profil AS2

Topik ini membahas cara membuat profil untuk digunakan dalam proses AS2. Profil lokal mendefinisikan organisasi lokal (AS2-enabled Transfer Family server) atau “pesta”. Demikian pula, profil mitra mendefinisikan organisasi mitra jarak jauh, eksternal untuk Transfer Family.

1. [Impor sertifikat AS2](#)
2. Buat profil AS2
3. [Buat server AS2](#)
4. [Buat perjanjian AS2](#)
5. [Konfigurasi konektor AS2](#)

Gunakan prosedur ini untuk membuat profil lokal dan mitra. Prosedur ini menjelaskan cara membuat profil AS2 dengan menggunakan konsol Transfer Family. Jika Anda ingin menggunakan AWS CLI sebagai gantinya, lihat [the section called “Langkah 3: Buat profil untuk Anda dan mitra dagang Anda”](#).

Untuk membuat profil AS2

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, di bawah AS2 Trading Partners, pilih Profil, lalu pilih Buat profil.
3. Di bagian Konfigurasi profil, masukkan ID AS2 untuk profil. Nilai ini digunakan untuk header HTTP khusus protokol AS2 `as2-from` dan `as2-to` untuk mengidentifikasi kemitraan perdagangan, yang menentukan sertifikat yang akan digunakan, dan sebagainya.
4. Di bagian Jenis profil, pilih Profil lokal atau Profil mitra.
5. Di bagian Sertifikat, pilih satu atau beberapa sertifikat dari menu tarik-turun.

Tip: Jika Anda ingin mengimpor sertifikat yang tidak tercantum di menu tarik-turun, pilih Impor Sertifikat baru. Ini membuka jendela browser baru di layar Impor sertifikat. Untuk prosedur tentang mengimpor sertifikat lihat [Impor sertifikat AS2](#).

6. (Opsional) Di tag bagian, tentukan satu atau beberapa pasangan nilai kunci untuk membantu mengidentifikasi profil ini.
7. Pilih Buat profil untuk menyelesaikan proses dan menyimpan profil baru.

Buat server AS2

Topik ini memberikan instruksi untuk membuat server AS2-enabled Transfer Family, menggunakan konsol atau CloudFormation templat. Untuk contoh konfigurasi AS2 end-to-end, lihat [Menyiapkan konfigurasi AS2](#). Setelah Anda membuat server AS2, Anda dapat menambahkan perjanjian ke server.

1. [Impor sertifikat AS2](#)
2. [Buat profil AS2](#)
3. Buat server AS2
4. [Buat perjanjian AS2](#)
5. [Konfigurasi konektor AS2](#)

Topik

- [Membuat server AS2 menggunakan konsol Transfer Family](#)

- [Gunakan template untuk membuat demo Transfer Family AS2 stack](#)
- [Buat perjanjian AS2](#)

Membuat server AS2 menggunakan konsol Transfer Family

Prosedur ini menjelaskan cara membuat AS2-enabled server dengan menggunakan konsol Transfer Family. Jika Anda ingin menggunakan AWS CLI sebagai gantinya, lihat [the section called “Langkah 4: Buat server Transfer Family yang menggunakan protokol AS2”](#).

Note

Anda dapat melampirkan alur kerja pemrosesan file ke server Transfer Family yang menggunakan protokol AS2: namun, pesan AS2 tidak menjalankan alur kerja yang dilampirkan ke server.

Untuk membuat AS2-enabled server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server, lalu pilih Buat server.
3. Pada halaman Pilih protokol, pilih AS2 (Pernyataan Penerapan 2), lalu pilih Berikutnya.
4. Pada halaman Pilih penyedia identitas, pilih Berikutnya.

Note

Untuk AS2, Anda tidak dapat memilih penyedia identitas karena otentikasi dasar tidak didukung untuk protokol AS2. Sebagai gantinya, Anda mengontrol akses melalui grup keamanan virtual private cloud (VPC).

5. Pada halaman Pilih titik akhir, lakukan hal berikut:

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

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

☐ FIPS Enabled endpoint

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

- a. Untuk jenis Endpoint, pilih VPC yang dihosting untuk meng-host endpoint server Anda. Untuk informasi tentang pengaturan VPC-hosted titik akhir Anda, lihat [Buat server di cloud pribadi virtual](#).

 Note

Titik akhir yang dapat diakses publik tidak didukung untuk protokol AS2. Untuk membuat titik akhir VPC Anda dapat diakses melalui internet, pilih Internet Facing di bawah Access, lalu berikan alamat IP Elastic Anda.

- b. Untuk Access, pilih salah satu opsi berikut:

- Internal — Pilih opsi ini untuk menyediakan akses dari dalam VPC dan VPC-connected lingkungan Anda, seperti pusat data lokal atau VPN. Direct Connect
- Menghadapi Internet — Pilih opsi ini untuk menyediakan akses melalui internet dan dari dalam VPC dan VPC-connected lingkungan Anda, seperti pusat data lokal di atas Direct Connect atau VPN.

Jika Anda memilih Internet Facing, berikan alamat IP Elastis Anda saat diminta.

- c. Untuk VPC, pilih VPC yang sudah ada atau pilih Buat VPC untuk membuat VPC baru.
- d. Untuk FIPS Diaktifkan, biarkan kotak centang titik akhir FIPS Enabled tetap bersih.

 Note

FIPS-enabled endpoint tidak didukung untuk protokol AS2.

- e. Pilih Berikutnya.
6. Pada halaman Pilih domain, pilih Amazon S3 untuk menyimpan dan mengakses file Anda sebagai objek dengan menggunakan protokol yang dipilih.

Pilih Berikutnya.

7. Pada halaman Konfigurasi detail tambahan, pilih pengaturan yang Anda butuhkan.

 Note

Jika Anda mengonfigurasi protokol lain bersama dengan AS2, semua pengaturan detail tambahan berlaku. Namun, untuk protokol AS2, satu-satunya pengaturan yang berlaku adalah yang ada di bagian CloudWatch logging dan Tags.

Meskipun pengaturan peran CloudWatch logging bersifat opsional, kami sangat menyarankan untuk mengaturnya sehingga Anda dapat melihat status pesan dan memecahkan masalah konfigurasi.

8. Pada halaman Tinjau dan buat, tinjau pilihan Anda untuk memastikannya benar.
 - Jika Anda ingin mengedit pengaturan apa pun, pilih Edit di samping langkah yang ingin Anda ubah.

 Note

Jika Anda mengedit langkah, kami sarankan Anda meninjau setiap langkah setelah langkah yang Anda pilih untuk diedit.

- Jika Anda tidak memiliki perubahan, pilih Buat server untuk membuat server Anda. Anda dibawa ke halaman Server, ditampilkan berikut, di mana server baru Anda terdaftar.

Diperlukan beberapa menit sebelum status server baru Anda berubah menjadi Online. Pada saat itu, server Anda dapat melakukan operasi file untuk pengguna Anda.

Gunakan template untuk membuat demo Transfer Family AS2 stack

Kami menyediakan CloudFormation template mandiri untuk membuat server AS2-enabled Transfer Family dengan cepat. Template mengonfigurasi server dengan titik akhir VPC Amazon publik, sertifikat, profil lokal dan mitra, perjanjian, dan konektor.

Template server AS2 dasar membuat sumber daya berikut:

- Server AS2-enabled Transfer Family dengan titik akhir VPC
- Profil AS2 lokal dan mitra dengan sertifikat
- Kesepakatan antara profil
- Bucket Amazon S3 untuk penyimpanan file
- Peran dan kebijakan IAM yang diperlukan
- CloudWatch konfigurasi logging

Sebelum menggunakan template ini, perhatikan hal berikut:

- Jika Anda membuat tumpukan dari template ini, Anda akan ditagih untuk AWS sumber daya yang digunakan.
- Template membuat beberapa sertifikat dan menyimpannya AWS Secrets Manager untuk menyimpannya dengan aman. Anda dapat menghapus sertifikat ini dari Secrets Manager jika mau, karena Anda dikenakan biaya untuk menggunakan layanan ini. Menghapus sertifikat ini di Secrets Manager tidak akan menghapusnya dari server Transfer Family. Oleh karena itu, fungsionalitas tumpukan demo tidak terpengaruh. Namun, untuk sertifikat yang akan Anda gunakan dengan

server produksi AS2, Anda mungkin ingin menggunakan Secrets Manager untuk mengelola dan memutar sertifikat tersimpan secara berkala.

- Kami menyarankan Anda menggunakan template sebagai basis saja, dan terutama untuk tujuan demonstrasi. Jika Anda ingin menggunakan tumpukan demo ini dalam produksi, kami sarankan Anda memodifikasi kode YAML template untuk membuat tumpukan yang lebih kuat. Misalnya, buat sertifikat tingkat produksi, dan buat AWS Lambda fungsi yang dapat Anda gunakan dalam produksi.

Untuk membuat server AS2-enabled Transfer Family dari CloudFormation template

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
 2. Di panel navigasi sebelah kiri, pilih Tumpukan.
 3. Pilih Buat tumpukan, lalu pilih Dengan sumber daya baru (standar).
 4. Di bagian Prasyarat - Siapkan templat, pilih Pilih templat yang ada.
 5. Salin tautan ini, [templat demo AS2](#), dan tempel ke bidang URL Amazon S3.
 6. Pilih Berikutnya.
 7. Pada halaman Tentukan detail tumpukan, beri nama tumpukan Anda, lalu tentukan parameter berikut:
 - Di bawah AS2, masukkan nilai untuk ID AS2 Lokal dan ID AS2 Mitra, atau terima default, dan, masing-masing. `local partner`
 - Di bawah Jaringan, masukkan nilai untuk masuk grup Keamanan CIDR IP, atau terima default, `0.0.0.0/0`
-  **Note**

Nilai ini, dalam format CIDR, menentukan alamat IP mana yang diizinkan untuk lalu lintas masuk ke server AS2. Nilai default, `0.0.0.0/0`, memungkinkan semua alamat IP.
- Di bawah Umum, masukkan nilai untuk Awalan, atau terima default, `transfer-as2`. Awalan ini ditempatkan sebelum nama sumber daya apa pun yang dibuat oleh tumpukan. Misalnya, jika Anda menggunakan awalan default, bucket Amazon S3 Anda diberi nama. `transfer-as2-amzn-s3-demo-bucket`
8. Pilih Berikutnya. Pada halaman Configure stack options, pilih Next lagi.

9. Tinjau detail tumpukan yang Anda buat, lalu pilih Buat tumpukan.

Note

Di bagian bawah halaman, di bawah Kemampuan, Anda harus mengakui bahwa CloudFormation mungkin membuat sumber daya AWS Identity and Access Management (IAM).

Setelah tumpukan dibuat, Anda dapat mengirim pesan uji AS2 dari server mitra ke server Transfer Family lokal Anda dengan menggunakan AWS Command Line Interface (AWS CLI). AWS CLI Perintah sampel untuk mengirim pesan pengujian dibuat bersama dengan semua sumber daya lain di tumpukan.

Untuk menggunakan perintah sampel ini, buka tab Output dari tumpukan Anda, dan salin. TransferExampleAs2Command Anda kemudian dapat menjalankan perintah dengan menggunakan AWS CLI. Jika Anda belum menginstal AWS CLI, lihat [Menginstal atau memperbarui versi terbaru dari AWS CLI](#) Panduan AWS Command Line Interface Pengguna.

Perintah sampel memiliki format berikut:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

Note

Versi Anda dari perintah ini berisi nilai aktual untuk *amzn-s3-demo-bucket* dan *TransferConnectorId* sumber daya di tumpukan Anda.

Perintah sampel ini terdiri dari dua perintah terpisah yang dirantai bersama dengan menggunakan && string.

Perintah pertama membuat file teks baru yang kosong di bucket Anda:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt
```

Kemudian, perintah kedua menggunakan konektor untuk mengirim file dari profil mitra ke profil lokal. Server Transfer Family memiliki pengaturan perjanjian yang memungkinkan profil lokal menerima pesan dari profil mitra.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
--send-file-paths /amzn-s3-demo-bucket/test.txt
```

Setelah menjalankan perintah, Anda dapat pergi ke bucket Amazon S3 (*amzn-s3-demo-bucket*) dan melihat isinya. Jika perintah berhasil, Anda akan melihat objek berikut di ember Anda:

- *processed/*— Folder ini berisi file JSON yang menjelaskan file yang ditransfer dan respons MDN.
- *processing/*— Folder ini sementara berisi file saat sedang diproses, tetapi setelah transfer selesai, folder ini harus kosong.
- *server-id/*— Folder ini diberi nama berdasarkan ID server Transfer Family Anda. Ini berisi *from-partner* (folder ini dinamai secara dinamis, berdasarkan ID AS2 mitra), yang berisi, *failed/processed/*, dan *processing/* folder. */server-id/from-partner/processed/* Folder berisi salinan file teks yang ditransfer, dan file JSON dan MDN yang sesuai.
- *test.txt*— Objek ini adalah file (kosong) yang ditransfer.

Buat perjanjian AS2

Perjanjian terkait dengan server Transfer Family. Mereka menentukan detail untuk mitra dagang yang menggunakan protokol AS2 untuk bertukar pesan atau file dengan menggunakan Transfer Family, untuk transfer masuk—mengirim file AS2 dari sumber eksternal milik mitra ke server Transfer Family.

Prosedur ini menjelaskan cara membuat perjanjian AS2 dengan menggunakan konsol Transfer Family. Jika Anda ingin menggunakan AWS CLI sebagai gantinya, lihat [the section called “Langkah 5: Buat kesepakatan antara Anda dan pasangan”](#).

Untuk membuat perjanjian untuk server Transfer Family

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server, lalu pilih server yang menggunakan protokol AS2.

Sebagai alternatif, selama Anda memiliki setidaknya satu server Transfer Family yang menggunakan protokol AS2, pilih Perjanjian untuk menerima pesan dari menu Mitra Trading AS2. Kemudian, di layar Buat perjanjian, pilih server AS2 yang ingin Anda kaitkan dengan perjanjian ini.

3. Pada halaman detail server, gulir ke bawah ke bagian Perjanjian.
4. Pilih Tambahkan perjanjian.
5. Isi parameter perjanjian, sebagai berikut:
 - a. Di bagian Konfigurasi Perjanjian, masukkan nama deskriptif. Pastikan bahwa Anda dapat mengidentifikasi tujuan perjanjian dengan namanya. Juga, atur Status untuk perjanjian: Aktif (dipilih secara default) atau Tidak Aktif.
 - b. Di bagian Konfigurasi komunikasi, pilih profil lokal dan profil mitra. Juga, pilih apakah akan menerapkan penandatanganan pesan atau tidak.
 - Secara default, Menegakkan penandatanganan pesan diaktifkan, yang berarti Transfer Family menolak pesan yang tidak ditandatangani dari mitra dagang Anda untuk perjanjian ini.
 - Hapus pengaturan ini untuk memungkinkan Transfer Family menerima pesan yang tidak ditandatangani dari mitra dagang Anda untuk perjanjian ini.
 - c. Di bagian konfigurasi direktori Kotak Masuk, berikan informasi berikut.
 - Tentukan apakah akan memilih Tentukan direktori terpisah untuk menyimpan pesan AS2, file MDN, dan file status JSON Anda atau tidak.
 - Jika Anda memilih opsi ini, Anda menentukan lokasi terpisah untuk file payload, file gagal, file MDN, file status, dan file sementara.
 - Jika Anda menghapus opsi ini, semua file AS2 masuk ke lokasi yang Anda tentukan untuk direktori dasar Anda.
 - Untuk S3 Bucket, pilih bucket Amazon S3.
 - Untuk Prefix, Anda dapat memasukkan awalan (folder) yang akan digunakan untuk menyimpan file di bucket.

Misalnya, jika Anda memasukkan **amzn-s3-demo-bucket** bucket dan **incoming** awalan, file AS2 Anda akan disimpan ke folder/**amzn-s3-demo-bucket**/incoming.

- Jika Anda menghapus pengaturan ini, ketika Transfer Family menyimpan file, nama file disesuaikan, seperti yang dijelaskan dalam. [Nama dan lokasi file](#)
- d. (Opsional) Tambahkan tag di bagian Tag.
 - e. Setelah Anda memasukkan semua informasi untuk perjanjian, pilih Buat perjanjian.

Perjanjian baru muncul di bagian Perjanjian pada halaman detail server.

Konfigurasikan konektor AS2

Tujuan dari konektor adalah untuk membangun hubungan antara mitra dagang untuk transfer keluar — mengirim file AS2 dari server Transfer Family ke tujuan eksternal milik mitra. Untuk konektor, Anda menentukan pihak lokal, mitra jarak jauh, dan sertifikat mereka (dengan membuat profil lokal dan mitra).

Setelah Anda memiliki konektor, Anda dapat mentransfer informasi ke mitra dagang Anda. Setiap server AS2 diberi tiga alamat IP statis. Konektor AS2 menggunakan alamat IP ini untuk mengirim mDNS asinkron ke mitra dagang Anda melalui AS2.

Note

Ukuran pesan yang diterima oleh mitra dagang tidak akan cocok dengan ukuran objek di Amazon S3. Perbedaan ini terjadi karena pesan AS2 membungkus file dalam amplop sebelum dikirim. Jadi, ukuran file mungkin meningkat, bahkan jika file dikirim dengan kompresi. Oleh karena itu, pastikan bahwa ukuran file maksimum mitra dagang lebih besar dari ukuran file yang Anda kirim.

1. [Impor sertifikat AS2](#)
2. [Buat profil AS2](#)
3. [Buat server AS2](#)
4. [Buat perjanjian AS2](#)
5. Buat konektor AS2

Buat konektor AS2

Prosedur ini menjelaskan cara membuat konektor AS2 dengan menggunakan AWS Transfer Family konsol. Jika Anda ingin menggunakan AWS CLI sebagai gantinya, lihat [the section called “Langkah 6: Buat konektor antara Anda dan pasangan”](#).

Untuk membuat konektor AS2

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Konektor untuk mengirim pesan, dari menu Mitra Perdagangan AS2, lalu pilih Buat konektor AS2.
3. Di bagian Konfigurasi konektor, tentukan informasi berikut:
 - URL — Masukkan URL untuk koneksi keluar.
 - Mode pengalamatan IP — Pilih IPv4 saja (default) untuk menggunakan alamat IPv4 secara eksklusif, atau Dual-stack untuk mendukung IPv6 dan IPv4. Dalam mode dual-stack, konektor lebih memilih IPv6 ketika resolusi DNS mengembalikan hasil IPv6, dan menggunakan IPv4 ketika hanya hasil DNS IPv4 yang dikembalikan.
 - Peran akses — Pilih Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang akan digunakan. Pastikan bahwa peran ini menyediakan akses baca dan tulis ke direktori induk dari lokasi file yang digunakan dalam `StartFileTransfer` permintaan. Selain itu, pastikan bahwa peran tersebut menyediakan akses baca dan tulis ke direktori induk dari file yang ingin Anda kirim `StartFileTransfer`.

Note

Jika Anda menggunakan otentikasi Dasar untuk konektor Anda, peran akses memerlukan `secretsmanager:GetSecretValue` izin untuk rahasia tersebut. Jika rahasia dienkripsi dengan menggunakan kunci yang dikelola pelanggan alih-alih Kunci yang dikelola AWS masuk AWS Secrets Manager, maka peran tersebut juga memerlukan `kms:Decrypt` izin untuk kunci itu. Jika Anda memberi nama rahasia Anda dengan awalan `aws/transfer/`, Anda dapat menambahkan izin yang diperlukan dengan karakter wildcard (*), seperti yang ditunjukkan dalam [izin Contoh untuk membuat](#) rahasia.

- Peran logging (opsional) - Pilih peran IAM untuk konektor yang akan digunakan untuk mendorong peristiwa ke CloudWatch log Anda.

4. Di bagian konfigurasi AS2, pilih profil lokal dan mitra, algoritma enkripsi dan penandatanganan, dan apakah akan mengompres informasi yang ditransfer. Perhatikan hal-hal berikut:

- Content-TypeParameter Preserve S3 diaktifkan secara default.

Saat disetel, Transfer Family menggunakan Amazon S3 Content-Type yang dikaitkan dengan objek di S3 alih-alih memetakan jenis konten berdasarkan ekstensi file. Hapus setelah ini jika Anda ingin layanan memetakan jenis konten untuk pesan AS2 Anda berdasarkan ekstensi file, daripada menggunakan jenis konten dari objek S3.

- Untuk algoritma enkripsi, jangan memilih DES_EDE3_CBC kecuali Anda harus mendukung klien lama yang membutuhkannya, karena ini adalah algoritma enkripsi yang lemah.
- Subjek digunakan sebagai atribut header subject HTTP dalam pesan AS2 yang sedang dikirim dengan konektor.
- Jika Anda memilih untuk membuat konektor tanpa algoritma enkripsi, Anda harus menentukan HTTPS sebagai protokol Anda.

5. Di bagian otentikasi dasar, tentukan informasi berikut.

- Untuk mengirim kredensial masuk bersama dengan pesan keluar, pilih Aktifkan otentikasi Dasar. Jika Anda tidak ingin mengirim kredensial apa pun dengan pesan keluar, pastikan Aktifkan otentikasi Dasar tetap bersih.
- Jika Anda menggunakan otentikasi, pilih atau buat rahasia.
 - Untuk membuat rahasia baru, pilih Buat rahasia baru lalu masukkan nama pengguna dan kata sandi. Kredensial ini harus sesuai dengan pengguna yang terhubung ke titik akhir mitra.

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret
☐ Choose an existing secret

Username
test-user

Password

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- Untuk menggunakan rahasia yang ada, pilih Pilih rahasia yang ada, lalu pilih rahasia dari menu tarik-turun. Untuk detail tentang membuat rahasia yang diformat dengan benar di Secrets Manager, lihat [Aktifkan otentikasi dasar untuk konektor AS2](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret
☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

6. Di bagian konfigurasi MDN, tentukan informasi berikut:

- Minta MDN — Anda memiliki opsi untuk meminta mitra dagang Anda mengirimkan Anda MDN setelah mereka berhasil menerima pesan Anda melalui AS2.

- Ditandatangani MDN — Anda memiliki opsi untuk meminta mDNS ditandatangani. Opsi ini hanya tersedia jika Anda telah memilih Permintaan MDN.
7. Setelah Anda mengonfirmasi semua pengaturan Anda, pilih **Buat konektor AS2** untuk membuat konektor.

Halaman Konektor muncul, dengan ID konektor baru Anda ditambahkan ke daftar. Untuk melihat detail konektor Anda, lihat [Lihat detail konektor AS2](#).

Algoritma konektor AS2

Saat Anda membuat konektor AS2, algoritma keamanan berikut terpasang ke konektor.

Tipe	Algoritme
Cipher TLS	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

Otentikasi dasar untuk konektor AS2

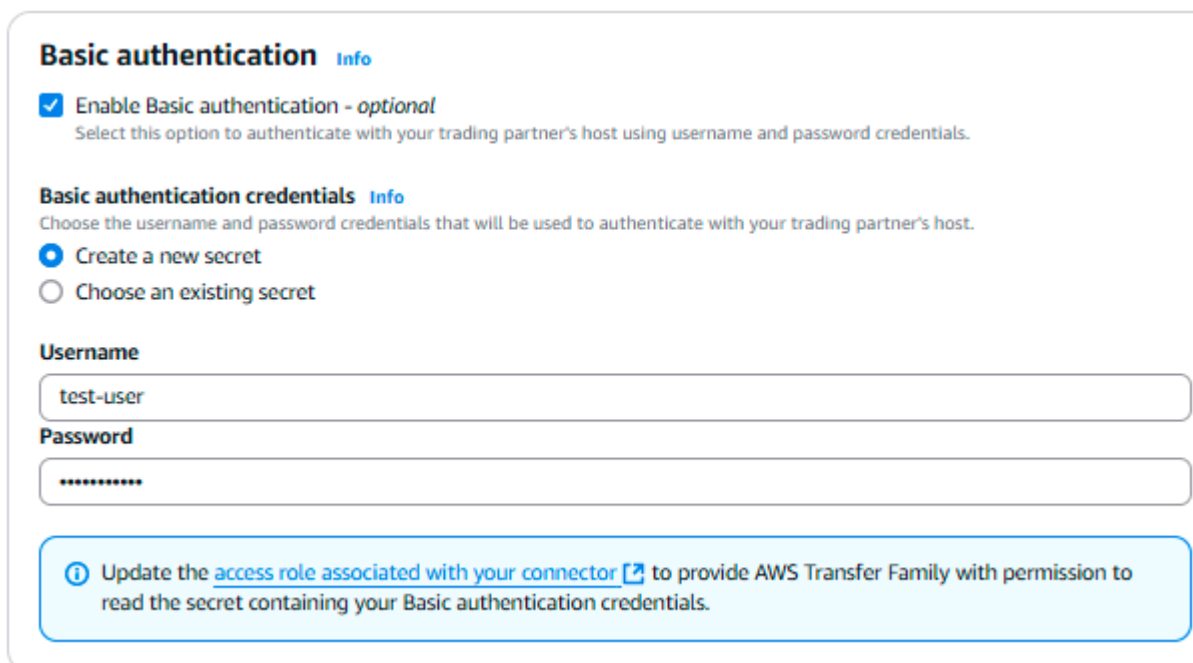
Saat membuat atau memperbarui server Transfer Family yang menggunakan protokol AS2, Anda dapat menambahkan otentikasi Dasar untuk pesan keluar. Anda melakukan ini dengan menambahkan informasi otentikasi ke konektor.

Note

Otentikasi dasar hanya tersedia jika Anda menggunakan HTTPS.

Untuk menggunakan otentikasi untuk konektor Anda, pilih Aktifkan otentikasi Dasar di bagian Autentikasi dasar. Setelah mengaktifkan otentikasi Dasar, Anda dapat memilih untuk membuat rahasia baru, atau menggunakan yang sudah ada. Dalam kedua kasus tersebut, kredensial dalam rahasia dikirim dengan pesan keluar yang menggunakan konektor ini. Kredensial harus sesuai dengan pengguna yang mencoba terhubung ke titik akhir jarak jauh mitra dagang.

Tangkapan layar berikut menunjukkan Aktifkan otentikasi Dasar dipilih, dan Buat rahasia baru yang dipilih. Setelah membuat pilihan ini, Anda dapat memasukkan nama pengguna dan kata sandi untuk rahasianya.



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.

Tangkapan layar berikut menunjukkan Aktifkan otentikasi dasar dipilih, dan Pilih rahasia yang ada dipilih. Rahasia Anda harus dalam format yang benar, seperti yang dijelaskan dalam [Aktifkan otentikasi dasar untuk konektor AS2](#).

Aktifkan otentikasi dasar untuk konektor AS2

Saat Anda mengaktifkan otentikasi Dasar untuk konektor AS2, Anda dapat membuat rahasia baru di konsol Transfer Family, atau Anda dapat menggunakan rahasia yang Anda buat. AWS Secrets Manager Dalam kedua kasus tersebut, rahasia Anda disimpan di Secrets Manager.

Topik

- [Buat rahasia baru di konsol](#)
- [Gunakan secret yang sudah ada](#)
- [Buat rahasia di AWS Secrets Manager](#)

Buat rahasia baru di konsol

Saat Anda membuat konektor di konsol, Anda dapat membuat rahasia baru.

Untuk membuat rahasia baru, pilih Buat rahasia baru lalu masukkan nama pengguna dan kata sandi. Kredensial ini harus sesuai dengan pengguna yang terhubung ke titik akhir mitra.

Basic authentication [Info](#)☒ **Enable Basic authentication - optional**

Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)

Choose the username and password credentials that will be used to authenticate with your trading partner's host.

- ☒ Create a new secret
- ☐ Choose an existing secret

Username**Password**

[i](#) Update the [access role associated with your connector](#) [↗](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

Note

Saat Anda membuat rahasia baru di konsol, nama rahasia mengikuti konvensi penamaan ini: **/aws/transfer/connector-id**, di mana **connector-id** ID konektor yang Anda buat. Pertimbangkan ini ketika Anda mencoba menemukan rahasianya AWS Secrets Manager.

Gunakan secret yang sudah ada

Saat Anda membuat konektor di konsol, Anda dapat menentukan rahasia yang ada.

Untuk menggunakan rahasia yang ada, pilih **Pilih rahasia yang ada**, lalu pilih rahasia dari menu tarik-turun. Untuk detail tentang membuat rahasia yang diformat dengan benar di Secrets Manager, lihat [Buat rahasia di AWS Secrets Manager](#).

Buat rahasia di AWS Secrets Manager

Prosedur berikut menjelaskan cara membuat rahasia yang sesuai untuk digunakan dengan konektor AS2 Anda.

Note

Otentikasi dasar hanya tersedia jika Anda menggunakan HTTPS.

Untuk menyimpan kredensial pengguna di Secrets Manager untuk otentikasi AS2 Basic

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pada panel navigasi kiri, pilih Rahasia.
3. Pada halaman Rahasia, pilih Simpan rahasia baru.
4. Pada halaman Pilih jenis rahasia, untuk tipe Rahasia, pilih Jenis rahasia lainnya.
5. Di bagian Key/value pasangan, pilih Key/valuetab.
 - Kunci — Masukkan **Username**.
 - nilai — Masukkan nama pengguna yang berwenang untuk terhubung ke server mitra.

6. Jika Anda ingin memberikan kata sandi, pilih Tambah baris, dan di bagian Key/value pasangan, pilih Key/valueta.

Pilih Tambah baris, dan di bagian Key/value pasangan, pilih Key/valueta.

- Kunci — Masukkan **Password**.
 - nilai — Masukkan kata sandi untuk pengguna.
7. Jika Anda ingin memberikan kunci pribadi, pilih Tambah baris, dan di bagian Key/value pasangan, pilih Key/valueta.
 - Kunci — Masukkan **PrivateKey**.
 - nilai — Masukkan kunci pribadi untuk pengguna. Nilai ini harus disimpan dalam format OpenSSH, dan harus sesuai dengan kunci publik yang disimpan untuk pengguna ini di server jarak jauh.
8. Pilih Berikutnya.
 9. Pada halaman Konfigurasi rahasia, masukkan nama dan deskripsi untuk rahasia Anda. Kami menyarankan Anda menggunakan awalan **aws/transfer/** untuk nama tersebut. Misalnya, Anda bisa menyebutkan rahasia Anda **aws/transfer/connector-1**.
 10. Pilih Berikutnya, dan kemudian terima default pada halaman Konfigurasi rotasi. Lalu pilih Selanjutnya.
 11. Pada halaman Review, pilih Store untuk membuat dan menyimpan rahasia.

Setelah Anda membuat rahasia, Anda dapat memilihnya saat Anda membuat konektor (lihat [Konfigurasi konektor AS2](#)). Pada langkah di mana Anda mengaktifkan otentikasi Dasar, pilih rahasia dari daftar dropdown rahasia yang tersedia.

Lihat detail konektor AS2

Anda dapat menemukan daftar detail dan properti untuk AWS Transfer Family konektor AS2 di AWS Transfer Family konsol. Properti konektor AS2 mencakup URL, peran, profil, mDNS, tag, dan metrik pemantauannya.

Ini adalah prosedur untuk melihat detail konektor.

Untuk melihat detail konektor

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.

2. Di panel navigasi kiri, pilih Konektor.
3. Pilih pengenal di kolom Connector ID untuk melihat halaman detail untuk konektor yang dipilih.

Anda dapat mengubah properti untuk konektor AS2 pada halaman detail konektor dengan memilih Edit.

C-

Delete

Connector configuration

Info

Edit

Name

my-as2-connector

Access role

URL

<https://www.example.com>

Logging role

[AWSTransferLoggingAccess](#)

Communication settings

Info

AS2-From header

AS2-To header

AS2 configuration

Info

Edit

Local profile

Compression

Enabled

Encryption algorithm

AES128_CBC

Partner profile

Message Subject

[View](#)

Signing algorithm

SHA384

Preserve S3 Content-Type

Enabled

MDN configuration

Info

Edit

Request MDN

Enabled

Signed MDN

Default to message signing algorithm: SHA384

Synchronization

Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**
✓ Enabled**Secret**
aws/transfer/c- [REDACTED] [Copy](#)**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

[Copy](#) 23.23.130.9[Copy](#) 44.196.109.11[Copy](#) 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

< 1 >

Key	Value
Name	my-as2-connector

AS2 Monitoring

3h

1d

1w

[Calendar](#)

UTC timezone

[Refresh](#)[Dropdown](#)[More](#)**OutboundMessage**

● OutboundMessage

OutboundMessage

1.00 No data available.
Try adjusting the dashboard time range.

0.50

0

13:05 16:00

OutboundFailedMessage

● OutboundFailedMessage

OutboundFailedMessage

1.00 No data available.
Try adjusting the dashboard time range.

0.50

0

13:05 16:00

Note

Anda bisa mendapatkan banyak informasi ini, meskipun dalam format yang berbeda, dengan menjalankan perintah berikut AWS Command Line Interface (AWS CLI) :

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

Untuk informasi selengkapnya, lihat [DescribeConnector](#) di referensi API.

Mengirim dan menerima pesan AS2

Bagian ini menjelaskan proses untuk mengirim dan menerima pesan AS2. Ini juga memberikan rincian tentang nama file dan lokasi yang terkait dengan pesan AS2.

Tabel berikut mencantumkan algoritma enkripsi yang tersedia untuk pesan AS2, dan kapan Anda dapat menggunakannya.

Enkripsi algoritme	HTTP	HTTPS	Catatan
AES128_CBC	Ya	Ya	
AES192_CBC	Ya	Ya	
AES256_CBC	Ya	Ya	
DES_EDE3_CBC	Ya	Ya	Hanya gunakan algoritma ini jika Anda harus mendukung klien lama yang membutuhkannya, karena ini adalah algoritma enkripsi yang lemah.
NONE	Tidak	Ya	Jika Anda mengirim pesan ke server Transfer Family, Anda hanya dapat memilih NONE apakah Anda menggunakan an Application Load Balancer (ALB).

Topik

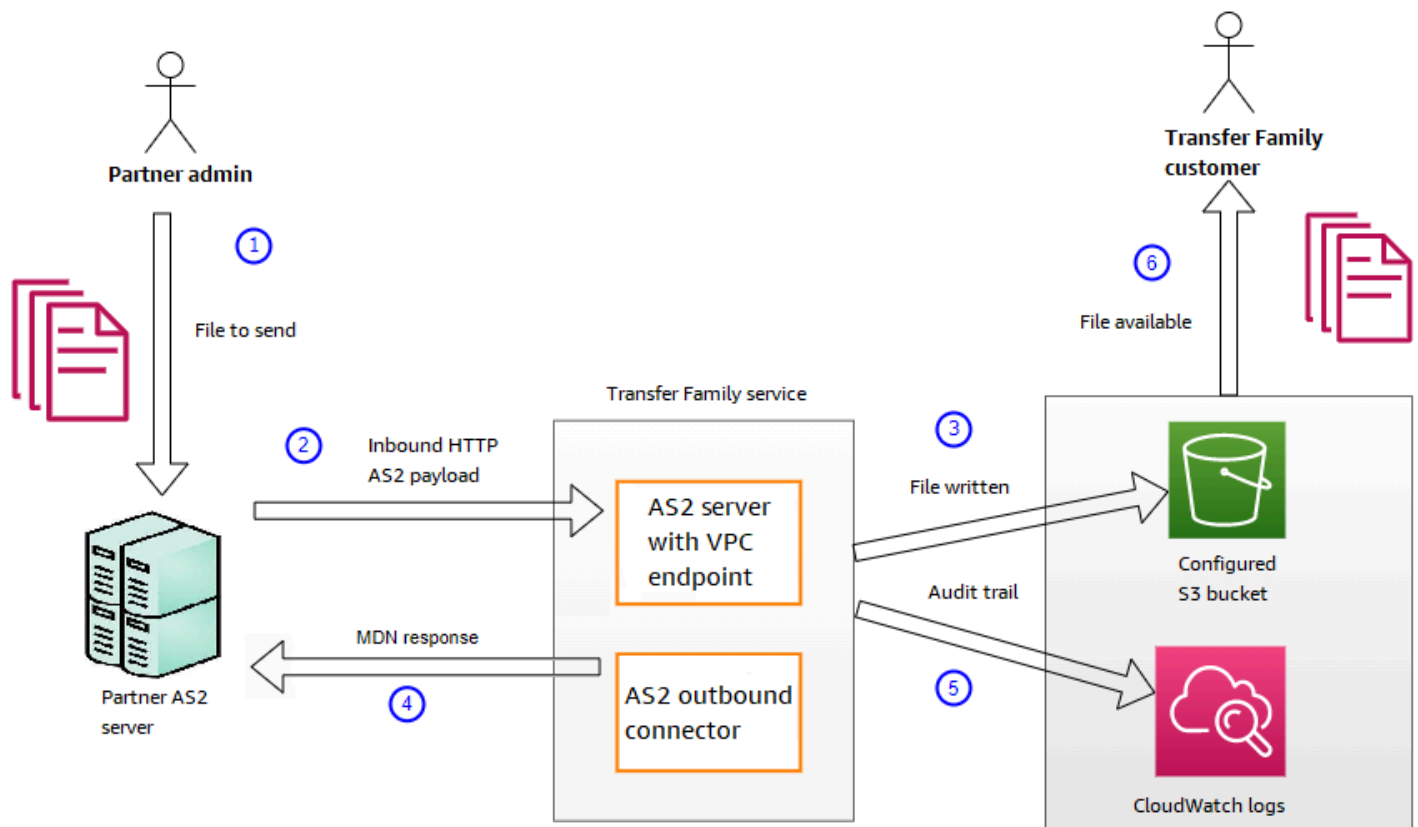
- [Menerima proses pesan AS2](#)
- [Mengirim dan menerima pesan AS2 melalui HTTPS](#)

- [Mentransfer file dengan menggunakan konektor AS2](#)
- [Nama dan lokasi file](#)
- [Kode status](#)
- [Contoh file JSON](#)

Menerima proses pesan AS2

Proses inbound didefinisikan sebagai pesan atau file yang sedang ditransfer ke AWS Transfer Family server Anda. Urutan pesan masuk adalah sebagai berikut:

1. Admin atau proses otomatis memulai transfer file AS2 di server AS2 jarak jauh mitra.
2. Server AS2 jarak jauh mitra menandatangani dan mengenkripsi konten file, lalu mengirimkan permintaan HTTP POST ke titik akhir masuk AS2 yang dihosting di Transfer Family.
3. Menggunakan nilai yang dikonfigurasi untuk server, mitra, sertifikat, dan perjanjian, Transfer Family mendekripsi dan memverifikasi payload AS2. Isi file disimpan di toko file Amazon S3 yang dikonfigurasi.
4. Respons MDN yang ditandatangani dikembalikan baik sebaris dengan respons HTTP, atau secara asinkron melalui permintaan HTTP POST terpisah kembali ke server asal.
5. Jejak audit ditulis ke Amazon CloudWatch dengan rincian tentang pertukaran.
6. File yang didekripsi tersedia dalam folder bernama. `inbox/processed`



Mengirim dan menerima pesan AS2 melalui HTTPS

Bagian ini menjelaskan cara mengonfigurasi server Transfer Family yang menggunakan protokol AS2 untuk mengirim dan menerima pesan melalui HTTPS.

Topik

- [Kirim pesan AS2 melalui HTTPS](#)
- [Terima pesan AS2 melalui HTTPS](#)

Kirim pesan AS2 melalui HTTPS

Untuk mengirim pesan AS2 menggunakan HTTPS, buat konektor dengan informasi berikut:

- Untuk URL, tentukan URL HTTPS
- Untuk algoritma enkripsi, pilih salah satu algoritma yang tersedia.

Note

Untuk mengirim pesan ke server Transfer Family saat tidak menggunakan enkripsi (yaitu, Anda memilih NONE algoritma enkripsi), Anda harus menggunakan Application Load Balancer (ALB).

- Berikan nilai yang tersisa untuk konektor seperti yang dijelaskan dalam [Konfigurasi konektor AS2](#).

Terima pesan AS2 melalui HTTPS

AWS Transfer Family Server AS2 saat ini hanya menyediakan transportasi HTTP melalui port 5080. Namun, Anda dapat menghentikan TLS pada penyeimbang beban jaringan atau aplikasi di depan titik akhir VPC server Transfer Family Anda dengan menggunakan port dan sertifikat pilihan Anda. Dengan pendekatan ini, Anda dapat memiliki pesan AS2 yang masuk menggunakan HTTPS.

Prasyarat

- VPC harus sama Wilayah AWS dengan server Transfer Family Anda.
- Subnet VPC Anda harus berada dalam Availability Zones tempat Anda ingin menggunakan server Anda.

Note

Setiap server Transfer Family dapat mendukung hingga tiga Availability Zone.

- Alokasikan hingga tiga alamat IP Elastis di Wilayah yang sama dengan server Anda. Atau, Anda dapat memilih untuk membawa rentang alamat IP Anda sendiri (BYOIP).

Note

Jumlah alamat IP Elastis harus sesuai dengan jumlah Availability Zone yang Anda gunakan dengan endpoint server Anda.

Anda dapat mengonfigurasi Network Load Balance (NLB) atau Application Load Balancer (ALB). Tabel berikut mencantumkan pro dan kontra untuk setiap pendekatan.

Tabel di bawah ini memberikan perbedaan kemampuan saat Anda menggunakan NLB versus ALB untuk mengakhiri TLS.

Fitur	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latensi	Latensi yang lebih rendah karena beroperasi pada lapisan jaringan.	Latensi yang lebih tinggi karena beroperasi pada lapisan aplikasi.
Dukungan IP statis	Dapat melampirkan alamat IP Elastis yang bisa statis.	Tidak dapat melampirkan alamat IP Elastis: menyediakan domain yang alamat IP dasarnya dapat berubah.
Perutean lanjutan	Tidak mendukung perutean lanjutan.	Mendukung perutean lanjutan. Dapat menyuntikkan X-Forwarded-Proto header yang diperlukan untuk AS2 tanpa enkripsi. Header ini dijelaskan di situs X-Forwarded-Proto web developer.mozilla.org .
TLS/SSL pemutusan	Mendukung TLS/SSL penghentian	Mendukung TLS/SSL penghentian
TLS Bersama (mTLS)	Transfer Family saat ini tidak mendukung penggunaan NLB untuk mTL	Support untuk mTLS

Configure NLB

Prosedur ini menjelaskan cara mengatur Network Load Balancer (NLB) yang menghadap ke internet di VPC Anda.

Untuk membuat Network Load Balancer dan mendefinisikan titik akhir VPC server sebagai target penyeimbang beban

1. Buka konsol Amazon Elastic Compute Cloud di <https://console.aws.amazon.com/ec2/>.
2. Dari panel navigasi, pilih Load Balancers, lalu pilih Create load balancer.
3. Di bawah Penyeimbang Beban Jaringan, pilih Buat.
4. Di bagian Konfigurasi dasar, masukkan informasi berikut:
 - Untuk Nama, masukkan nama deskriptif untuk penyeimbang beban.
 - Untuk Skema, pilih Internet-facing.
 - Untuk jenis alamat IP, pilih IPv4.
5. Di bagian Pemetaan jaringan, masukkan informasi berikut:
 - Untuk VPC, pilih virtual private cloud (VPC) yang Anda buat.
 - Di bawah Pemetaan, pilih Availability Zones yang terkait dengan subnet publik yang tersedia di VPC yang sama yang Anda gunakan dengan endpoint server Anda.
 - Untuk alamat IPv4 dari setiap subnet, pilih salah satu alamat IP elastis yang Anda alokasikan.
6. Di bagian Pendengar dan perutean, masukkan informasi berikut:
 - Untuk Protokol, pilih TLS.
 - Untuk Port, masukkan **5080**.
 - Untuk tindakan Default, pilih Buat grup target. Untuk detail pembuatan grup target baru, lihat [Untuk membuat grup target](#).

Setelah Anda membuat grup target, masukkan namanya di bidang Tindakan default.

7. Di bagian Pengaturan pendengar aman, pilih sertifikat Anda di area SSL/TLS sertifikat default.
8. Pilih Buat penyeimbang beban untuk membuat NLB Anda.
9. (Opsional, tetapi disarankan) Aktifkan log akses untuk Network Load Balancer untuk mempertahankan jejak audit penuh, seperti yang dijelaskan dalam [log Access untuk Network Load Balancer Anda](#).

Kami merekomendasikan langkah ini karena koneksi TLS dihentikan di NLB. Oleh karena itu, alamat IP sumber yang tercermin dalam grup CloudWatch log Transfer Family AS2 Anda adalah alamat IP pribadi NLB, bukan alamat IP eksternal mitra dagang Anda.

Configure ALB

Prosedur ini menjelaskan cara menyiapkan Application Load Balancer (ALB) di VPC Anda.

Untuk membuat Application Load Balancer dan mendefinisikan titik akhir VPC server sebagai target penyeimbang beban

1. Buka konsol Amazon Elastic Compute Cloud di <https://console.aws.amazon.com/ec2/>.
2. Dari panel navigasi, pilih Load Balancers, lalu pilih Create load balancer.
3. Di bawah Application Load Balancer, pilih Buat.
4. Di konsol ALB, buat pendengar HTTP baru di port 443 (HTTPS).
5. (Opsional). Jika Anda ingin mengatur otentikasi timbal balik (mTLS), konfigurasi pengaturan keamanan dan toko kepercayaan.
 - a. Lampirkan SSL/TLS sertifikat Anda ke pendengar.
 - b. Di bawah penanganan sertifikat Klien, pilih Mutual Authentication (mTLS).
 - c. Pilih Verifikasi dengan toko kepercayaan.
 - d. Di bawah pengaturan mTLS tingkat lanjut, pilih atau buat toko kepercayaan dengan mengunggah sertifikat CA Anda.
6. Buat grup target baru dan tambahkan alamat IP pribadi titik akhir server Transfer Family AS2 Anda sebagai target pada port 5080. Untuk detail pembuatan grup target baru, lihat [Untuk membuat grup target](#).
7. Konfigurasi pemeriksaan kesehatan untuk kelompok target untuk menggunakan protokol HTTP pada port 5080.
8. Buat aturan baru untuk meneruskan lalu lintas HTTPS dari pendengar ke grup target.
9. Konfigurasi listener untuk menggunakan SSL/TLS sertifikat Anda.

Setelah Anda mengatur penyeimbang beban, klien berkomunikasi dengan penyeimbang beban melalui pendengar port kustom. Kemudian, penyeimbang beban berkomunikasi dengan server melalui port 5080.

Untuk membuat grup target

1. Setelah Anda memilih Buat grup target dalam prosedur sebelumnya, Anda akan dibawa ke halaman Tentukan rincian grup untuk grup target baru.
2. Di bagian Konfigurasi dasar, masukkan informasi berikut.
 - Untuk Pilih jenis target, pilih alamat IP.
 - Untuk Name, masukkan nama untuk grup target.
 - Untuk Protokol, pilihan Anda tergantung pada apakah Anda menggunakan ALB atau NLB.
 - Untuk Network Load Balancer (NLB), pilih TCP
 - Untuk Application Load Balancer (ALB), pilih HTTP
 - Untuk Port, masukkan **5080**.
 - Untuk jenis alamat IP, pilih IPv4.
 - Untuk VPC, pilih VPC yang Anda buat untuk server Transfer Family AS2 Anda.
3. Di bagian Pemeriksaan Kesehatan, pilih protokol Pemeriksaan Kesehatan.
 - Untuk ALB, pilih HTTP
 - Untuk NLB, pilih TCP
4. Pilih Berikutnya.
5. Pada halaman Daftar target, masukkan informasi berikut:
 - Untuk Jaringan, konfirmasikan bahwa VPC yang Anda buat untuk server Transfer Family AS2 Anda ditentukan.
 - Untuk alamat IPv4, masukkan alamat IPv4 pribadi dari endpoint server Transfer Family AS2 Anda.

Jika Anda memiliki lebih dari satu titik akhir untuk server Anda, pilih Tambahkan alamat IPv4 untuk menambahkan baris lain untuk memasukkan alamat IPv4 lain. Ulangi proses ini sampai Anda memasukkan alamat IP pribadi untuk semua titik akhir server Anda.
 - Pastikan bahwa Port diatur ke **5080**.
 - Pilih Sertakan sebagai tertunda di bawah ini untuk menambahkan entri Anda ke bagian Tinjau target.
6. Di bagian Tinjau target, tinjau target IP Anda.
7. Pilih Buat grup target, lalu kembali ke prosedur sebelumnya untuk membuat NLB Anda dan masukkan grup target baru di mana ditunjukkan.

Uji akses ke server dari alamat IP Elastis

Connect ke server melalui port kustom dengan menggunakan alamat IP Elastis atau nama DNS Network Load Balancer.

Important

Kelola akses ke server Anda dari alamat IP klien dengan menggunakan [daftar kontrol akses jaringan \(ACL jaringan\)](#) untuk subnet yang dikonfigurasi pada penyeimbang beban. Izin ACL jaringan ditetapkan pada tingkat subnet, sehingga aturan berlaku untuk semua sumber daya yang menggunakan subnet. Anda tidak dapat mengontrol akses dari alamat IP klien dengan menggunakan grup keamanan, karena jenis target penyeimbang beban disetel ke alamat IP, bukan Instans. Oleh karena itu, penyeimbang beban tidak mempertahankan alamat IP sumber. Jika [pemeriksaan kesehatan Network Load Balancer](#) gagal, ini berarti penyeimbang beban tidak dapat terhubung ke titik akhir server. Untuk memecahkan masalah ini, periksa hal berikut:

- Konfirmasikan bahwa [grup keamanan terkait titik akhir](#) server memungkinkan koneksi masuk dari subnet yang dikonfigurasi pada penyeimbang beban. Load balancer harus dapat terhubung ke endpoint server melalui port 5080.
- Konfirmasikan bahwa Status server sedang Online.

Mentransfer file dengan menggunakan konektor AS2

Konektor AS2 membangun hubungan antara mitra dagang untuk transfer pesan AS2 dari server Transfer Family ke tujuan eksternal milik mitra.

Anda dapat menggunakan Transfer Family untuk mengirim pesan AS2 dengan mereferensikan ID konektor dan jalur ke file, seperti yang diilustrasikan dalam perintah `start-file-transfer` AWS Command Line Interface (AWS CLI) berikut:

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

Untuk mendapatkan detail konektor Anda, jalankan perintah berikut:

```
aws transfer list-connectors
```

list-connectors Perintah mengembalikan ID konektor, URL, dan Nama Sumber Daya Amazon (ARN) untuk konektor Anda.

Untuk mengembalikan properti konektor tertentu, jalankan perintah berikut dengan ID yang ingin Anda gunakan:

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

describe-connector Perintah mengembalikan semua properti untuk konektor, termasuk URL, peran, profil, Pemberitahuan Disposisi Pesan (mDNS), tag, dan metrik pemantauan.

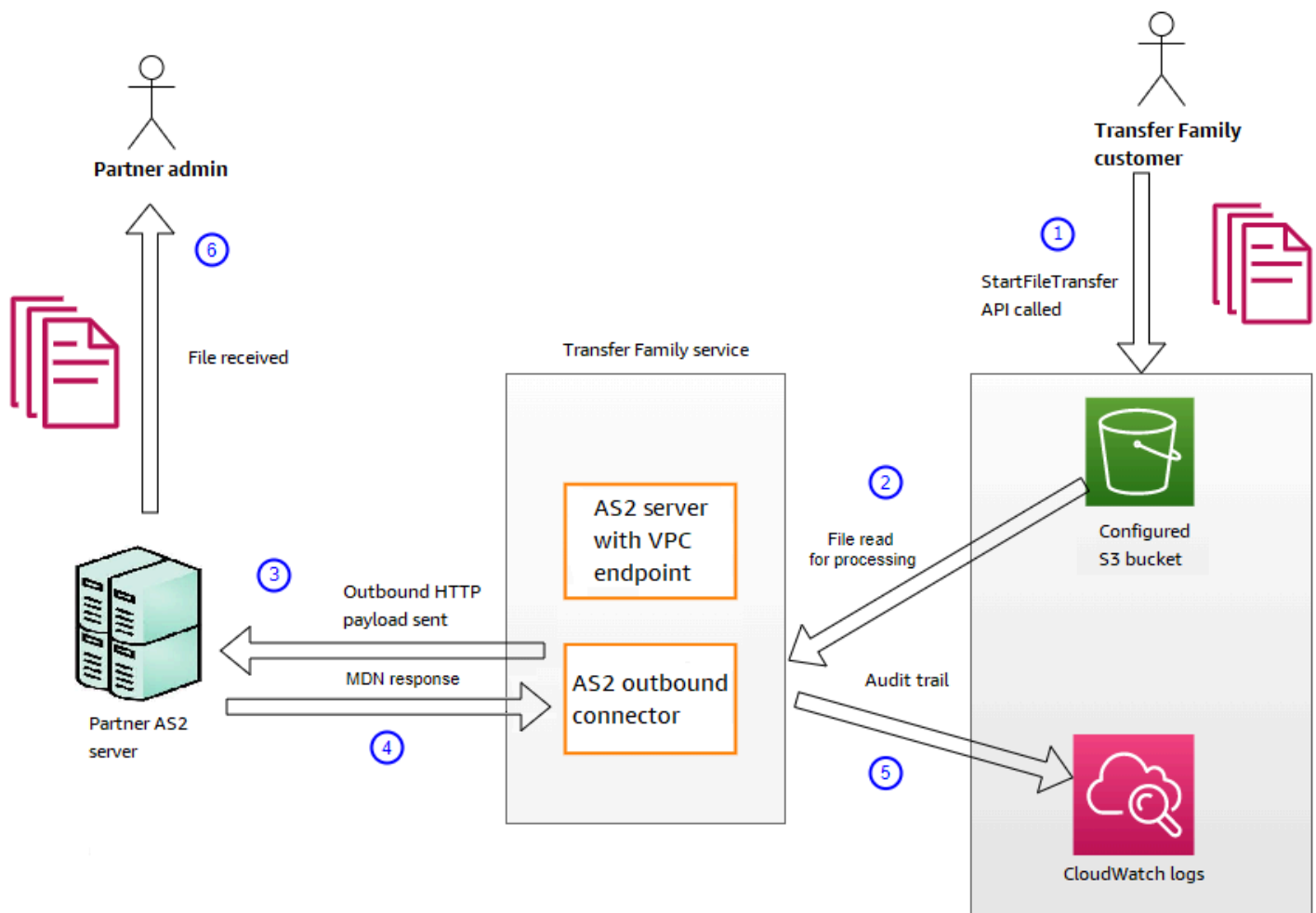
Anda dapat mengonfirmasi bahwa mitra berhasil menerima file dengan melihat file JSON dan MDN. File-file ini diberi nama sesuai dengan konvensi yang dijelaskan dalam [Nama dan lokasi file](#). Jika Anda mengonfigurasi peran logging saat membuat konektor, Anda juga dapat memeriksa CloudWatch log Anda untuk status pesan AS2.

Untuk melihat detail konektor AS2, lihat [Lihat detail konektor AS2](#). Untuk informasi selengkapnya tentang membuat konektor AS2, lihat [Konfigurasi konektor AS2](#).

Untuk mengirim pesan keluar AS2

Proses keluar didefinisikan sebagai pesan atau file yang dikirim dari AWS ke klien atau layanan eksternal. Urutan pesan keluar adalah sebagai berikut:

1. Admin memanggil perintah `start-file-transfer` AWS Command Line Interface (AWS CLI) atau operasi `StartFileTransfer` API. Operasi ini mereferensikan `connector` konfigurasi.
2. Transfer Family mendeteksi permintaan file baru dan menemukan file tersebut. File dikompresi, ditandatangani, dan dienkripsi.
3. Klien HTTP transfer melakukan permintaan HTTP POST untuk mengirimkan muatan ke server AS2 mitra.
4. Proses mengembalikan respons MDN yang ditandatangani, baik sejalan dengan respons HTTP (MDN sinkron atau asinkron).
5. Saat file bergerak di antara berbagai tahap transmisi, proses memberikan tanda terima respons MDN dan rincian pemrosesan kepada pelanggan.
6. Server AS2 jarak jauh membuat file yang didekripsi dan diverifikasi tersedia untuk admin mitra.



Pemrosesan AS2 mendukung banyak protokol RFC 4130, dengan fokus pada kasus penggunaan umum dan integrasi dengan implementasi server yang ada. AS2-enabled Untuk detail konfigurasi yang didukung, lihat [Konfigurasi AS2](#).

Nama dan lokasi file

Bagian ini membahas konvensi penamaan file untuk transfer AS2.

Untuk transfer file masuk, perhatikan hal berikut:

- Anda menentukan direktori dasar dalam perjanjian. Direktori dasar adalah nama bucket Amazon S3 yang dikombinasikan dengan awalan, jika ada. Misalnya, **/amzn-s3-demo-bucket/AS2-folder**.
- Jika file yang masuk berhasil diproses, file (dan file JSON yang sesuai) disimpan ke folder/processed. Misalnya, **/amzn-s3-demo-bucket/AS2-folder/processed**.

File JSON berisi bidang-bidang berikut:

- 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
- Jika file yang masuk tidak dapat diproses dengan sukses, file (dan file JSON yang sesuai) disimpan ke folder/failed. Misalnya, /amzn-s3-demo-bucket/AS2-folder/failed.
 - File yang ditransfer disimpan dalam processed folder sebagai *original_filename.messageId.original_extension*. Artinya, ID pesan untuk transfer ditambahkan ke nama file, sebelum ekstensi aslinya.
 - File JSON dibuat dan disimpan sebagai *original_filename.messageId.original_extension.json* file. Selain ID pesan yang ditambahkan, string .json ditambahkan ke nama file yang ditransfer.
 - File Message Disposition Notice (MDN) dibuat dan disimpan sebagai *original_filename.messageId.original_extension.mdn* file. Selain ID pesan yang ditambahkan, string .mdn ditambahkan ke nama file yang ditransfer.
 - Jika ada file inbound bernama `ExampleFileInS3Payload.dat`, file-file berikut dibuat:

- Berkas —

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

- JSON —

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

- MDN —

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

Untuk transfer keluar, penamaannya serupa, dengan perbedaan bahwa tidak ada file pesan masuk, dan juga, ID transfer untuk pesan yang ditransfer ditambahkan ke nama file. ID transfer dikembalikan oleh operasi StartFileTransfer API (atau ketika proses atau skrip lain memanggil operasi ini).

- `transfer-id` adalah pengidentifikasi yang terkait dengan transfer file. Semua permintaan yang merupakan bagian dari StartFileTransfer panggilan berbagi `transfer-id`.
- Direktori dasar sama dengan jalur yang Anda gunakan untuk file sumber. Artinya, direktori dasar adalah jalur yang Anda tentukan dalam operasi atau `start-file-transfer` AWS CLI perintah StartFileTransfer API. Contoh:

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/
file-to-send.txt
```

Jika Anda menjalankan perintah ini, file MDN dan JSON disimpan di `/amzn-s3-demo-bucket/AS2-folder/processed` (untuk transfer yang berhasil), atau `/amzn-s3-demo-bucket/AS2-folder/failed` (untuk transfer yang gagal).

- File JSON dibuat dan disimpan sebagai `original_filename.transferId.messageId.original_extension.json` file.
- File MDN dibuat dan disimpan sebagai `original_filename.transferId.messageId.original_extension.mdn` file.
- Jika ada file keluar bernama `ExampleFileOutTestOutboundSyncMdn.dat`, file berikut dibuat:
 - 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`

Anda juga dapat memeriksa CloudWatch log untuk melihat detail transfer Anda, termasuk yang gagal.

Kode status

Tabel berikut mencantumkan semua kode status yang dapat dicatat ke CloudWatch log saat Anda atau pasangan Anda mengirim pesan AS2. Langkah-langkah pemrosesan pesan yang berbeda berlaku untuk jenis pesan yang berbeda dan dimaksudkan untuk pemantauan saja. Status COMPLETED dan FAILED mewakili langkah terakhir dalam pemrosesan, dan terlihat dalam file JSON.

Kode	Deskripsi	Pemrosesan selesai?
PENGOLAHAN	Pesan sedang dalam proses dikonversi ke format akhirnya. Misalnya, langkah dekompresi dan dekripsi keduanya memiliki status ini.	Tidak
MDN_TRANSMIT	Pemrosesan pesan adalah mengirimkan respons MDN.	Tidak
MDN_RECEIVE	Pemrosesan pesan menerima respons MDN.	Tidak
DISELESAIKAN	Pemrosesan pesan telah selesai dengan sukses. Keadaan ini termasuk ketika MDN dikirim untuk pesan masuk atau untuk verifikasi MDN dari pesan keluar.	Ya
FAILED	Pemrosesan pesan telah gagal. Untuk daftar kode kesalahan, lihat Kode kesalahan AS2 .	Ya

Contoh file JSON

Bagian ini mencantumkan contoh file JSON untuk transfer masuk dan keluar, termasuk file sampel untuk transfer yang berhasil dan transfer yang gagal.

Contoh file keluar yang berhasil ditransfer:

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/amzn-s3-demo-bucket/as2testcell10000/openAs2/TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

Contoh file keluar yang tidak berhasil ditransfer:

```
{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner 9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
}
```

```

"connector-id": "c-056e15cc851f4b2e9",
"file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
"timestamp": "2022-07-11T21:17:24.802378Z"
}

```

Contoh file inbound yang berhasil ditransfer:

```

{
  "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_0ID",
  "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_0ID_PartnerA_0ID",
  "as2-to": "PartnerA_0ID",
  "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"
}

```

Contoh file masuk yang tidak berhasil ditransfer:

```

{
  "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"
}
```

Sesuaikan header HTTP untuk pesan AS2

Saat mengirim pesan AS2 ke mitra dagang, Anda mungkin perlu menyesuaikan header HTTP untuk memenuhi persyaratan tertentu atau meningkatkan kompatibilitas dengan konfigurasi server AS2 mitra Anda. CloudFormation Template ini membuat infrastruktur untuk mengaktifkan header HTTP yang disesuaikan untuk pesan AS2 yang dikirim. AWS Transfer Family Ini mengatur fungsi Amazon API Gateway dan Lambda untuk bertindak sebagai proxy, memungkinkan modifikasi dinamis header yang diperlukan oleh server AS2 mitra dagang.

Gunakan template ini untuk melakukan hal berikut:

- Tambahkan header HTTP kustom ke pesan AS2 keluar
- Ganti nilai header default dengan nilai kustom

Important

Hati-hati saat mengganti nilai header default, karena dapat menyebabkan kegagalan pengiriman: beberapa header AS2 diperlukan.

- Pastikan kompatibilitas dengan mitra dagang yang memiliki persyaratan header tertentu

Gambaran Umum Templat

Template membuat komponen utama berikut:

- Fungsi Lambda yang memproses dan meneruskan pesan AS2
- Amazon API Gateway untuk mengekspos fungsi Lambda
- Peran dan izin IAM untuk fungsi Lambda
- Sumber daya bersyarat untuk dukungan HTTPS

File template tersedia di sini: [Template header HTTP dinamis](#).

Cara Kerjanya

1. Amazon API Gateway menerima pesan AS2 masuk dari. AWS Transfer Family
2. Permintaan diteruskan ke fungsi Lambda.
3. Fungsi Lambda memproses permintaan, menambahkan atau memodifikasi header sesuai kebutuhan.
4. Permintaan yang dimodifikasi kemudian diteruskan ke server AS2 mitra.
5. Respons dari server mitra dikembalikan melalui Lambda dan Amazon API Gateway kembali ke. AWS Transfer Family

Fitur Utama

- Modifikasi Header Dinamis: Memungkinkan kustomisasi header Subjek dan penambahan header lain yang diperlukan.
- Protocol Support: Bekerja dengan protokol HTTP dan HTTPS.
- Konfigurasi Fleksibel: Memungkinkan spesifikasi host mitra, port, dan jalur.

Detail Implementasi

Template mengimplementasikan komponen kunci berikut:

Fungsi Lambda

Inti dari solusinya adalah fungsi Node.js Lambda yang:

- Menerima permintaan dari Amazon API Gateway
- Memodifikasi header berdasarkan konfigurasi dan data permintaan masuk
- Meneruskan permintaan yang dimodifikasi ke server AS2 mitra
- Menangani protokol HTTP dan HTTPS
- Termasuk penanganan kesalahan dan pencatatan

Amazon API Gateway

API HTTP diatur untuk:

- Terima pesan AS2 yang masuk
- Permintaan rute ke fungsi Lambda
- Kembalikan tanggapan kembali ke AWS Transfer Family

Parameter template

Masukkan informasi untuk parameter template sebagai berikut. Perhatikan bahwa semua parameter ini adalah string.

- `Environment`: parameter ini digunakan untuk memberi nama sumber daya yang dibuat template: apakah mereka dimaksudkan untuk pengembangan atau lingkungan produksi. Nilai yang valid adalah `dev` dan `prod`.
- `PartnerHost`: alamat IP atau nama host dari server mitra AS2.
- `PartnerPort`: nomor port untuk server mitra AS2. Jika tidak ditentukan, default ke 80 untuk HTTP dan 443 untuk HTTPS.
- `PartnerPath`: jalur ke titik akhir AS2 di server mitra
- `ProtocolType`: protokol yang digunakan untuk komunikasi AS2: nilai yang valid adalah HTTP dan HTTPS.

Sumber Daya Bersyarat

Untuk dukungan HTTPS, template membuat secara kondisional:

- Lapisan Lambda untuk sertifikat CA
- HTTPS-specific konfigurasi dalam fungsi Lambda

Penerapan dan Penggunaan

Untuk menyesuaikan header HTTP AS2 menggunakan template CloudFormation

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Di panel navigasi sebelah kiri, pilih Tumpukan.
3. Pilih Buat tumpukan, lalu pilih Dengan sumber daya baru (standar).
4. Di bagian Prasyarat - Siapkan templat, pilih Pilih templat yang ada.
5. Salin tautan ini, [template header HTTP Dinamis](#), dan tempel ke bidang URL Amazon S3.

6. Pilih Berikutnya.
7. Isi detail parameter dengan informasi Anda. Ini dirinci dalam [Parameter template](#).
8. Pilih Berikutnya. Pada halaman Configure stack options, pilih Next lagi.
9. Tinjau detail tumpukan yang Anda buat, lalu pilih Buat tumpukan.

 Note

Di bagian bawah halaman, di bawah Kemampuan, Anda harus mengakui bahwa CloudFormation mungkin membuat sumber daya AWS Identity and Access Management (IAM).

Setelah menerapkan CloudFormation tumpukan ini:

1. Perhatikan URL titik akhir Amazon API Gateway yang disediakan dalam output tumpukan.
2. Perbarui AWS Transfer Family Konektor yang ada untuk menggunakan titik akhir Amazon API Gateway baru ini.
3. Solusinya sekarang akan menangani pesan AS2, menambahkan atau memodifikasi header seperti yang dikonfigurasi.

 Warning

Hanya ubah header Subjek atau tambahkan header yang diharapkan pasangan Anda secara eksplisit. Mengubah header lain dapat menyebabkan kegagalan transfer.

Memantau penggunaan AS2

Anda dapat memantau aktivitas AS2 menggunakan Amazon CloudWatch dan AWS CloudTrail. Untuk melihat metrik server Transfer Family lainnya, lihat [Amazon CloudWatch logging untuk AWS Transfer Family server](#)

Metrik AS2

Metrik	Deskripsi
InboundMessage	Jumlah total pesan AS2 yang berhasil diterima dari mitra dagang. Unit: Hitungan Periode: 5 menit
InboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil diterima dari mitra dagang. Artinya, mitra dagang mengirim pesan, tetapi server Transfer Family tidak berhasil memprosesnya. Unit: Hitungan Periode: 5 menit
OutboundMessage	Jumlah total pesan AS2 yang berhasil dikirim dari server Transfer Family ke mitra dagang. Unit: Hitungan Periode: 5 menit
OutboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil dikirim ke mitra dagang. Artinya, mereka dikirim dari server Transfer Family, tetapi tidak berhasil diterima oleh mitra dagang. Unit: Hitungan Periode: 5 menit
DaysUntilExpiry	Jumlah hari sampai Sertifikat berakhir ditentukan oleh InactiveDate set pada Sertifikat saat mengimpor. Unit: Hitungan

Metrik	Deskripsi
	Dimensi: CertificateId , Description (jika disediakan) Periode: 1 hari Untuk informasi selengkapnya, lihat Rotasi sertifikat AS2.

Kode Status AS2

Tabel berikut mencantumkan semua kode status yang dapat dicatat ke CloudWatch log saat Anda atau pasangan Anda mengirim pesan AS2. Langkah-langkah pemrosesan pesan yang berbeda berlaku untuk jenis pesan yang berbeda dan dimaksudkan untuk pemantauan saja. Status COMPLETED dan FAILED mewakili langkah terakhir dalam pemrosesan, dan terlihat dalam file JSON.

Kode	Deskripsi	Pemrosesan selesai?
PENGOLAHAN	Pesan sedang dalam proses dikonversi ke format akhirnya. Misalnya, langkah dekompresi dan dekripsi keduanya memiliki status ini.	Tidak
MDN_TRANSMIT	Pemrosesan pesan adalah mengirimkan respons MDN.	Tidak
MDN_RECEIVE	Pemrosesan pesan menerima respons MDN.	Tidak
DISELESAIKAN	Pemrosesan pesan telah berhasil diselesaikan. Keadaan ini termasuk ketika MDN dikirim untuk pesan masuk atau untuk verifikasi MDN dari pesan keluar.	Ya

Kode	Deskripsi	Pemrosesan selesai?
FAILED	Pemrosesan pesan telah gagal. Untuk daftar kode kesalahan, lihat Kode kesalahan AS2 .	Ya

Kode kesalahan AS2

Tabel berikut mencantumkan dan menjelaskan kode kesalahan yang mungkin Anda terima dari transfer file AS2.

Kode kesalahan AS2

Kode	Kesalahan	Deskripsi dan resolusi
ACCESS_DENIED	- Akses ditolak. Periksa apakah peran akses Anda memiliki izin yang diperlukan. - Jalur berkas tidak valid <i>send-file-path</i> - Gagal mendapatkan kredensial dengan: ErrorCode <i>error-code</i>	Terjadi saat menangani <code>StartFileTransfer</code> permintaan di mana salah satu dari <code>SendFilePaths</code> yang tidak valid atau cacat. Artinya, jalur tersebut tidak memiliki nama bucket Amazon S3, atau jalurnya menyertakan karakter yang tidak valid. Juga terjadi jika Transfer Family gagal mengambil peran akses atau peran logging. Pastikan jalur berisi nama bucket Amazon S3 dan nama kunci yang valid.
AGREEMENT_NOT_FOUND	Kesepakatan tidak ditemukan.	Entah perjanjian itu tidak ditemukan, atau perjanjian dikaitkan dengan profil yang tidak aktif.

Kode	Kesalahan	Deskripsi dan resolusi
		Perbarui perjanjian dalam server Transfer Family untuk menyertakan profil aktif.
CONNECTOR_NOT_FOUND	Konektor atau konfigurasi terkait tidak ditemukan.	Entah konektor tidak ditemukan, atau konektor dikaitkan dengan profil yang tidak aktif. Perbarui konektor untuk menyertakan profil aktif.

Kode	Kesalahan	Deskripsi dan resolusi
CREDENTIALS_RETRIEVAL_FAILED	1. Rahasia tidak ditemukan di Secrets Manager. 2. Tidak dapat mengakses Secrets Manager. 3. Gagal mendekripsi rahasia di Secrets Manager. 4. Tidak bisa mendapatkan nilai rahasia karena pelambatan.	Untuk otentikasi AS2 Basic, rahasia harus diformat dengan benar. Resolusi berikut sesuai dengan kesalahan yang tercantum di kolom sebelumnya. 1. Pastikan bahwa ID rahasia sudah benar. 2. Pastikan bahwa peran akses memiliki izin yang sesuai untuk membaca rahasia. Peran akses harus menyediakan akses baca dan tulis ke direktori induk dari lokasi file yang digunakan dalam <code>StartFileTransfer</code> permintaan. Selain itu, pastikan bahwa peran tersebut menyediakan akses baca dan tulis ke direktori induk dari file yang ingin Anda kirim <code>StartFileTransfer</code>. 3. Jika kunci yang dikelola pelanggan digunakan untuk rahasia, pastikan bahwa peran akses memiliki izin untuk kunci AWS Key Management Service (AWS KMS).

Kode	Kesalahan	Deskripsi dan resolusi
		4. Untuk kuota yang berlaku, lihat Kuota untuk menangani rahasia .
DECOMPRESSION_FAILED	Gagal mendekompresi pesan.	Entah file yang dikirim rusak, atau algoritma kompresi tidak valid. Kirim ulang pesan dan verifikasi bahwa kompresi ZLIB digunakan, atau kirim ulang pesan tanpa kompresi diaktifkan.
DECRYPT_FAILED	Gagal mendekripsi pesan. <i>message-ID</i> Pastikan mitra memiliki kunci enkripsi publik yang benar.	Dekripsi gagal. Konfirmasikan bahwa mitra mengirim muatan dengan menggunakan sertifikat yang valid dan enkripsi itu dilakukan dengan menggunakan algoritma enkripsi yang valid.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	Tidak dapat mengurai mimePart yang diselimuti.	Payload MIME rusak atau dalam format SMIME yang tidak didukung. Pengirim harus memastikan bahwa format yang mereka gunakan didukung, dan kemudian mengirim ulang payload.

Kode	Kesalahan	Deskripsi dan resolusi
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	Tidak ada kunci dekripsi yang cocok ditemukan.	Profil mitra tidak memiliki sertifikat yang ditetapkan yang cocok dengan pesan, atau sertifikat yang cocok dengan pesan sekarang kedaluwarsa atau tidak lagi valid. Anda harus memperbarui profil mitra dan memastikan bahwa itu berisi sertifikat yang valid.
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	Dekripsi Muatan SMIME diminta menggunakan algoritma yang tidak didukung dengan ID: <i>encryption-ID</i>	Pengirim jarak jauh telah mengirim muatan AS2 dengan algoritma enkripsi yang tidak didukung. Pengirim harus memilih algoritma enkripsi yang didukung oleh AWS Transfer Family.
DUPLICATE_MESSAGE	Langkah duplikat atau proses ganda.	Muatan memiliki langkah pemrosesan duplikat. Misalnya, ada dua langkah enkripsi. Kirim ulang pesan dengan satu langkah untuk penandatanganan, kompresi, dan enkripsi.

Kode	Kesalahan	Deskripsi dan resolusi
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	Tidak ada sertifikat enkripsi publik yang valid yang ditemukan di profil: <i>local-profile-ID</i>	Transfer Family mencoba mengenkripsi pesan keluar, tetapi tidak ada sertifikat enkripsi yang ditemukan untuk profil lokal. Opsi resolusi: • Pastikan bahwa profil lokal memiliki sertifikat dan kunci pribadi untuk enkripsi terlampir. • Pastikan sertifikat enkripsi saat ini aktif.
ENCRYPTION_FAILED	Gagal mengenkripsi file <i>file-name</i> .	File yang akan dikirim tidak tersedia untuk enkripsi. Verifikasi bahwa file tersebut berada di lokasi AS2 yang diharapkan dan yang AWS Transfer Family memiliki izin untuk membaca file.
FILE_SIZE_TOO_LARGE	Ukuran file terlalu besar.	Ini terjadi saat mengirim atau menerima file yang melebihi batas ukuran file.

Kode	Kesalahan	Deskripsi dan resolusi
HTTP_ERROR_RESPONSE_FROM_PARTNER	<i>partner-URL</i> mengembalikan status 400 untuk pesan dengan ID <i>=message-ID</i> .	Berkomunikasi dengan server AS2 mitra mengembalikan kode respons HTTP yang tidak terduga. Mitra mungkin dapat memberikan lebih banyak diagnostik dari log server AS2 mereka.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	Enkripsi diperlukan.	Mitra mengirim pesan yang tidak terenkripsi ke Transfer Family, yang tidak didukung. Pengirim harus menggunakan muatan terenkripsi.
INVALID_ENDPOINT_PROTOCOL	Hanya HTTP dan HTTPS yang didukung.	Anda harus menentukan HTTP atau HTTPS sebagai protokol dalam konfigurasi konektor AS2 Anda.

Kode	Kesalahan	Deskripsi dan resolusi
INVALID_REQUEST	1. Ada masalah dengan header pesan. 2. Tidak dapat mengurai JSON rahasia. Secret JSON tidak cocok dengan format yang diharapkan. 3. Rahasia harus berupa string JSON. 4. Nama pengguna tidak boleh mengandung titik dua. Nama pengguna tidak boleh mengandung karakter kontrol. Nama pengguna harus hanya berisi karakter ASCII. Kata sandi tidak boleh mengandung karakter kontrol. Kata sandi harus hanya berisi karakter ASCII.	Kesalahan ini memiliki beberapa penyebab. Resolusi berikut sesuai dengan kesalahan yang tercantum di kolom sebelumnya. 1. Periksa as2-from dan as2-to bidang. Pastikan ID pesan asli akurat untuk format MDN. Pastikan juga bahwa format ID pesan tidak hilang header AS2. 2. Pastikan bahwa nilai rahasia cocok dengan format yang didokumentasikan, seperti yang dijelaskan dalam Aktifkan otentikasi dasar untuk konektor AS2. 3. Pastikan bahwa rahasia disediakan sebagai string, dan bukan sebagai biner. 4. Lakukan koreksi yang diperlukan untuk nama pengguna atau kata sandi.

Kode	Kesalahan	Deskripsi dan resolusi
INVALID_URL_FORMAT	Format URL tidak valid: <i>URL</i>	Ini terjadi ketika Anda mengirim pesan keluar menggunakan konektor yang dikonfigurasi dengan URL yang salah bentuk. Pastikan konektor dikonfigurasi dengan URL HTTP atau HTTPS yang valid.
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	Tidak berlaku	Penerima tidak dapat mengautentikasi pengirim. Mitra dagang mengembalikan MDN ke Transfer Family dengan pengubah disposisi Error: authentication-failed.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	Tidak berlaku	Ini terjadi ketika penerima tidak dapat mendekomposisi isi pesan. Mitra dagang mengembalikan MDN ke Transfer Family dengan pengubah disposisi Error: decompression-failed.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	Tidak berlaku	Penerima tidak dapat mendekripsi isi pesan. Mitra dagang mengembalikan MDN ke Transfer Family dengan pengubah disposisi Error: authentication-failed.

Kode	Kesalahan	Deskripsi dan resolusi
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	Tidak berlaku	Penerima mengharapkan pesan ditandatangani atau dienkripsi, tetapi sebenarnya tidak. Mitra dagang mengembalikan MDN ke Transfer Family dengan pengubah disposisi Kesalahan : insufficient-message-security. Aktifkan and/or enkripsi penandatanganan pada konektor agar sesuai dengan harapan mitra dagang.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Tidak berlaku	Penerima tidak dapat memverifikasi integritas konten. Mitra dagang mengembalikan MDN ke Transfer Family dengan pengubah disposisi Error: integrity-check-failed.
PATH_NOT_FOUND	Tidak dapat membuat direktori <i>file-path</i> . Jalur induk tidak dapat ditemukan.	Transfer Family mencoba membuat direktori di bucket Amazon S3 pelanggan, tetapi bucket tidak ditemukan. Pastikan bahwa setiap jalur yang disebutkan dalam StartFileTransfer perintah berisi nama bucket yang ada.

Kode	Kesalahan	Deskripsi dan resolusi
SEND_FILE_NOT_FOUND	Jalur file <i>file-path</i> tidak ditemukan.	Transfer Family tidak dapat menemukan file dalam operasi kirim file. Periksa apakah direktori dan jalur home yang dikonfigurasi valid dan Transfer Family telah membaca izin untuk file tersebut.
SERVER_NOT_FOUND	Server yang terkait dengan pesan tidak dapat ditemukan.	Transfer Family tidak dapat menemukan server saat menerima pesan. Hal ini dapat terjadi jika server dihapus selama pemrosesan pesan masuk.
SERVER_NOT_ONLINE	Server <i>server-ID</i> tidak online.	Server Transfer Family sedang offline. Mulai server sehingga dapat menerima dan memproses pesan.
SIGNING_FAILED	Gagal menandatangani berkas.	File yang akan dikirim tidak tersedia untuk ditandatangani, atau penandatanganan tidak dapat dilakukan. Verifikasi bahwa file tersebut berada di lokasi AS2 yang diharapkan dan yang AWS Transfer Family memiliki izin untuk membaca file.

Kode	Kesalahan	Deskripsi dan resolusi
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	Tidak ada sertifikat yang ditemukan untuk profil: <i>local-profile-ID</i> .	Mencoba menandatangani pesan keluar, tetapi tidak ada sertifikat penandatanganan yang ditemukan untuk profil lokal. Opsi resolusi: • Pastikan bahwa profil lokal memiliki sertifikat dan kunci pribadi untuk penandatanganan terlampir. • Pastikan sertifikat penandatanganan saat ini aktif.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	Tidak dapat menyelesaikan nama host ke alamat IP.	Transfer Family tidak dapat melakukan resolusi alamat DNS ke IP pada server DNS publik yang dikonfigurasi di konektor AS2. Perbarui konektor untuk menunjuk ke URL mitra yang valid.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	Koneksi ke titik akhir habis waktu.	Transfer Family tidak dapat membuat koneksi soket ke server AS2 mitra yang dikonfigurasi. Periksa apakah server AS2 mitra tersedia di alamat IP yang dikonfigurasi.

Kode	Kesalahan	Deskripsi dan resolusi
UNABLE_TO_RESOLVE_HOSTNAME	Tidak dapat menyelesaikan nama host <i>hostname</i> .	Server Transfer Family tidak dapat menyelesaikan nama host mitra dengan menggunakan server DNS publik. Periksa apakah host yang dikonfigurasi terdaftar dan catatan DNS memiliki waktu untuk mempublikasikan.
VERIFICATION_FAILED	Verifikasi tanda tangan gagal untuk pesan AS2 <i>message-ID</i> atau kode MIC tidak cocok.	Periksa apakah sertifikat penandatanganan pengirim cocok dengan sertifikat penandatanganan untuk profil jarak jauh. Periksa juga apakah algoritma MIC kompatibel dengan AWS Transfer Family.

Kode	Kesalahan	Deskripsi dan resolusi
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- Tidak ada tanda tangan pesan yang cocok dengan sertifikat publik yang dapat ditemukan di profil:<i>partner-profile-ID</i> . - Tidak bisa mendapatkan sertifikat untuk profil yang tidak ada: <i>partner-profile-ID</i> - Tidak ada sertifikat yang valid ditemukan di profil:<i>partner-profile-ID</i> .	AWS Transfer Family sedang mencoba memverifikasi tanda tangan untuk pesan yang diterima, tetapi tidak ada sertifikat penandatanganan yang cocok ditemukan untuk profil mitra. Opsi resolusi: - Pastikan bahwa profil mitra memiliki sertifikat penandatanganan terlampir. - Pastikan sertifikat saat ini aktif. - Pastikan bahwa sertifikat adalah sertifikat penandatanganan yang benar untuk mitra.

Pemantauan kedaluwarsa sertifikat

AWS Transfer Family secara otomatis memantau tanggal kedaluwarsa sertifikat AS2 dan menerbitkan metrik CloudWatch Amazon untuk membantu Anda melacak kapan sertifikat mendekati kedaluwarsa. Ini memungkinkan Anda untuk secara proaktif mengelola perpanjangan sertifikat dan menghindari gangguan layanan.

DaysUntilExpiry metrik

Saat Anda mengimpor sertifikat untuk penggunaan AS2, Transfer Family secara otomatis membuat CloudWatch metrik yang dipanggil `DaysUntilExpiry`. Metrik ini melacak jumlah hari yang tersisa hingga sertifikat kedaluwarsa berdasarkan yang `InactiveDate` Anda tentukan saat mengimpor sertifikat.

Detail metrik:

- Nama metrik: `DaysUntilExpiry`
- Ruang nama: `AWS/Transfer`
- Dimensi: `CertificateId` (selalu ada), `Description` (jika disediakan selama impor sertifikat)
- Unit: Hitung (hari)
- Frekuensi: Diterbitkan setiap hari

Important

Diperlukan waktu hingga satu hari penuh setelah mengimpor sertifikat Transfer Family untuk memancarkan metrik ini ke akun Anda.

Nilai metrik berkurang satu per hari saat sertifikat mendekati tanggal tidak aktifnya. Misalnya, jika sertifikat memiliki 30 hari hingga kedaluwarsa, metrik akan menunjukkan 30, lalu 29 hari berikutnya, dan seterusnya.

Praktik terbaik untuk pemantauan sertifikat

Ikuti praktik terbaik ini saat menyiapkan pemantauan kedaluwarsa sertifikat:

- Tetapkan beberapa ambang peringatan: Buat alarm untuk periode waktu yang berbeda (misalnya, 30 hari, 14 hari, dan 7 hari sebelum kedaluwarsa) untuk memberikan waktu yang memadai untuk perpanjangan sertifikat.
- Gunakan statistik yang sesuai: Gunakan `Maximum` statistik saat membuat alarm untuk memastikan Anda menangkap nilai metrik terbaru.
- Konfigurasi tindakan alarm yang tepat: Siapkan notifikasi untuk memberi tahu anggota tim yang sesuai yang dapat memperbarui sertifikat.
- Uji peringatan Anda: Uji sistem notifikasi Anda secara teratur untuk memastikan peringatan dikirimkan dengan benar.
- Dokumentasikan proses Anda: Menjaga dokumentasi tentang proses perpanjangan sertifikat Anda dan siapa yang bertanggung jawab atas sertifikat yang berbeda.

Contoh konfigurasi alarm

Berikut adalah beberapa contoh konfigurasi alarm untuk skenario notifikasi yang berbeda:

Peringatan kedaluwarsa 30 hari

Buat alarm yang memicu ketika sertifikat memiliki 30 hari atau kurang hingga kedaluwarsa:

- Metrik: DaysUntilExpiry
- Statistik: Maksimum
- Periode: 1 hari
- Ambang: 30
- Perbandingan: Kurang dari atau sama dengan ambang
- Perlakuan data yang hilang: Perlakukan data yang hilang sebagai hal yang baik (tidak melanggar)

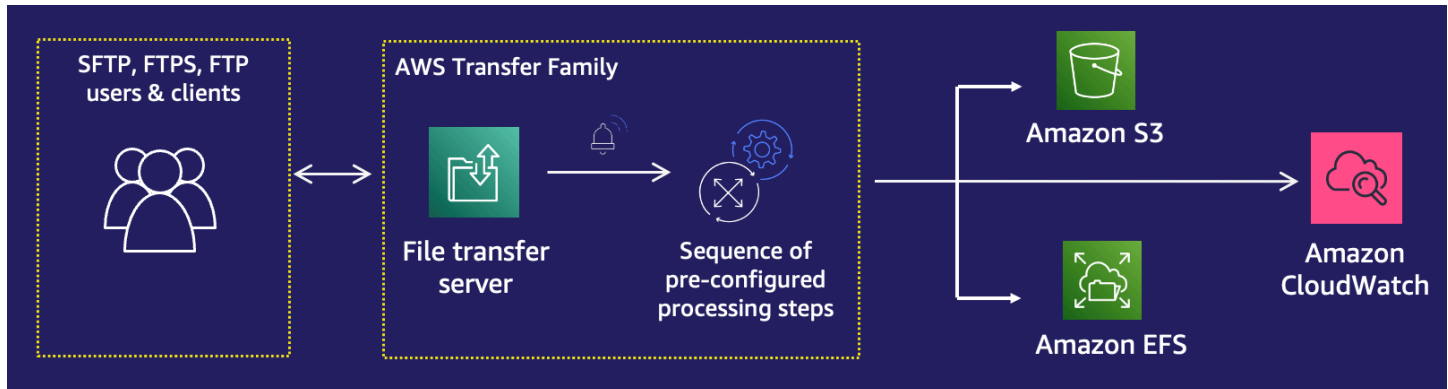
Peringatan kedaluwarsa 7 hari kritis

Buat alarm kritis yang memicu ketika sertifikat memiliki 7 hari atau kurang hingga kedaluwarsa:

- Metrik: DaysUntilExpiry
- Statistik: Maksimum
- Periode: 1 hari
- Ambang: 7
- Perbandingan: Kurang dari atau sama dengan ambang
- Perlakuan data yang hilang: Perlakukan data yang hilang sebagai hal yang baik (tidak melanggar)

AWS Transfer Family alur kerja terkelola

AWS Transfer Family mendukung alur kerja terkelola untuk pemrosesan file. Dengan alur kerja terkelola, Anda dapat memulai alur kerja setelah file ditransfer melalui SFTP, FTPS, atau FTP. Dengan menggunakan fitur ini, Anda dapat dengan aman dan hemat biaya memenuhi persyaratan kepatuhan Anda untuk pertukaran file bisnis-ke-bisnis (B2B) dengan mengoordinasikan semua langkah yang diperlukan untuk pemrosesan file. Selain itu, Anda mendapat manfaat dari audit dan visibilitas ujung ke ujung.



Dengan mengatur tugas pemrosesan file, alur kerja terkelola membantu Anda memproses data sebelum dikonsumsi oleh aplikasi hilir. Tugas pemrosesan file tersebut mungkin termasuk:

- Memindahkan file ke folder khusus pengguna.
- Mendekripsi file sebagai bagian dari alur kerja.
- Menandai file.
- Melakukan pemrosesan kustom dengan membuat dan melampirkan AWS Lambda fungsi ke alur kerja.
- Mengirim pemberitahuan ketika file telah berhasil ditransfer. (Untuk posting blog yang merinci kasus penggunaan ini, lihat [Menyesuaikan pemberitahuan pengiriman file menggunakan alur kerja AWS Transfer Family terkelola](#).)

Untuk dengan cepat mereplikasi dan menstandarisasi tugas pemrosesan file pasca-unggah umum yang mencakup beberapa unit bisnis di organisasi Anda, Anda dapat menerapkan alur kerja dengan menggunakan infrastruktur sebagai kode (IaC). Anda dapat menentukan alur kerja terkelola yang akan dimulai pada file yang diunggah secara penuh. Anda juga dapat menentukan alur kerja terkelola yang berbeda untuk dimulai pada file yang hanya diunggah sebagian karena pemutusan sesi prematur. Built-in Penanganan pengecualian membantu Anda bereaksi dengan cepat terhadap hasil

pemrosesan file, sambil menawarkan Anda kontrol atas cara menangani kegagalan. Selain itu, setiap langkah alur kerja menghasilkan log terperinci, yang dapat Anda audit untuk melacak garis keturunan data.

Untuk memulai, lakukan tugas-tugas berikut:

1. Siapkan alur kerja Anda agar berisi tindakan pra-pemrosesan, seperti menyalin, menandai, dan langkah-langkah lain berdasarkan kebutuhan Anda. Lihat [Buat alur kerja](#) untuk detail.
2. Konfigurasi peran eksekusi, yang digunakan Transfer Family untuk menjalankan alur kerja. Lihat [Kebijakan IAM untuk alur kerja](#) untuk detail.
3. Petakan alur kerja ke server, sehingga pada saat kedatangan file, tindakan yang ditentukan dalam alur kerja ini dievaluasi dan dimulai secara real time. Lihat [Konfigurasi dan jalankan alur kerja](#) untuk detail.

Informasi terkait

- Untuk memantau eksekusi alur kerja Anda, lihat. [Menggunakan CloudWatch metrik untuk server Transfer Family](#)
- Untuk detail log eksekusi dan informasi pemecahan masalah, lihat. [Memecahkan masalah kesalahan terkait alur kerja menggunakan Amazon CloudWatch](#)
- Transfer Family menyediakan posting blog dan lokakarya yang memandu Anda membangun solusi transfer file. Solusi ini memanfaatkan AWS Transfer Family SFTP/FTPS endpoint terkelola dan Amazon Cognito dan DynamoDB untuk manajemen pengguna.

Posting blog tersedia di [Menggunakan Amazon Cognito sebagai penyedia identitas dengan AWS Transfer Family dan Amazon S3](#). Anda dapat melihat detail untuk lokakarya [di sini](#).

- Lihat [Alur Kerja AWS Transfer Family Terkelola](#) untuk pengenalan singkat tentang alur kerja Transfer Family.
- [Lokakarya berikut menyediakan laboratorium langsung untuk membangun alur kerja yang sepenuhnya otomatis dan digerakkan oleh peristiwa yang melibatkan transfer file ke atau dari server SFTP eksternal ke Amazon S3, dan pra dan pasca pemrosesan umum dari file-file tersebut: lokakarya MFT. Event-driven](#)

Video ini memberikan jalan-jalan melalui lokakarya ini.

Topik

- [Buat alur kerja](#)
- [Gunakan langkah-langkah yang telah ditentukan](#)
- [Gunakan langkah-langkah pemrosesan file khusus](#)
- [Kebijakan IAM untuk alur kerja](#)
- [Penanganan pengecualian untuk alur kerja](#)
- [Pantau eksekusi alur kerja](#)
- [Buat alur kerja dari template](#)
- [Menghapus alur kerja dari server Transfer Family](#)
- [Pembatasan dan batasan alur kerja yang dikelola](#)

Untuk bantuan selengkapnya untuk memulai alur kerja terkelola, lihat sumber daya berikut:

- AWS Transfer Family video demo [alur kerja terkelola](#)
- [Membangun platform transfer file cloud-native menggunakan AWS Transfer Family alur kerja posting blog](#)

Buat alur kerja

Anda dapat membuat alur kerja terkelola menggunakan Konsol Manajemen AWS, seperti yang dijelaskan dalam topik ini. Untuk membuat proses pembuatan alur kerja semudah mungkin, panel bantuan kontekstual tersedia untuk sebagian besar bagian di konsol.

Alur kerja memiliki dua jenis langkah:

- Langkah nominal — Langkah nominal adalah langkah pemrosesan file yang ingin Anda terapkan ke file yang masuk. Jika Anda memilih lebih dari satu langkah nominal, setiap langkah diproses dalam urutan linier.
- Exception-handling langkah-langkah - Penangan pengecualian adalah langkah-langkah pemrosesan file yang AWS Transfer Family dijalankan jika ada langkah nominal yang gagal atau mengakibatkan kesalahan validasi.

Buat alur kerja

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Alur kerja.

3. Pada halaman Alur kerja, pilih Buat alur kerja.
4. Pada halaman Buat alur kerja, masukkan deskripsi. Deskripsi ini muncul di halaman Alur Kerja.
5. Di bagian Langkah nominal, pilih Tambah langkah. Tambahkan satu atau lebih langkah.
 - a. Pilih jenis langkah dari opsi yang tersedia. Untuk informasi selengkapnya tentang berbagai jenis langkah, lihat [the section called “Gunakan langkah-langkah yang telah ditentukan”](#).
 - b. Pilih Berikutnya, lalu konfigurasi parameter untuk langkah tersebut.
 - c. Pilih Berikutnya, lalu tinjau detail langkahnya.
 - d. Pilih Buat langkah untuk menambahkan langkah dan melanjutkan.
 - e. Lanjutkan menambahkan langkah-langkah sesuai kebutuhan. Jumlah maksimum langkah dalam alur kerja adalah 8.
 - f. Setelah Anda menambahkan semua langkah nominal yang diperlukan, gulir ke bawah ke penanganan Exception - bagian opsional, dan pilih Tambah langkah.

 Note

Agar Anda diberitahu tentang kegagalan secara real time, kami sarankan Anda menyiapkan penanganan pengecualian dan langkah-langkah untuk mengeksekusi ketika alur kerja Anda gagal.

6. Untuk mengonfigurasi penanganan pengecualian, tambahkan langkah dengan cara yang sama seperti yang dijelaskan sebelumnya. Jika file menyebabkan langkah apa pun untuk melempar pengecualian, penanganan pengecualian Anda dipanggil satu per satu.
7. (Opsional) Gulir ke bawah ke bagian Tag, dan tambahkan tag untuk alur kerja Anda.
8. Tinjau konfigurasi, dan pilih Buat alur kerja.

 Important

Setelah membuat alur kerja, Anda tidak dapat mengeditnya, jadi pastikan untuk meninjau konfigurasi dengan cermat.

Konfigurasi dan jalankan alur kerja

Sebelum Anda dapat menjalankan alur kerja, Anda harus mengaitkannya dengan server Transfer Family.

Untuk mengonfigurasi Transfer Family untuk menjalankan alur kerja pada file yang diunggah

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server.
 - Untuk menambahkan alur kerja ke server yang ada, pilih server yang ingin Anda gunakan untuk alur kerja Anda.
 - Atau, buat server baru dan tambahkan alur kerja ke dalamnya. Untuk informasi selengkapnya, lihat [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#).
3. Pada halaman detail untuk server, gulir ke bawah ke bagian Detail tambahan, lalu pilih Edit.

 Note

Secara default, server tidak memiliki alur kerja terkait. Anda menggunakan bagian Detail tambahan untuk mengaitkan alur kerja dengan server yang dipilih.

4. Pada halaman Edit detail tambahan, di bagian Alur kerja terkelola, pilih alur kerja yang akan dijalankan di semua unggahan.

 Note

Jika Anda belum memiliki alur kerja, pilih Buat Alur Kerja baru untuk membuatnya.

- a. Pilih ID alur kerja yang akan digunakan.
- b. Pilih peran eksekusi. Ini adalah peran yang diasumsikan Transfer Family saat menjalankan langkah-langkah alur kerja. Untuk informasi selengkapnya, lihat [Kebijakan IAM untuk alur kerja](#). Pilih Simpan.

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-

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-

Create a new Workflow

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

Note

Jika Anda tidak lagi ingin alur kerja dikaitkan dengan server, Anda dapat menghapus asosiasi tersebut. Lihat perinciannya di [Menghapus alur kerja dari server Transfer Family](#).

Untuk menjalankan alur kerja

Untuk menjalankan alur kerja, Anda mengunggah file ke server Transfer Family yang dikonfigurasi dengan alur kerja terkait.

Note

Setiap kali Anda menghapus alur kerja dari server dan menggantinya dengan yang baru, atau memperbarui konfigurasi server (yang memengaruhi peran eksekusi alur kerja), Anda harus menunggu sekitar 10 menit sebelum menjalankan alur kerja baru. Server Transfer Family menyimpan cache detail alur kerja, dan dibutuhkan waktu 10 menit bagi server untuk menyegarkan cache-nya.

Selain itu, Anda harus keluar dari sesi SFTP aktif apa pun, dan kemudian masuk kembali setelah masa tunggu 10 menit untuk melihat perubahannya.

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

Setelah file Anda diunggah, tindakan yang ditentukan dilakukan pada file Anda. Misalnya, jika alur kerja Anda berisi langkah penyalinan, file tersebut disalin ke lokasi yang Anda tentukan di langkah itu. Anda dapat menggunakan Amazon CloudWatch Logs untuk melacak langkah-langkah yang dijalankan dan status eksekusi mereka.

Lihat detail alur kerja

Anda dapat melihat detail tentang alur kerja yang dibuat sebelumnya atau eksekusi alur kerja. Untuk melihat detail ini, Anda dapat menggunakan konsol atau AWS Command Line Interface (AWS CLI).

Console

Lihat detail alur kerja

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Alur kerja.
3. Pada halaman Alur Kerja, pilih alur kerja.

Halaman detail alur kerja terbuka.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with options: Servers, Connectors, AS2 Trading Partners (Certificates, Profiles), Workflows (selected), Feature Spotlight, What's New, Documentation, About servers, and About SFTP connectors. The main content area displays details for a specific workflow (ID: w-1234567890abcdef0). It includes a 'Description' section with Name 'Test my workflow' and Workflow description 'Test workflow A'. Below is a 'Nominal steps (1)' table with one step: Number 1, Description 'tag_step', Type 'TAG', and Configuration 'Details'. Next is an 'Exception handlers (1)' table with one handler: Number 1, Description 'delete_if_exception', Type 'DELETE', and Configuration 'Details'. The 'In-flight executions (0)' section shows a search bar and a table with columns: Execution ID, Status, Input filename, Server ID, and Username. It displays 'No executions' and 'No executions to display'. At the bottom is a 'Tags (1)' section with a 'Manage tags' button and a note about using tags to organize workflows.

CLI

Untuk melihat detail alur kerja, gunakan perintah `describe-workflow` CLI, seperti yang ditunjukkan pada contoh berikut. Ganti ID alur kerja `w-1234567890abcdef0` dengan nilai Anda sendiri. Untuk informasi selengkapnya, lihat [menjelaskan alur kerja di Referensi Perintah.AWS CLI](#)

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
  "Workflow": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/w-1234567890abcdef0",
    "WorkflowId": "w-1234567890abcdef0",
    "Name": "Copy file to shared_files",
    "Steps": [
      {
```

```

        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "amzn-s3-demo-bucket",
              "Key": "home/shared_files/"
            }
          }
        }
      ],
      "OnException": {}
    }
  }
}

```

Jika alur kerja Anda dibuat sebagai bagian dari AWS CloudFormation tumpukan, Anda dapat mengelola alur kerja menggunakan CloudFormation console () <https://console.aws.amazon.com/cloudformation>.

Transfer Family > Workflows > w-...

W-... Delete

Info This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name	Workflow description
Stack-managed	Workflow for blogpost

Nominal steps (4) [Info](#)

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

Gunakan langkah-langkah yang telah ditentukan

Saat membuat alur kerja, Anda dapat memilih untuk menambahkan salah satu langkah yang telah ditentukan berikut yang dibahas dalam topik ini. Anda juga dapat memilih untuk menambahkan langkah-langkah pemrosesan file kustom Anda sendiri. Untuk informasi selengkapnya, lihat [the section called “Gunakan langkah-langkah pemrosesan file khusus”](#).

Topik

- [Salin berkas](#)
- [Dekripsi file](#)
- [Berkas tag](#)
- [Hapus berkas](#)
- [Variabel bernama untuk alur kerja](#)
- [Contoh tag dan hapus alur kerja](#)

Salin berkas

Langkah salin file membuat salinan file yang diunggah di lokasi Amazon S3 baru. Saat ini, Anda dapat menggunakan langkah salin file hanya dengan Amazon S3.

Langkah copy file berikut menyalin file ke dalam test folder di *amzn-s3-demo-destination-bucket*.

Jika langkah salin file bukan langkah pertama alur kerja Anda, Anda dapat menentukan lokasi File. Dengan menentukan lokasi file, Anda dapat menyalin file yang digunakan pada langkah sebelumnya atau file asli yang diunggah. Anda dapat menggunakan fitur ini untuk membuat beberapa salinan dari file asli sambil menjaga file sumber tetap utuh untuk arsip file dan penyimpanan catatan. Sebagai contoh, lihat [Contoh tag dan hapus alur kerja](#).

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

Berikan ember dan detail kunci

Anda harus memberikan nama bucket dan kunci untuk tujuan langkah salin file. Kuncinya bisa berupa nama jalur atau nama file. Apakah kunci diperlakukan sebagai nama jalur atau nama file ditentukan oleh apakah Anda mengakhiri kunci dengan karakter garis miring (/) maju.

Jika karakter terakhir adalah /, file Anda disalin ke folder, dan namanya tidak berubah. Jika karakter terakhir adalah alfanumerik, file yang Anda unggah diubah namanya menjadi nilai kunci. Dalam hal

ini, jika file dengan nama itu sudah ada, perilaku tergantung pada pengaturan untuk bidang Timpa yang ada.

- Jika Timpa yang ada dipilih, file yang ada diganti dengan file yang sedang diproses.
- Jika Timpa yang ada tidak dipilih, tidak ada yang terjadi, dan pemrosesan alur kerja berhenti.

Tip

Jika penulisan bersamaan dijalankan pada jalur file yang sama, hal itu dapat mengakibatkan perilaku yang tidak terduga saat menimpa file.

Misalnya, jika nilai kunci Anda adalah `test/`, file yang Anda unggah akan disalin ke folder. `test` Jika nilai kunci Anda `test/today`, (dan Timpa yang ada dipilih) setiap file yang Anda unggah disalin ke file bernama `today` di `test` folder, dan setiap file berikutnya menimpa yang sebelumnya.

Note

Amazon S3 mendukung bucket dan objek, dan tidak memiliki hierarki. Namun, Anda dapat menggunakan awalan dan pembatas dalam nama kunci objek untuk menyiratkan hierarki dan mengatur data Anda dengan cara yang mirip dengan folder.

Gunakan variabel bernama dalam langkah copy file

Dalam langkah salin file, Anda dapat menggunakan variabel untuk menyalin file Anda secara dinamis ke folder khusus pengguna. Saat ini, Anda dapat menggunakan `${transfer:UserName}` atau `${transfer:UploadDate}` sebagai variabel untuk menyalin file ke lokasi tujuan untuk pengguna tertentu yang mengunggah file, atau berdasarkan tanggal saat ini.

Dalam contoh berikut, jika pengguna `richard-roe` mengunggah file, itu akan disalin ke folder `amzn-s3-demo-destination-bucket/richard-roe/processed/`. Jika pengguna `mary-major` mengunggah file, itu akan disalin ke folder. `amzn-s3-demo-destination-bucket/mary-major/processed/`

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

Demikian pula, Anda dapat menggunakan `${transfer:UploadDate}` sebagai variabel untuk menyalin file ke lokasi tujuan yang dinamai untuk tanggal saat ini. Dalam contoh berikut, jika Anda menetapkan tujuan `${transfer:UploadDate}/processed` pada 1 Februari 2022, file yang diunggah akan disalin ke folder `amzn-s3-demo-destination-bucket/2022-02-01/processed/`.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

Anda juga dapat menggunakan kedua variabel ini bersama-sama, menggabungkan fungsionalitasnya. Misalnya, Anda dapat mengatur awalan key Destination ke **folder/**`${transfer:UserName}/${transfer:UploadDate}/`, yang akan membuat folder bersarang, misalnya. `folder/marymajor/2023-01-05/`

Izin IAM untuk langkah penyalinan

Agar langkah penyalinan berhasil, pastikan peran eksekusi untuk alur kerja Anda berisi izin berikut.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
```

```
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

s3:ListBucketIzin hanya diperlukan jika Anda tidak memilih Timpa yang sudah ada. Izin ini memeriksa bucket Anda untuk melihat apakah file dengan nama yang sama sudah ada. Jika Anda telah memilih Timpa yang ada, alur kerja tidak perlu memeriksa file, dan hanya bisa menuliskannya.

Jika file Amazon S3 Anda memiliki tag, Anda perlu menambahkan satu atau dua izin ke kebijakan IAM Anda.

- Tambahkan s3:GetObjectTagging file Amazon S3 yang tidak berversi.
- Tambahkan s3:GetObjectVersionTagging untuk file Amazon S3 yang berversi.

Dekripsi file

Blog AWS penyimpanan memiliki posting yang menjelaskan cara mendekripsi file tanpa menulis kode apa pun menggunakan alur kerja Transfer Family Managed, [Enkripsi dan dekripsi file dengan PGP dan](#). AWS Transfer Family

Algoritma enkripsi simetris yang didukung

Untuk dekripsi PGP, Transfer Family mendukung algoritma enkripsi simetris yang digunakan untuk mengenkripsi data file aktual dalam file PGP.

- Untuk informasi rinci tentang algoritme enkripsi simetris yang didukung, lihat. [Algoritma enkripsi simetris PGP](#)
- Untuk informasi tentang algoritma key pair PGP yang digunakan dengan algoritma simetris ini, lihat. [Algoritma key pair PGP](#)

Gunakan dekripsi PGP dalam alur kerja Anda

Transfer Family memiliki dukungan bawaan untuk dekripsi Pretty Good Privacy (PGP). Anda dapat menggunakan dekripsi PGP pada file yang diunggah melalui SFTP, FTPS, atau FTP ke Amazon Simple Storage Service (Amazon S3) atau Amazon Elastic File System (Amazon EFS).

Untuk menggunakan dekripsi PGP, Anda harus membuat dan menyimpan kunci pribadi PGP yang akan digunakan untuk dekripsi file Anda. Pengguna Anda kemudian dapat mengenkripsi file dengan menggunakan kunci enkripsi PGP yang sesuai sebelum mengunggah file ke server Transfer Family Anda. Setelah Anda menerima file terenkripsi, Anda dapat mendekripsi file-file tersebut dalam alur kerja Anda. Untuk tutorial detail, lihat [Menyiapkan alur kerja terkelola untuk mendekripsi file](#).

Untuk informasi tentang algoritma dan rekomendasi PGP yang didukung, lihat [Enkripsi PGP dan algoritma dekripsi](#)

Untuk menggunakan dekripsi PGP dalam alur kerja Anda

1. Identifikasi server Transfer Family untuk meng-host alur kerja Anda, atau buat yang baru. Anda harus memiliki ID server sebelum Anda dapat menyimpan kunci PGP Anda AWS Secrets Manager dengan nama rahasia yang benar.
2. Simpan kunci PGP Anda di AWS Secrets Manager bawah nama rahasia yang diperlukan. Lihat perinciannya di [Kelola kunci PGP](#). Alur kerja dapat secara otomatis menemukan kunci PGP yang benar untuk digunakan untuk dekripsi berdasarkan nama rahasia di Secrets Manager.

Note

Ketika Anda menyimpan rahasia di Secrets Manager, Anda Akun AWS dikenakan biaya. Untuk informasi tentang harga, lihat [AWS Secrets Manager Harga](#).

3. Enkripsi file dengan menggunakan key pair PGP Anda. (Untuk daftar klien yang didukung, lihat [Klien PGP yang didukung](#).) Jika Anda menggunakan baris perintah, jalankan perintah berikut. Untuk menggunakan perintah ini, ganti *username@example.com* dengan alamat email yang Anda gunakan untuk membuat key pair PGP. Ganti *testfile.txt* dengan nama file yang ingin Anda enkripsi.

```
gpg -e -r username@example.com testfile.txt
```

 Important

Saat mengenkripsi file untuk digunakan dengan AWS Transfer Family alur kerja, selalu pastikan Anda menentukan penerima non-anonim menggunakan parameter.

- ☒ Enkripsi anonim (tanpa menentukan penerima) dapat menyebabkan kegagalan dekripsi dalam alur kerja karena sistem tidak akan dapat mengidentifikasi kunci mana yang akan digunakan untuk dekripsi. Informasi debugging untuk masalah ini tersedia di [Memecahkan masalah enkripsi penerima anonim](#).

4. Unggah file terenkripsi ke server Transfer Family Anda.
5. Konfigurasi langkah dekripsi dalam alur kerja Anda. Untuk informasi selengkapnya, lihat [Tambahkan langkah dekripsi](#).

Tambahkan langkah dekripsi

Langkah dekripsi mendekripsi file terenkripsi yang diunggah ke Amazon S3 atau Amazon EFS sebagai bagian dari alur kerja Anda. Untuk detail tentang mengonfigurasi dekripsi, lihat [Gunakan dekripsi PGP dalam alur kerja Anda](#)

Saat Anda membuat langkah dekripsi untuk alur kerja, Anda harus menentukan tujuan untuk file yang didekripsi. Anda juga harus memilih apakah akan menimpa file yang ada jika file sudah ada di lokasi tujuan. Anda dapat memantau hasil alur kerja dekripsi dan mendapatkan log audit untuk setiap file secara real time menggunakan Amazon Logs. CloudWatch

Setelah Anda memilih jenis file Dekripsi untuk langkah Anda, halaman Konfigurasi parameter akan muncul. Isi nilai untuk bagian Konfigurasi parameter dekripsi PGP.

Opsi yang tersedia adalah sebagai berikut:

- Nama langkah - Masukkan nama deskriptif untuk langkah tersebut.
- Lokasi file — Dengan menentukan lokasi file, Anda dapat mendekripsi file yang digunakan pada langkah sebelumnya atau file asli yang diunggah.

 Note

Parameter ini tidak tersedia jika langkah ini adalah langkah pertama dari alur kerja.

- Tujuan untuk file yang didekripsi — Pilih bucket Amazon S3 atau sistem file Amazon EFS sebagai tujuan untuk file yang didekripsi.
- Jika memilih Amazon S3, Anda harus memberikan nama bucket tujuan dan awalan key tujuan. Untuk memparameterisasi awalan key tujuan dengan nama pengguna, **`${transfer:UserName}`** masukkan untuk Destination key prefix. Demikian pula, untuk parameterisasi awalan key tujuan dengan tanggal upload, **`${Transfer:UploadDate}`** masukkan untuk Destination key prefix.
- Jika Anda memilih Amazon EFS, Anda harus menyediakan sistem dan jalur file tujuan.

 Note

Opsi penyimpanan yang Anda pilih di sini harus sesuai dengan sistem penyimpanan yang digunakan oleh server Transfer Family yang terkait dengan alur kerja ini. Jika tidak, Anda akan menerima kesalahan saat mencoba menjalankan alur kerja ini.

- Timpa yang ada — Jika Anda mengunggah file, dan file dengan nama file yang sama sudah ada di tujuan, perilaku tergantung pada pengaturan untuk parameter ini:
 - Jika Timpa yang ada dipilih, file yang ada diganti dengan file yang sedang diproses.
 - Jika Timpa yang ada tidak dipilih, tidak ada yang terjadi, dan pemrosesan alur kerja berhenti.

 Tip

Jika penulisan bersamaan dijalankan pada jalur file yang sama, hal itu dapat mengakibatkan perilaku yang tidak terduga saat menimpa file.

Tangkapan layar berikut menunjukkan contoh opsi yang mungkin Anda pilih untuk langkah dekripsi file Anda.

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.

Izin IAM untuk langkah dekripsi

Agar langkah dekripsi berhasil, pastikan peran eksekusi untuk alur kerja Anda berisi izin berikut.

Dekripsi file

480

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
  ],
  "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

s3:ListBucketIzin hanya diperlukan jika Anda tidak memilih Timpa yang sudah ada. Izin ini memeriksa bucket Anda untuk melihat apakah file dengan nama yang sama sudah ada. Jika Anda telah memilih Timpa yang ada, alur kerja tidak perlu memeriksa file, dan hanya bisa menuliskannya.

Jika file Amazon S3 Anda memiliki tag, Anda perlu menambahkan satu atau dua izin ke kebijakan IAM Anda.

- Tambahkan s3:GetObjectTagging file Amazon S3 yang tidak berversi.
- Tambahkan s3:GetObjectVersionTagging untuk file Amazon S3 yang berversi.

Berkas tag

Untuk menandai file yang masuk untuk pemrosesan hilir lebih lanjut, gunakan langkah tag. Masukkan nilai tag yang ingin Anda tetapkan ke file yang masuk. Saat ini, operasi tag hanya didukung jika Anda menggunakan Amazon S3 untuk penyimpanan server Transfer Family Anda.

Berikut contoh langkah tag menetapkan `scan_outcome` dan `clean` sebagai kunci tag dan nilai, masing-masing.

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

Agar langkah tag berhasil, pastikan peran eksekusi untuk alur kerja Anda berisi izin berikut.

```
{
  "Sid": "Tag",
  "Effect": "Allow",
  "Action": [
    "s3:PutObjectTagging",
    "s3:PutObjectVersionTagging"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
}
```

}

Note

Jika alur kerja Anda berisi langkah tag yang berjalan sebelum langkah salin atau dekripsi, Anda perlu menambahkan satu atau dua izin ke kebijakan IAM Anda.

- Tambahkan `s3:GetObjectTagging` file Amazon S3 yang tidak berversi.
- Tambahkan `s3:GetObjectVersionTagging` untuk file Amazon S3 yang berversi.

Hapus berkas

Untuk menghapus file yang diproses dari langkah alur kerja sebelumnya atau untuk menghapus file yang diunggah semula, gunakan langkah menghapus file.

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

Agar langkah penghapusan berhasil, pastikan peran eksekusi untuk alur kerja Anda berisi izin berikut.

```
{
    "Sid": "Delete",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/"
}
```

```
}
```

Variabel bernama untuk alur kerja

Untuk langkah salin dan dekripsi, Anda dapat menggunakan variabel untuk melakukan tindakan secara dinamis. Saat ini, AWS Transfer Family mendukung variabel bernama berikut.

- Gunakan `${transfer:UserName}` untuk menyalin atau mendekripsi file ke tujuan berdasarkan pengguna yang mengunggah file.
- Gunakan `${transfer:UploadDate}` untuk menyalin atau mendekripsi file ke lokasi tujuan berdasarkan tanggal saat ini.

Contoh tag dan hapus alur kerja

Contoh berikut menggambarkan alur kerja yang menandai file masuk yang perlu diproses oleh aplikasi hilir, seperti platform analisis data. Setelah menandai file yang masuk, alur kerja kemudian menghapus file yang awalnya diunggah untuk menghemat biaya penyimpanan.

Console

Contoh tag dan pindahkan alur kerja

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Alur kerja.
3. Pada halaman Alur kerja, pilih Buat alur kerja.
4. Pada halaman Buat alur kerja, masukkan deskripsi. Deskripsi ini muncul di halaman Alur Kerja.
5. Tambahkan langkah pertama (salin).
 - a. Di bagian Langkah nominal, pilih Tambah langkah.
 - b. Pilih Salin file, lalu pilih Berikutnya.
 - c. Masukkan nama langkah, lalu pilih bucket tujuan dan key prefix.

The screenshot shows the AWS Transfer Family console interface. On the left, there is a sidebar with three steps: 'Step 1 Choose step type', 'Step 2 Configure parameters' (which is the active step), and 'Step 3 Review and create'. The main area is titled 'Configure parameters' and contains a section 'Configure copy parameters'. This section includes three input fields: 'Step name' with the value 'copy-step-first-step', 'Destination bucket name' with a dropdown menu showing 'example-bucket', and 'Destination key prefix' with the value 'test/'. Below these fields is a checkbox labeled 'Overwrite existing' which is currently unchecked. A small text note explains that the prefix should end with a slash and can be parametrized using variables like \${transfer:UserName} or \${transfer:UploadDate}.

- d. Pilih Berikutnya, lalu tinjau detail langkahnya.
 - e. Pilih Buat langkah untuk menambahkan langkah dan melanjutkan.
6. Tambahkan langkah kedua (tag).
- a. Di bagian Langkah nominal, pilih Tambah langkah.
 - b. Pilih File Tag, lalu pilih Berikutnya.
 - c. Masukkan nama langkah.
 - d. Untuk lokasi File, pilih Tag file yang dibuat dari langkah sebelumnya.
 - e. Masukkan Kunci dan Nilai.

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. Pilih Berikutnya, lalu tinjau detail langkahnya.
 - g. Pilih Buat langkah untuk menambahkan langkah dan melanjutkan.
7. Tambahkan langkah ketiga (hapus).
- a. Di bagian Langkah nominal, pilih Tambah langkah.
 - b. Pilih Hapus file, lalu pilih Berikutnya.

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. Masukkan nama langkah.

- d. Untuk lokasi File, pilih Hapus file sumber asli.
 - e. Pilih Berikutnya, lalu tinjau detail langkahnya.
 - f. Pilih Buat langkah untuk menambahkan langkah dan melanjutkan.
8. Tinjau konfigurasi alur kerja, lalu pilih Buat alur kerja.

CLI

Contoh tag dan pindahkan alur kerja

1. Simpan kode berikut ke dalam file; misalnya, `tagAndMoveWorkflow.json`. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```

```

        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
]

```

Langkah pertama menyalin file yang diunggah ke lokasi Amazon S3 baru. Langkah kedua menambahkan tag (pasangan nilai kunci) ke file (`previous.file`) yang disalin ke lokasi baru. Dan, akhirnya, langkah ketiga menghapus file asli (`original.file`).

2. Buat alur kerja dari file yang disimpan. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID
```

Contoh:

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1
```

Note

Untuk detail selengkapnya tentang menggunakan file untuk memuat parameter, lihat [Cara memuat parameter dari file](#).

3. Perbarui server yang ada.

Note

Langkah ini mengasumsikan Anda sudah memiliki server Transfer Family dan Anda ingin mengaitkan alur kerja dengannya. Jika belum, lihat [Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP](#). Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
aws transfer update-server --server-id server-ID --region region-ID
```

```
--workflow-details '{"OnUpload":[{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'
```

Contoh:

```
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"}]}'
```

Gunakan langkah-langkah pemrosesan file khusus

Dengan menggunakan langkah pemrosesan file kustom, Anda dapat menggunakan logika pemrosesan file Anda Sendiri. AWS Lambda Setelah kedatangan file, server Transfer Family memanggil fungsi Lambda yang berisi logika pemrosesan file khusus, seperti mengenkripsi file, memindai malware, atau memeriksa jenis file yang salah. Dalam contoh berikut, AWS Lambda fungsi target digunakan untuk memproses file output dari langkah sebelumnya.

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

Untuk contoh fungsi Lambda, lihat. [Contoh fungsi Lambda untuk langkah alur kerja khusus](#). Misalnya peristiwa (termasuk lokasi untuk file yang diteruskan ke Lambda), lihat. [Contoh peristiwa dikirim ke AWS Lambda saat file upload](#)

Dengan langkah alur kerja khusus, Anda harus mengonfigurasi fungsi Lambda untuk memanggil operasi API [SendWorkflowStepState](#). `SendWorkflowStepState` memberitahukan eksekusi alur kerja bahwa langkah telah selesai dengan status sukses atau kegagalan. Status operasi `SendWorkflowStepState` API memanggil langkah penanganan pengecualian atau langkah nominal dalam urutan linier, berdasarkan hasil fungsi Lambda.

Jika fungsi Lambda gagal atau habis waktu, langkahnya gagal, dan Anda lihat `StepErrored` di log Anda CloudWatch. Jika fungsi Lambda adalah bagian dari langkah nominal dan fungsi merespons `SendWorkflowStepState` dengan `Status="FAILURE"` atau waktu habis, aliran berlanjut dengan langkah-langkah penanganan pengecualian. Dalam hal ini, alur kerja tidak terus mengeksekusi langkah-langkah nominal yang tersisa (jika ada). Untuk detail selengkapnya, lihat [Penanganan pengecualian untuk alur kerja](#).

Ketika Anda memanggil operasi `SendWorkflowStepState` API, Anda harus mengirim parameter berikut:

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Anda dapat mengekstrak `ExecutionId`, `Token`, dan `WorkflowId` dari peristiwa masukan yang diteruskan ketika fungsi Lambda dijalankan (contoh ditampilkan di bagian berikut). `Status` nilainya bisa berupa `SUCCESS` atau `FAILURE`.

Untuk dapat memanggil operasi `SendWorkflowStepState` API dari fungsi Lambda, Anda harus menggunakan versi AWS SDK yang diterbitkan setelah [Alur Kerja Terkelola diperkenalkan](#).

Menggunakan beberapa fungsi Lambda secara berurutan

Bila Anda menggunakan beberapa langkah kustom satu demi satu, opsi lokasi File bekerja secara berbeda daripada jika Anda hanya menggunakan satu langkah kustom. Transfer Family tidak mendukung Lambda-processed penerusan file kembali untuk digunakan sebagai input langkah berikutnya. Jadi, jika Anda memiliki beberapa langkah khusus yang semuanya dikonfigurasi untuk menggunakan `previous.file` opsi, semuanya menggunakan lokasi file yang sama (lokasi file input untuk langkah kustom pertama).

Note

`previous.file` Pengaturan juga bekerja secara berbeda jika Anda memiliki langkah yang telah ditentukan (tag, salin, dekripsi, atau hapus) setelah langkah khusus. Jika langkah yang telah ditentukan dikonfigurasi untuk menggunakan `previous.file` pengaturan, langkah yang telah ditentukan menggunakan file input yang sama yang digunakan oleh langkah kustom. File yang diproses dari langkah kustom tidak diteruskan ke langkah yang telah ditentukan.

Mengakses file setelah pemrosesan kustom

Jika Anda menggunakan Amazon S3 sebagai penyimpanan, dan jika alur kerja menyertakan langkah khusus yang melakukan tindakan pada file yang diunggah semula, langkah selanjutnya tidak dapat mengakses file yang diproses tersebut. Artinya, langkah apa pun setelah langkah khusus tidak dapat mereferensikan file yang diperbarui dari output langkah khusus.

Misalnya, Anda memiliki tiga langkah berikut dalam alur kerja Anda.

- Langkah 1 - Unggah file bernama `example-file.txt`.
- Langkah 2 — Memanggil fungsi Lambda yang `example-file.txt` berubah dalam beberapa cara.
- Langkah 3 — Mencoba untuk melakukan pemrosesan lebih lanjut pada versi terbaru dari `example-file.txt`.

Jika Anda mengonfigurasi `sourceFileLocation` untuk Langkah 3 `${original.file}`, Langkah 3 menggunakan lokasi file asli dari saat server mengunggah file ke penyimpanan di Langkah 1. Jika

Anda menggunakan `${previous.file}` untuk Langkah 3, Langkah 3 menggunakan kembali lokasi file yang Langkah 2 digunakan sebagai input.

Oleh karena itu, Langkah 3 menyebabkan kesalahan. Misalnya, jika langkah 3 mencoba menyalin yang diperbarui `example-file.txt`, Anda menerima kesalahan berikut:

```
{
  "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"
  },
}
```

Kesalahan ini terjadi karena langkah kustom memodifikasi tag entitas (ETag) `example-file.txt` agar tidak cocok dengan file asli.

Note

Perilaku ini tidak terjadi jika Anda menggunakan Amazon EFS karena Amazon EFS tidak menggunakan tag entitas untuk mengidentifikasi file.

Contoh peristiwa dikirim ke AWS Lambda saat file upload

Contoh berikut menunjukkan peristiwa yang dikirim ke AWS Lambda ketika file upload selesai. Salah satu contoh menggunakan server Transfer Family tempat domain dikonfigurasi dengan Amazon S3. Contoh lainnya menggunakan server Transfer Family di mana domain menggunakan Amazon EFS.

Custom step that uses an Amazon S3 domain

```
{
  "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
  "serviceMetadata": {
    "executionDetails": {
      "workflowId": "w-1234567890example",
      "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
  },
  "transferDetails": {
```



```

        "sessionId": "36688ff5d2deda8c",
        "userName": "myuser",
        "serverId": "s-example1234567890"
    },
    "fileLocation": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}

```

Custom step that uses an Amazon EFS domain

```

{
    "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "EFS",
        "fileSystemId": "fs-1234567",
        "path": "/path/to/myfile"
    }
}

```

Contoh fungsi Lambda untuk langkah alur kerja khusus

Fungsi Lambda berikut mengekstrak informasi mengenai status eksekusi, dan kemudian memanggil operasi [SendWorkflowStepState](#) API untuk mengembalikan status ke alur kerja untuk langkah tersebut—baik atau. SUCCESS FAILURE Sebelum fungsi Anda memanggil operasi

SendWorkflowStepState API, Anda dapat mengonfigurasi Lambda untuk mengambil tindakan berdasarkan logika alur kerja Anda.

```
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)
    }
```

Izin IAM untuk langkah khusus

Agar langkah yang memanggil Lambda berhasil, pastikan peran eksekusi untuk alur kerja Anda berisi izin berikut.

```
{
  "Sid": "Custom",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:region:account-id:function:function-name"
  ]
}
```

Kebijakan IAM untuk alur kerja

Ketika Anda menambahkan alur kerja ke server, Anda harus memilih peran eksekusi. Server menggunakan peran ini ketika menjalankan alur kerja. Jika peran tidak memiliki izin yang tepat, AWS Transfer Family tidak dapat menjalankan alur kerja.

Bagian ini menjelaskan satu kemungkinan set izin AWS Identity and Access Management (IAM) yang dapat Anda gunakan untuk menjalankan alur kerja. Contoh lain dijelaskan nanti dalam topik ini.

Note

Jika file Amazon S3 Anda memiliki tag, Anda perlu menambahkan satu atau dua izin ke kebijakan IAM Anda.

- Tambahkan `s3:GetObjectTagging` file Amazon S3 yang tidak berversi.
- Tambahkan `s3:GetObjectVersionTagging` untuk file Amazon S3 yang berversi.

Untuk membuat peran eksekusi untuk alur kerja Anda

1. Buat peran IAM baru, dan tambahkan kebijakan AWS terkelola `AWSTransferFullAccess` ke peran tersebut. Untuk informasi selengkapnya tentang membuat peran IAM baru, lihat [the section called "Buat peran dan kebijakan IAM"](#).
2. Buat kebijakan lain dengan izin berikut, dan lampirkan ke peran Anda. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConsoleAccess",
      "Effect": "Allow",
      "Action": "s3:GetBucketLocation",
      "Resource": "*"
    },
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ],
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
    },
    {
        "Sid": "GetObjectVersion",
        "Effect": "Allow",
        "Action": "s3:GetObjectVersion",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:123456789012:function:function-name"
        ],
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
    },
]
}

```

3. Simpan peran ini dan tentukan sebagai peran eksekusi saat Anda menambahkan alur kerja ke server.

Note

Ketika Anda membangun peran IAM, AWS merekomendasikan agar Anda membatasi akses ke sumber daya Anda sebanyak mungkin untuk alur kerja Anda.

Hubungan kepercayaan alur kerja

Peran eksekusi alur kerja juga membutuhkan hubungan kepercayaan dengan `transfer.amazonaws.com`. Untuk membangun hubungan kepercayaan AWS Transfer Family, lihat [Untuk membangun hubungan kepercayaan](#).

Saat Anda membangun hubungan kepercayaan Anda, Anda juga dapat mengambil langkah-langkah untuk menghindari masalah wakil yang membingungkan. Untuk deskripsi masalah ini, serta contoh cara menghindarinya, lihat [the section called "Cross-service pencegahan wakil bingung"](#).

Contoh peran eksekusi: Dekripsi, salin, dan tag

Jika Anda memiliki alur kerja yang menyertakan langkah penandaan, penyalinan, dan dekripsi, Anda dapat menggunakan kebijakan IAM berikut. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyRead",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    },
    {
      "Sid": "CopyWrite",
```

```

    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
        "StringEquals": {
            "s3:RequestObjectTag/Archive": "yes"
        }
    }
},
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",

```

```

        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  },
  {
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
  }
]
}

```

Contoh peran eksekusi: Jalankan fungsi dan hapus

Dalam contoh ini, Anda memiliki alur kerja yang memanggil fungsi. AWS Lambda Jika alur kerja menghapus file yang diunggah dan memiliki langkah penanganan pengecualian untuk bertindak atas eksekusi alur kerja yang gagal pada langkah sebelumnya, gunakan kebijakan IAM berikut. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Delete",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    },
    {
      "Sid": "Custom",
      "Effect": "Allow",
      "Action": [

```

```
        "lambda:InvokeFunction"  
      ],  
      "Resource": [  
        "arn:aws:lambda:us-east-1:123456789012:function:function-name"  
      ]  
    }  
  ]  
}
```

Penanganan pengecualian untuk alur kerja

Jika terjadi kesalahan selama eksekusi alur kerja, langkah-langkah penanganan pengecualian yang Anda tentukan akan dijalankan. Anda menentukan langkah penanganan kesalahan untuk alur kerja dengan cara yang sama seperti Anda menentukan langkah nominal untuk alur kerja. Misalnya, misalkan Anda telah mengonfigurasi pemrosesan kustom dalam langkah-langkah nominal untuk memvalidasi file yang masuk. Jika validasi file gagal, langkah penanganan pengecualian dapat mengirim email ke administrator.

Contoh alur kerja berikut berisi dua langkah:

- Satu langkah nominal yang memeriksa apakah file yang diunggah dalam format CSV
- Langkah penanganan pengecualian yang mengirim email jika file yang diunggah tidak dalam format CSV, dan langkah nominal gagal

Untuk memulai langkah penanganan pengecualian, AWS Lambda fungsi dalam langkah nominal harus merespons dengan `Status="FAILURE"`. Untuk informasi selengkapnya tentang penanganan kesalahan dalam alur kerja, lihat [the section called “Gunakan langkah-langkah pemrosesan file khusus”](#).

w-1234567890abcdef0
Delete

Description

Name
Delete after upload

Workflow description
test-my-workflow

Nominal steps (1) Info

Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details

Exception handlers (1) Info

Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

Pantau eksekusi alur kerja

Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS Cloud secara real time. Anda dapat menggunakan Amazon CloudWatch untuk mengumpulkan dan melacak metrik, yang merupakan variabel yang dapat Anda ukur untuk alur kerja Anda. Anda dapat melihat metrik alur kerja dan log gabungan menggunakan Amazon. CloudWatch

CloudWatch logging untuk alur kerja

CloudWatch menyediakan audit dan pencatatan terkonsolidasi untuk kemajuan dan hasil alur kerja.

Lihat CloudWatch log Amazon untuk alur kerja

1. Buka CloudWatch konsol Amazon di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi kiri, pilih Log, lalu pilih Grup log.
3. Pada halaman Grup log, pada bilah navigasi, pilih Wilayah yang benar untuk AWS Transfer Family server Anda.
4. Pilih grup log yang sesuai dengan server Anda.

Misalnya, jika ID server Anda-1234567890abcdef0, grup log Anda adalah/aws/transfer/s-1234567890abcdef0.

5. Pada halaman detail grup log untuk server Anda, aliran log terbaru ditampilkan. Ada dua aliran log untuk pengguna yang Anda jelajahi:
- Satu untuk setiap sesi Secure Shell (SSH) File Transfer Protocol (SFTP).
 - Satu untuk alur kerja yang sedang dijalankan untuk server Anda. Format untuk aliran log untuk alur kerja adalah *username.workflowID.uniqueStreamSuffix*.

Misalnya, jika pengguna Andamary-major, Anda memiliki aliran log berikut:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

 Note

Pengidentifikasi alfanumerik 16 digit yang tercantum dalam contoh ini adalah fiktif. Nilai yang Anda lihat di Amazon CloudWatch berbeda.

Halaman peristiwa Log untuk mary-major-usa-east.1234567890abcdef0 menampilkan detail untuk setiap sesi pengguna, dan aliran mary.w-abcdef01234567890.021345abcdef6789 log berisi detail untuk alur kerja.

Berikut ini adalah contoh aliran log untuk mary.w-abcdef01234567890.021345abcdef6789, berdasarkan alur kerja (w-abcdef01234567890) yang berisi langkah salin.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
}
```

```

    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepStarted",
    "details": {
      "input": {
        "fileLocation": {
          "backingStore": "S3",
          "bucket": "amzn-s3-demo-bucket",
          "key": "mary/workflowSteps2.json",
          "versionId": "version-id",
          "etag": "etag-id"
        }
      },
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepCompleted",
    "details": {
      "output": {},
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",

```

```

        "sessionId": "session-id"
    },
    {
        "type": "ExecutionCompleted",
        "details": {},
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    }
}

```

CloudWatch metrik untuk alur kerja

AWS Transfer Family menyediakan beberapa metrik untuk alur kerja. Anda dapat melihat metrik berapa banyak eksekusi alur kerja yang dimulai, diselesaikan dengan sukses, dan gagal pada menit sebelumnya. Semua CloudWatch metrik untuk Transfer Family dijelaskan dalam [Menggunakan CloudWatch metrik untuk server Transfer Family](#).

Buat alur kerja dari template

Anda dapat menerapkan CloudFormation tumpukan yang membuat alur kerja dan server dari template. Prosedur ini berisi contoh yang dapat Anda gunakan untuk menyebarkan alur kerja dengan cepat.

Untuk membuat CloudFormation tumpukan yang membuat AWS Transfer Family alur kerja dan server

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Simpan kode berikut ke file.

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. Ganti item berikut dengan nilai aktual Anda.
 - Ganti *workflow-execution-role-arn* dengan ARN untuk peran eksekusi alur kerja yang sebenarnya. Sebagai contoh, `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`.
 - Ganti `arn:aws:lambda:region:account-id:function:function-name` dengan ARN untuk fungsi Lambda Anda. Misalnya, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.
4. Ikuti petunjuk untuk menerapkan CloudFormation tumpukan dari template yang ada di [Memilih template tumpukan](#) di Panduan AWS CloudFormation Pengguna.

Setelah tumpukan digunakan, Anda dapat melihat detailnya di tab Output di CloudFormation konsol. Template membuat server AWS Transfer Family SFTP baru yang menggunakan pengguna yang dikelola layanan, dan alur kerja baru, dan mengaitkan alur kerja dengan server baru.

Menghapus alur kerja dari server Transfer Family

Jika Anda telah mengaitkan alur kerja dengan server Transfer Family, dan sekarang Anda ingin menghapus asosiasi tersebut, Anda dapat melakukannya dengan menggunakan konsol atau secara terprogram.

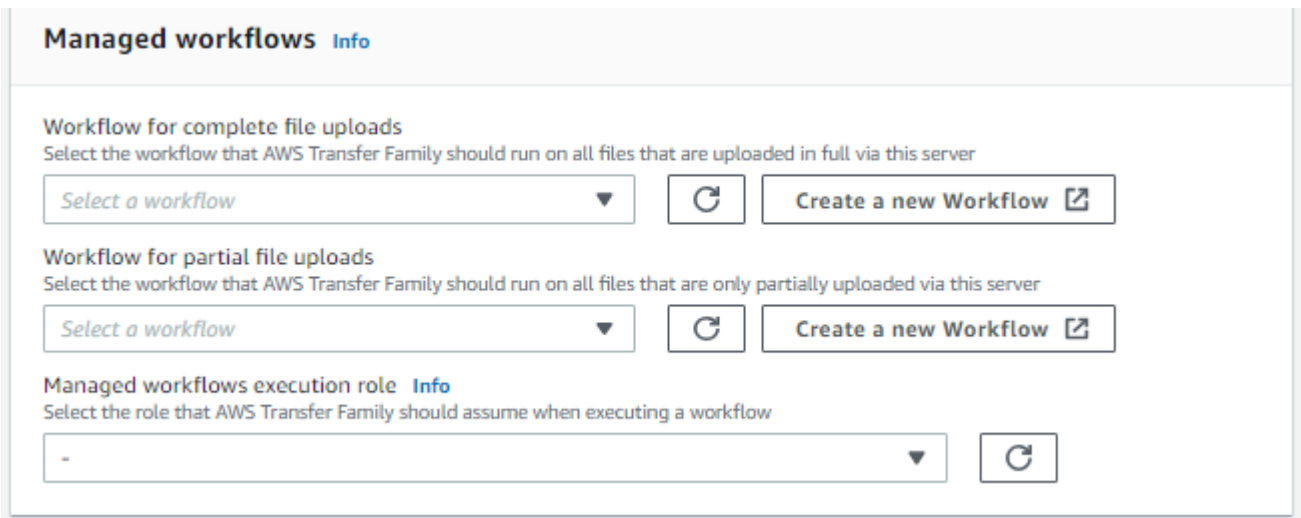
Console

Untuk menghapus alur kerja dari server Transfer Family

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server.
3. Pilih pengenalan untuk server di kolom ID Server.
4. Pada halaman detail untuk server, gulir ke bawah ke bagian Detail tambahan, lalu pilih Edit.
5. Pada halaman Edit detail tambahan, di bagian Alur kerja terkelola, kosongkan informasi untuk semua pengaturan:
 - Pilih tanda hubung (-) dari daftar alur kerja untuk Alur Kerja untuk upload file lengkap.
 - Jika belum dihapus, pilih tanda hubung (-) dari daftar alur kerja untuk Alur Kerja untuk unggahan file sebagian.
 - Pilih tanda hubung (-) dari daftar peran untuk peran eksekusi alur kerja terkelola.

Jika Anda tidak melihat tanda hubung, gulir ke atas hingga Anda melihatnya, karena ini adalah nilai pertama di setiap menu.

Layar akan terlihat seperti berikut ini.



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. Gulir ke bawah dan pilih Simpan untuk menyimpan perubahan Anda.

CLI

Anda menggunakan panggilan `update-server` (atau `UpdateServer` untuk API), dan memberikan argumen kosong untuk `OnUpload` dan `OnPartialUpload` parameter.

Dari AWS CLI, jalankan perintah berikut:

```
aws transfer update-server --server-id your-server-id --workflow-details  
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Ganti *your-server-id* dengan ID untuk server Anda. Misalnya, jika ID server Anda `s-01234567890abcdef`, perintahnya adalah sebagai berikut:

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details  
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Pembatasan dan batasan alur kerja yang dikelola

Pembatasan

Pembatasan berikut saat ini berlaku untuk alur kerja pemrosesan pasca-unggah untuk AWS Transfer Family

- Cross-account dan AWS Lambda fungsi lintas wilayah tidak didukung. Namun, Anda dapat menyalin seluruh akun, asalkan kebijakan AWS Identity and Access Management (IAM) Anda dikonfigurasi dengan benar.
- Untuk semua langkah alur kerja, setiap bucket Amazon S3 yang diakses oleh alur kerja harus berada di wilayah yang sama dengan alur kerja itu sendiri.
- Untuk langkah dekripsi, tujuan dekripsi harus cocok dengan sumber untuk Wilayah dan penyimpanan cadangan (misalnya, jika file yang akan didekripsi disimpan di Amazon S3, maka tujuan yang ditentukan juga harus di Amazon S3).
- Hanya langkah kustom asinkron yang didukung.
- Batas waktu langkah khusus adalah perkiraan. Artinya, mungkin perlu waktu sedikit lebih lama dari yang ditentukan. Selain itu, alur kerja tergantung pada fungsi Lambda. Oleh karena itu, jika fungsi tertunda selama eksekusi, alur kerja tidak menyadari penundaan.
- Jika Anda melebihi batas pembatasan, Transfer Family tidak menambahkan operasi alur kerja ke antrian.
- Alur kerja tidak dimulai untuk file yang memiliki ukuran 0. File dengan ukuran lebih besar dari 0 melakukan memulai alur kerja terkait.
- Anda dapat melampirkan alur kerja pemrosesan file ke server Transfer Family yang menggunakan protokol AS2: namun, pesan AS2 tidak menjalankan alur kerja yang dilampirkan ke server.

Batasan

Selain itu, batasan fungsional berikut berlaku untuk alur kerja untuk Transfer Family:

- Jumlah alur kerja per Wilayah, per akun, dibatasi hingga 10.
- Batas waktu maksimum untuk langkah-langkah khusus adalah 30 menit.
- Jumlah maksimum langkah dalam alur kerja adalah 8.
- Jumlah maksimum tag per alur kerja adalah 50.
- Jumlah maksimum eksekusi bersamaan yang berisi langkah dekripsi adalah 250 per alur kerja.
- Anda dapat menyimpan maksimal 3 kunci pribadi PGP, per server Transfer Family, per pengguna.
- Ukuran maksimum untuk file yang didekripsi adalah 10 GB.
- Kami membatasi tingkat eksekusi baru menggunakan sistem [token bucket](#) dengan kapasitas burst 100 dan tingkat isi ulang 1.
- Setiap kali Anda menghapus alur kerja dari server dan menggantinya dengan yang baru, atau memperbarui konfigurasi server (yang memengaruhi peran eksekusi alur kerja), Anda harus

menunggu sekitar 10 menit sebelum menjalankan alur kerja baru. Server Transfer Family menyimpan cache detail alur kerja, dan dibutuhkan waktu 10 menit bagi server untuk menyegarkan cache-nya.

Selain itu, Anda harus keluar dari sesi SFTP aktif apa pun, dan kemudian masuk kembali setelah masa tunggu 10 menit untuk melihat perubahannya.

Mengelola server

Di bagian ini, Anda dapat menemukan informasi tentang cara melihat daftar server Anda, cara melihat detail server Anda, cara mengedit detail server Anda, dan cara mengubah kunci host untuk SFTP-enabled server Anda.

Topik

- [Lihat daftar server](#)
- [Hapus server](#)
- [Lihat detail server SFTP, FTPS, dan FTP](#)
- [Lihat detail server AS2](#)
- [Dukungan IPv6 untuk server Transfer Family](#)
- [Edit detail server](#)
- [Edit konfigurasi penyedia identitas](#)
- [Kelola kunci host untuk SFTP-enabled server Anda](#)
- [Memantau penggunaan di konsol](#)

Lihat daftar server

Di AWS Transfer Family konsol, Anda dapat menemukan daftar semua server Anda yang terletak di AWS Wilayah yang Anda pilih.

Untuk menemukan daftar server Anda yang ada di suatu AWS Wilayah

- Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.

Jika Anda memiliki satu atau beberapa server di AWS Wilayah saat ini, konsol terbuka untuk menampilkan daftar server Anda. Jika Anda tidak melihat daftar server, pastikan Anda berada di Wilayah yang benar. Anda juga dapat memilih Server dari panel navigasi.

Untuk informasi selengkapnya tentang melihat detail server Anda, lihat [Lihat detail server SFTP, FTPS, dan FTP](#).

Hapus server

Prosedur ini menjelaskan cara menghapus server Transfer Family dengan menggunakan AWS Transfer Family konsol atau AWS CLI.

Important

Anda ditagih, untuk setiap protokol yang diaktifkan untuk mengakses titik akhir Anda, hingga Anda menghapus server.

Warning

Menghapus server mengakibatkan semua penggunaanya dihapus. Data dalam bucket yang diakses dengan menggunakan server tidak dihapus, dan tetap dapat diakses oleh AWS pengguna yang memiliki hak istimewa untuk bucket Amazon S3 tersebut.

Console

Untuk menghapus server dengan menggunakan konsol

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server.
3. Pilih kotak centang server yang ingin Anda hapus.
4. Untuk Tindakan, pilih Hapus.
5. Di kotak dialog konfirmasi yang muncul, masukkan kata **delete**, lalu pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus server.

Server dihapus dari halaman Server dan Anda tidak lagi ditagih untuk itu.

AWS CLI

Untuk menghapus server dengan menggunakan CLI

1. (Opsional) Jalankan perintah berikut untuk melihat detail server yang ingin Anda hapus secara permanen.

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

`describe-server` Perintah ini mengembalikan semua detail untuk server Anda.

2. Jalankan perintah berikut untuk menghapus server.

```
aws transfer delete-server --server-id your-server-id
```

Jika berhasil, perintah menghapus server dan tidak mengembalikan informasi apa pun.

Lihat detail server SFTP, FTPS, dan FTP

Anda dapat menemukan daftar detail dan properti untuk AWS Transfer Family server individual. Properti server termasuk protokol, penyedia identitas, status, jenis titik akhir, nama host khusus, titik akhir, pengguna, peran logging, kunci host server, dan tag.

Untuk melihat detail server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih pengenal di kolom ID Server untuk melihat halaman detail Server, ditampilkan berikut.

Anda dapat mengubah properti server di halaman ini dengan memilih Edit. Untuk informasi selengkapnya tentang mengedit detail server, lihat [Edit detail server](#). Halaman detail untuk server AS2 sedikit berbeda. Untuk server AS2, lihat [Lihat detail server AS2](#).

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

Note

Kunci host server Deskripsi dan Nilai impor Tanggal baru per September 2022. Nilai-nilai ini diperkenalkan untuk mendukung fitur beberapa kunci host. Fitur ini memerlukan

migrasi dari setiap kunci host tunggal yang digunakan sebelum pengenalan beberapa kunci host.

Nilai tanggal yang diimpor untuk kunci host server yang dimigrasi diatur ke tanggal modifikasi terakhir untuk server. Artinya, tanggal yang Anda lihat untuk kunci host yang dimigrasi sesuai dengan tanggal terakhir Anda memodifikasi server dengan cara apa pun, sebelum migrasi kunci host server.

Satu-satunya kunci yang dimigrasikan adalah kunci host server tertua atau satu-satunya. Setiap kunci tambahan memiliki tanggal aktualnya sejak Anda mengimpornya. Selain itu, kunci yang dimigrasi memiliki deskripsi yang membuatnya mudah untuk mengidentifikasinya sebagai telah dimigrasi.

Migrasi terjadi antara 2 September dan 13 September. Tanggal migrasi aktual dalam rentang ini tergantung pada Wilayah server Anda.

Additional details

[Edit](#)

Log group

[/aws/transfer/s-](#)

Logging role

-

Security Policy

[Info](#)
TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner

[View the display message](#)

Optimized directories

[Info](#)
ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

Lihat detail server AS2

Anda dapat menemukan daftar detail dan properti untuk AWS Transfer Family server individual. Properti server termasuk protokol, status, dan banyak lagi. Untuk server AS2, Anda juga dapat melihat alamat IP keluar MDN asinkron AS2.

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

[Edit](#)

AS2 Auth

Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

Setiap server AS2 diberi tiga alamat IP statis. Gunakan alamat IP ini untuk mengirim mDNS asinkron ke mitra dagang Anda melalui AS2.

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

-  
-  
-  

Bagian bawah halaman detail server AS2 berisi detail untuk alur kerja terlampir dan informasi pemantauan dan penandaan.

Workflows

Workflow for complete uploads
w-  0

Workflow for partial uploads
-

Managed workflows execution role


[Edit](#)

Monitoring

1h 3h 12h 1d 3d 1w 

UTC timezone 

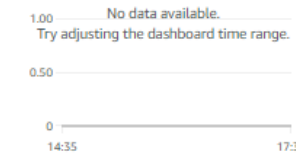
 

BytesIn

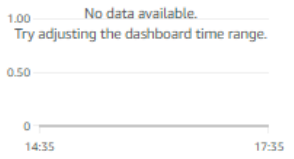
BytesOut

FilesIn

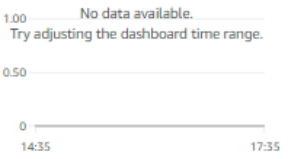
FilesOut



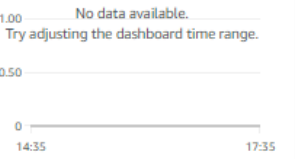
No data available.
Try adjusting the dashboard time range.



No data available.
Try adjusting the dashboard time range.



No data available.
Try adjusting the dashboard time range.



No data available.
Try adjusting the dashboard time range.

AS2 Monitoring

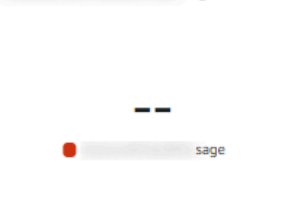
1h 3h 12h 1d 3d 1w 

UTC timezone 

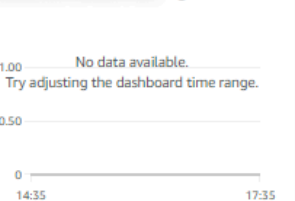
 

InboundMessage

InboundMessage



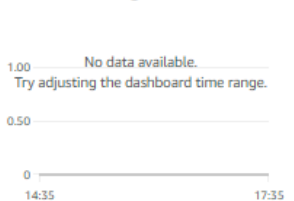
sage



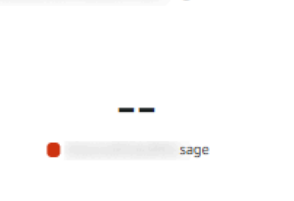
sage



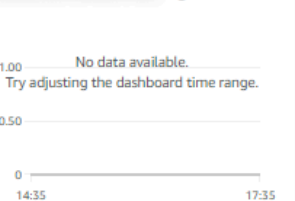
InboundMessage



No data available.
Try adjusting the dashboard time range.



sage



No data available.
Try adjusting the dashboard time range.

Dukungan IPv6 untuk server Transfer Family

AWS Transfer Family mendukung titik akhir dual-stack (IPv4 dan IPv6) untuk sumber daya berikut:

- Titik akhir publik SFTP
- Titik akhir internal VPC untuk semua protokol (dan AS2) SFTP/FTPS/FTP
- Titik akhir publik untuk server AS2-enabled Transfer Family, dengan menggunakan langkah-langkah yang disediakan di [Menggunakan Application Load Balancer untuk konektivitas server AS2 dual-stack](#)
- Titik akhir API

Dengan dukungan dual-stack, endpoint Transfer Family Anda dapat berkomunikasi dengan klien berkemampuan IPv4 dan IPv6. Ini memungkinkan Anda untuk secara bertahap beralih dari sistem berbasis IPv4 ke IPv6 tanpa perlu beralih sekaligus, memenuhi persyaratan kepatuhan IPv6, dan menghilangkan kebutuhan akan peralatan jaringan yang mahal untuk menangani terjemahan alamat antara IPv4 dan IPv6. Untuk detailnya, lihat [DNS dan Titik Akhir di Referensi AWS Transfer Family](#) API. Untuk daftar lengkap titik akhir yang tersedia, lihat [AWS Transfer Family titik akhir dan kuota](#) di Referensi Umum AWS

Keterbatasan IPv6

Sumber daya Transfer Family berikut saat ini tidak mendukung IPv6:

- VPC-Internet titik akhir
- Jenis titik akhir VPC_ENDPOINT (usang)

Protokol FTPS mendukung perintah PASV dan EPSV untuk meminta port data terbuka untuk daftar file, mendapatkan, dan menempatkan operasi. Namun, PASV tidak bekerja dengan IPv6 karena memerlukan respons. IPv4-specific EPSV terus bekerja karena hanya mengembalikan informasi port.

Untuk menggunakan FTPS, kami merekomendasikan salah satu dari yang berikut:

- Konfigurasi klien FTPS Anda untuk menggunakan EPSV
- Gunakan IPv4 alih-alih IPv6

SFTP mendukung IPv4 dan IPv6. Sebaiknya gunakan SFTP alih-alih FTPS saat bekerja dengan titik akhir dual-stack.

Mengkonfigurasi IPv6 untuk server

Saat membuat server baru atau memperbarui server yang ada, Anda dapat memilih jenis alamat IP:

- IPv4 (default): Untuk kompatibilitas mundur, server hanya akan menerima koneksi IPv4.
- Dual-stack: Server akan menerima koneksi IPv4 dan IPv6.

Untuk memperbarui jenis alamat IP server yang ada:

1. Hentikan server.
2. Edit detail titik akhir.
3. Ubah jenis alamat IP menjadi Dual-stack.
4. Mulai server .

Note

Untuk VPC-Internet titik akhir, mode dual-stack saat ini tidak didukung.

Menggunakan Application Load Balancer untuk konektivitas server AS2 dual-stack

Anda dapat mengaktifkan konektivitas dual-stack (IPv4 dan IPv6) ke server AS2 Anda dengan menggunakan Application Load Balancer yang memiliki titik akhir yang menghadap publik. Hal ini memungkinkan mitra dagang untuk terhubung ke server AS2 Anda menggunakan IPv4 atau IPv6.

Untuk menyiapkan Application Load Balancer dual-stack untuk server AS2 Anda

1. Buat VPC dengan pengaturan berikut:
 - Hanya VPC
 - Input IPv4 CIDR manual
 - Amazon-provided Blok IPv6 CIDR
2. Buat setidaknya dua subnet di Availability Zone yang berbeda:
 - Tambahkan IPv6 CIDR ke subnet

- Saat membuat subnet, alokasikan hanya sebagian dari alamat VPC agar IPv4/IPv6 alamat tersedia untuk subnet tambahan
3. Buat gateway internet untuk VPC.
 4. Edit tabel rute dan tambahkan dua rute:
 - Satu rute dengan Destinasi `0.0.0.0/0`
 - Satu rute dengan Destinasi `::/0`
 - Tetapkan kedua target rute ke gateway internet yang Anda buat
 5. Buat AS2-enabled server di VPC yang Anda buat di langkah 1. Pastikan untuk menentukan `IpAddressType` sebagai `DUALSTACK`.

Untuk detail tentang cara membuat server Transfer Family yang menggunakan protokol AS2, lihat [Buat server AS2](#).

6. Buat grup target:
 - Untuk Tentukan detail grup, konfigurasi:
 - Jenis target: Alamat IP
 - Nama: Masukkan nama
 - Protokol: HTTP
 - Pelabuhan: 5080
 - VPC: Pilih VPC yang Anda buat
 - Versi protokol: HTTP1
 - Pemeriksaan Kesehatan: Gunakan default
 - Untuk target Register:
 - Masukkan alamat IPv4 pribadi server AS2 Anda
 - Pilih Sertakan sebagai tertunda di bawah
7. Buat Application Load Balancer:
 - Masukkan nama
 - Untuk Skema, pilih Internet-facing
 - Untuk jenis alamat IP, pilih Dualstack
 - Untuk pemetaan Jaringan:

- Pilih Availability Zones tempat Anda membuat subnet
- Untuk grup Keamanan, pilih grup keamanan yang memungkinkan lalu lintas IPv4 dan IPv6 masuk dari alamat IP apa pun di port 80
- Untuk Pendengar dan perutean:
 - Protokol: HTTP
 - Pelabuhan: 80
 - Tindakan default: Teruskan ke grup target yang Anda buat
- Pilih Buat penyeimbang beban

Setelah Anda membuat Application Load Balancer, mitra dagang dapat menggunakan nama DNS-nya untuk mengirim lalu lintas ke server AS2 Anda. Konfigurasi ini memungkinkan server AS2 Anda untuk menerima koneksi dari klien IPv4 dan IPv6 melalui Application Load Balancer dual-stack.

Edit detail server

Setelah Anda membuat AWS Transfer Family server, Anda dapat mengedit konfigurasi server.

Topik

- [Edit protokol transfer file](#)
- [Edit titik akhir server](#)
- [Edit konfigurasi logging Anda](#)
- [Edit kebijakan keamanan](#)
- [Mengubah alur kerja terkelola untuk server Anda](#)
- [Ubah spanduk tampilan untuk server Anda](#)
- [Menempatkan server Anda secara online atau offline](#)

Untuk mengedit konfigurasi server

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server.
3. Pilih pengenal di kolom ID Server untuk melihat halaman detail Server, ditampilkan berikut.

Anda dapat mengubah properti server di halaman ini dengan memilih Edit:

- Untuk mengubah protokol, lihat. [Edit protokol transfer file](#)
- Untuk penyedia identitas, Anda sekarang dapat mengubah di antara semua jenis penyedia identitas (service-managed, AWS Directory Service, atau penyedia identitas kustom). Untuk detail tentang mengubah jenis penyedia identitas dan informasi yang diperlukan untuk setiap transisi, lihat [Edit konfigurasi penyedia identitas](#).
- Untuk mengubah jenis titik akhir atau nama host kustom, lihat. [Edit titik akhir server](#)
- Untuk menambahkan perjanjian, Anda harus terlebih dahulu menambahkan AS2 sebagai protokol ke server Anda. Lihat perinciannya di [Edit protokol transfer file](#).
- Untuk mengelola kunci host untuk server Anda, lihat [Kelola kunci host untuk SFTP-enabled server Anda](#).
- Di bawah Detail tambahan, Anda dapat mengedit informasi berikut:
 - Untuk mengubah peran logging, lihat [Edit konfigurasi logging Anda](#).
 - Untuk mengubah kebijakan keamanan, lihat [Edit kebijakan keamanan](#).
 - Untuk mengubah kunci host server, lihat [Kelola kunci host untuk SFTP-enabled server Anda](#).
 - Untuk mengubah alur kerja terkelola untuk server Anda, lihat [Mengubah alur kerja terkelola untuk server Anda](#).
 - Untuk mengedit spanduk tampilan untuk server Anda, lihat [Ubah spanduk tampilan untuk server Anda](#).
- Di bawah Konfigurasi tambahan, Anda dapat mengedit informasi berikut:
 - SetStat opsi: aktifkan opsi ini untuk mengabaikan kesalahan yang dihasilkan saat klien mencoba menggunakan SETSTAT pada file yang Anda unggah ke bucket Amazon S3. Untuk detail tambahan, lihat SetStatOption dokumentasi dalam [ProtocolDetailstopik](#).
 - Dimulainya kembali sesi TLS: menyediakan mekanisme untuk melanjutkan atau berbagi kunci rahasia yang dinegosiasikan antara kontrol dan koneksi data untuk sesi FTPS. Untuk detail tambahan, lihat TlsSessionResumptionMode dokumentasi dalam [ProtocolDetailstopik](#).
 - IP pasif: menunjukkan mode pasif, untuk protokol FTP dan FTPS. Masukkan satu alamat IPv4, seperti alamat IP publik firewall, router, atau penyeimbang beban. Untuk detail tambahan, lihat PassiveIp dokumentasi dalam [ProtocolDetailstopik](#).

Note

Hindari menempatkan Network Load Balancers (NLBs) atau gateway NAT di depan server. AWS Transfer Family Konfigurasi ini meningkatkan biaya dan dapat menyebabkan masalah kinerja. Untuk detail selengkapnya, lihat [Hindari menempatkan NLB dan NAT di depan AWS Transfer Family server](#)

- Untuk memulai atau menghentikan server Anda, lihat [Menempatkan server Anda secara online atau offline](#).
- Untuk menghapus server, lihat [Hapus server](#).
- Untuk mengedit properti pengguna, lihat [Mengelola kontrol akses](#).

Protocols[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider[Edit](#)

Identity provider type
Service managed

Note

Kunci host server Deskripsi dan Nilai impor Tanggal baru per September 2022. Nilai-nilai ini diperkenalkan untuk mendukung fitur beberapa kunci host. Fitur ini memerlukan migrasi dari setiap kunci host tunggal yang digunakan sebelum pengenalan beberapa kunci host.

Nilai tanggal yang diimpor untuk kunci host server yang dimigrasi diatur ke tanggal modifikasi terakhir untuk server. Artinya, tanggal yang Anda lihat untuk kunci host yang dimigrasi sesuai dengan tanggal terakhir Anda memodifikasi server dengan cara apa pun, sebelum migrasi kunci host server.

Satu-satunya kunci yang dimigrasikan adalah kunci host server tertua atau satu-satunya. Setiap kunci tambahan memiliki tanggal aktualnya sejak Anda mengimpornya. Selain itu, kunci yang dimigrasi memiliki deskripsi yang membuatnya mudah untuk mengidentifikasinya sebagai telah dimigrasi.

Migrasi terjadi antara 2 September dan 13 September. Tanggal migrasi aktual dalam rentang ini tergantung pada Wilayah server Anda.

Additional details Edit

Log group /aws/transfer/s-	Domain Amazon S3	SetStat option Ignore
Logging role Info -	Login display banner View the display message	TLS session resumption -
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	Passive IP -

Edit protokol transfer file

Di AWS Transfer Family konsol, Anda dapat mengedit protokol transfer file. Protokol transfer file menghubungkan klien ke titik akhir server Anda.

Untuk mengedit protokol

1. Pada halaman Detail Server, pilih Edit di samping Protokol.
2. Pada halaman Edit protokol, pilih atau kosongkan kotak centang protokol atau kotak centang untuk menambah atau menghapus protokol transfer file berikut:

- Secure Shell (SSH) File Transfer Protocol (SFTP) — transfer file melalui SSH

Untuk informasi lebih lanjut tentang SFTP, lihat [Buat SFTP-enabled server](#)

- File Transfer Protocol Secure (FTPS) — transfer file dengan enkripsi TLS

Untuk informasi lebih lanjut tentang FTP, lihat [Buat FTPS-enabled server](#).

- File Transfer Protocol (FTP) — transfer file tidak terenkripsi

Untuk informasi lebih lanjut tentang FTPS, lihat [Buat FTP-enabled server](#).

Note

Jika Anda memiliki server yang ada diaktifkan hanya untuk SFTP, dan Anda ingin menambahkan FTPS dan FTP, Anda harus memastikan bahwa Anda memiliki penyedia identitas yang tepat dan pengaturan tipe titik akhir yang kompatibel dengan FTPS dan FTP.

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](#)

Jika Anda memilih FTPS, Anda harus memilih sertifikat yang disimpan di AWS Certificate Manager (ACM) yang akan digunakan untuk mengidentifikasi server Anda ketika klien terhubung ke sana melalui FTPS.

Untuk meminta sertifikat publik baru, lihat [Meminta sertifikat publik](#) di Panduan AWS Certificate Manager Pengguna.

Untuk mengimpor sertifikat yang ada ke ACM, lihat [Mengimpor sertifikat ke ACM di Panduan Pengguna](#). AWS Certificate Manager

Untuk meminta sertifikat pribadi untuk menggunakan FTPS melalui alamat IP pribadi, lihat [Meminta sertifikat pribadi](#) di AWS Certificate Manager Panduan Pengguna.

Sertifikat dengan algoritme kriptografi dan ukuran kunci berikut didukung:

- 2048-bit RSA (RSA_2048)
- 4096-bit RSA (RSA_4096)
- Elliptic Prime Curve 256 bit (EC_prime256v1)
- Elliptic Prime Curve 384 bit (EC_secp384r1)
- Elliptic Prime Curve 521 bit (EC_secp521r1)

 Note

Sertifikat harus berupa sertifikat SSL/TLS X.509 versi 3 yang valid dengan FQDN atau alamat IP yang ditentukan dan berisi informasi tentang penerbit.

3. Pilih Simpan. Anda dikembalikan ke halaman detail Server.

Edit titik akhir server

Di AWS Transfer Family konsol, Anda dapat memodifikasi jenis titik akhir server dan nama host khusus. Selain itu, untuk titik akhir VPC, Anda dapat mengedit informasi zona ketersediaan.

Untuk mengedit detail titik akhir server

1. Pada halaman Detail Server, pilih Edit di samping Detail titik akhir.
2. Sebelum Anda dapat mengedit jenis Endpoint, Anda harus terlebih dahulu menghentikan server. Kemudian, pada halaman konfigurasi Edit titik akhir, untuk tipe Endpoint, Anda dapat memilih salah satu dari nilai berikut:
 - Publik — Opsi ini membuat server Anda dapat diakses melalui internet.
 - VPC — Opsi ini membuat server Anda dapat diakses di cloud pribadi virtual (VPC) Anda. Untuk informasi tentang VPC, lihat [Buat server di cloud pribadi virtual](#)
3. Untuk nama host Kustom, pilih salah satu dari berikut ini:
 - Tidak ada - Jika Anda tidak ingin menggunakan domain khusus, pilih Tidak Ada.

Anda mendapatkan nama host server yang disediakan oleh AWS Transfer Family. Nama host server mengambil formulir `serverId.server.transfer.regionId.amazonaws.com`.

- Amazon Route 53 Alias DNS — Untuk menggunakan alias DNS yang dibuat secara otomatis untuk Anda di Route 53, pilih opsi ini.
- DNS Lainnya — Untuk menggunakan nama host yang sudah Anda miliki di layanan DNS eksternal pilih DNS Lainnya.

Memilih Amazon Route 53 Alias DNS atau DNS Lainnya menentukan metode resolusi nama untuk dikaitkan dengan titik akhir server Anda.

Misalnya, domain kustom Anda mungkin `ftp.inbox.example.com`. Nama host khusus menggunakan nama DNS yang Anda berikan dan dapat diselesaikan oleh layanan DNS. Anda dapat menggunakan Route 53 sebagai penyelesai DNS Anda, atau menggunakan penyedia layanan DNS Anda sendiri. Untuk mempelajari cara AWS Transfer Family menggunakan Route 53 untuk merutekan lalu lintas dari domain kustom Anda ke titik akhir server, lihat [Bekerja dengan nama host khusus](#).

4. Untuk titik akhir VPC, Anda dapat mengubah informasi di panel Availability Zones.
5. Pilih Simpan. Anda dikembalikan ke halaman detail Server.

Edit konfigurasi logging Anda

Di AWS Transfer Family konsol, Anda dapat mengubah konfigurasi logging Anda.

Note

Jika Transfer Family membuat peran IAM CloudWatch logging untuk Anda saat membuat server, peran IAM akan dipanggil. `AWSTransferLoggingAccess` Anda dapat menggunakannya untuk semua server Transfer Family Anda.

Untuk mengedit konfigurasi logging Anda

1. Pada halaman Detail Server, pilih Edit di samping Detail tambahan.
2. Berdasarkan konfigurasi Anda, pilih antara peran logging, logging JSON terstruktur, atau keduanya. Untuk informasi selengkapnya, lihat [Memperbarui logging untuk server](#).

Edit kebijakan keamanan

Prosedur ini menjelaskan cara mengubah kebijakan keamanan server Transfer Family dengan menggunakan AWS Transfer Family konsol atau AWS CLI.

Note

Jika titik akhir Anda FIPS-enabled, Anda tidak dapat mengubah kebijakan keamanan FIPS menjadi kebijakan keamanan non-FIPS.

Console

Untuk mengedit kebijakan keamanan dengan menggunakan konsol

1. Pada halaman Detail Server, pilih Edit di samping Detail tambahan.
2. Di bagian Opsi Algoritma Kriptografi, pilih kebijakan keamanan yang berisi algoritme kriptografi yang diaktifkan untuk digunakan oleh server Anda.

Untuk informasi selengkapnya tentang kebijakan keamanan, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

3. Pilih Simpan.

Anda dikembalikan ke halaman Detail Server di mana Anda dapat melihat kebijakan keamanan yang diperbarui.

AWS CLI

Untuk mengedit kebijakan keamanan dengan menggunakan CLI

1. Jalankan perintah berikut untuk melihat kebijakan keamanan saat ini yang dilampirkan ke server Anda.

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

`describe-server` Perintah ini mengembalikan semua detail untuk server Anda, termasuk baris berikut:

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

Dalam hal ini, kebijakan keamanan untuk server adalah `TransferSecurityPolicy-2018-11`.

2. Pastikan untuk memberikan nama yang tepat dari kebijakan keamanan ke perintah. Misalnya, jalankan perintah berikut untuk memperbarui server ke `TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name  
"TransferSecurityPolicy-2023-05"
```

Note

Nama-nama kebijakan keamanan yang tersedia tercantum di [Kebijakan keamanan untuk AWS Transfer Family server](#).

Jika berhasil, perintah mengembalikan kode berikut, dan memperbarui kebijakan keamanan server Anda.

```
{  
  "ServerId": "your-server-id"  
}
```

Mengubah alur kerja terkelola untuk server Anda

Di AWS Transfer Family konsol, Anda dapat mengubah alur kerja terkelola yang terkait dengan server.

Untuk mengubah alur kerja terkelola

1. Pada halaman Detail Server, pilih Edit di samping Detail tambahan.
2. Pada halaman Edit detail tambahan, di bagian Alur kerja terkelola, pilih alur kerja yang akan dijalankan di semua unggahan.

Note

Jika Anda belum memiliki alur kerja, pilih Buat alur kerja baru untuk membuatnya.

- a. Pilih ID alur kerja yang akan digunakan.
- b. Pilih peran eksekusi. Ini adalah peran yang diasumsikan Transfer Family saat menjalankan langkah-langkah alur kerja. Untuk informasi selengkapnya, lihat [Kebijakan IAM untuk alur kerja](#). Pilih Simpan.

The screenshot shows the 'Managed workflows' section in the AWS Transfer Family console. It has a title bar with 'Managed workflows' and an 'Info' link. Below this, there are three main sections:

- Workflow for complete file uploads**: A subtitle 'Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server'. It contains a dropdown menu with 'w-' followed by a redacted ID, a refresh button, and a 'Create a new Workflow' button with an external link icon.
- Workflow for partial file uploads**: A subtitle 'Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server'. It contains a dropdown menu with 'w-' followed by a redacted ID, a refresh button, and a 'Create a new Workflow' button with an external link icon.
- Managed workflows execution role**: A subtitle 'Select the role that AWS Transfer Family should assume when executing a workflow'. It contains a dropdown menu with a redacted role name and a refresh button.

3. Pilih Simpan. Anda dikembalikan ke halaman detail Server.

Ubah spanduk tampilan untuk server Anda

Di AWS Transfer Family konsol, Anda dapat mengubah spanduk tampilan yang terkait dengan server.

Untuk mengubah spanduk tampilan

1. Pada halaman Detail Server, pilih Edit di samping Detail tambahan.
2. Pada halaman Edit detail tambahan, di bagian Tampilan spanduk, masukkan teks untuk spanduk tampilan yang tersedia.
3. Pilih Simpan. Anda dikembalikan ke halaman detail Server.

Menempatkan server Anda secara online atau offline

Di AWS Transfer Family konsol, Anda dapat membawa server Anda online atau membawanya offline.

Untuk membawa server Anda secara online

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.
3. Pilih kotak centang server yang sedang offline.
4. Untuk Tindakan, pilih Mulai.

Diperlukan beberapa menit bagi server untuk beralih dari offline ke online.

Note

Ketika Anda menghentikan server untuk membuatnya offline, saat ini Anda masih dikenakan biaya layanan untuk server itu. Untuk menghilangkan biaya berbasis server tambahan, hapus server itu.

Untuk membuat server Anda offline

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi, pilih Server.

3. Pilih kotak centang server yang sedang online.
4. Untuk Tindakan, pilih Berhenti.

Saat server memulai atau mematikan, server tidak tersedia untuk operasi file. Konsol tidak menampilkan status mulai dan berhenti.

Jika Anda menemukan kondisi kesalahan `START_FAILED` atau `STOP_FAILED`, hubungi AWS Dukungan untuk membantu menyelesaikan masalah Anda.

Edit konfigurasi penyedia identitas

Anda dapat mengubah jenis penyedia identitas server Anda dari jenis apa pun ke jenis lainnya. Jenis penyedia identitas yang tersedia adalah:

- Layanan dikelola - Simpan kredensial pengguna dalam layanan
- AWS Directory Service — Menggunakan Microsoft AD atau AWS Directory Service yang AWS Dikelola untuk Layanan Domain Entra ID
- Kustom - Gunakan fungsi Lambda atau Amazon API Gateway untuk berintegrasi dengan penyedia identitas yang ada

Saat mengubah jenis penyedia identitas, Anda perlu memberikan informasi spesifik tergantung pada transisi yang Anda buat. Bagian berikut menjelaskan informasi yang diperlukan untuk setiap jenis perubahan.

Important

Pertimbangan saat mengubah penyedia identitas:

- Migrasi pengguna — Saat mengubah jenis penyedia identitas, konfigurasi pengguna yang ada tidak dimigrasikan secara otomatis. Anda harus mengatur pengguna di sistem penyedia identitas baru.
- Pengujian - Uji konfigurasi penyedia identitas baru secara menyeluruh sebelum membuat perubahan di lingkungan produksi.
- Izin — Pastikan bahwa penyedia identitas baru memiliki izin dan peran IAM yang diperlukan yang dikonfigurasi sebelum melakukan perubahan.

Mengubah ke penyedia identitas yang dikelola layanan

Saat mengubah dari jenis penyedia identitas lain ke yang dikelola layanan, Anda perlu:

- Pilih Layanan yang dikelola sebagai tipe penyedia identitas
- Buat pengguna baru secara langsung AWS Transfer Family setelah perubahan selesai, karena konfigurasi pengguna yang ada dari penyedia identitas lain tidak akan ditransfer

Contoh: Jika Anda mengubah dari penyedia identitas kustom ke yang dikelola layanan, Anda harus membuat ulang semua akun pengguna dan izin terkait mereka dalam layanan. AWS Transfer Family

Mengubah ke AWS Directory Service

Saat mengubah dari jenis penyedia identitas lain ke AWS Directory Service, Anda perlu menyediakan:

- Direktori — Pilih AWS Managed Microsoft AD atau AWS Directory Service yang ada untuk direktori Entra ID Domain Services
- Akses — Pilih apakah akan membatasi akses ke grup tertentu atau mengizinkan akses ke semua pengguna di direktori
- Peran akses - Peran IAM yang memungkinkan AWS Transfer Family untuk mengakses direktori Anda

Contoh: Jika Anda mengubah dari service-managed ke AWS Directory Service, Anda akan memilih d-1234567890 direktori yang ada, memilih untuk membatasi akses ke TransferUsers grup, dan menentukan peran IAM. TransferDirectoryAccessRole

Mengubah ke penyedia identitas khusus

Saat mengubah dari jenis penyedia identitas lain ke penyedia identitas khusus, Anda harus memilih antara fungsi Lambda atau Amazon API Gateway dan menyediakan konfigurasi yang diperlukan:

Menggunakan fungsi Lambda

Untuk integrasi fungsi Lambda, berikan:

- Fungsi - Pilih fungsi Lambda yang ada yang menangani otentikasi
- Metode otentikasi (untuk protokol SFTP) - Pilih kata sandi, kunci publik, atau keduanya

Contoh: Jika Anda mengubah dari AWS Directory Service ke penyedia identitas Lambda kustom, Anda akan memilih `TransferCustomAuth` fungsi Anda dan memilih Kata Sandi sebagai metode otentikasi.

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

Mengubah ke penyedia identitas khusus

533

Menggunakan Amazon API Gateway

Untuk integrasi Amazon API Gateway, berikan:

- API Gateway URL — URL pemanggilan titik akhir API Gateway Anda
- Peran pemanggilan - Peran IAM yang memungkinkan AWS Transfer Family untuk memanggil API Gateway Anda
- Metode otentikasi (untuk protokol SFTP) - Pilih kata sandi, kunci publik, atau keduanya

Contoh: Jika Anda mengubah dari yang dikelola layanan ke API Gateway, Anda akan memberikan URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, menentukan peran `TransferApiGatewayInvocationRole` IAM, dan memilih kunci Publik sebagai metode otentikasi.

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

[Refresh](#)

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

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

Cancel Save

Mengubah dari Amazon API Gateway ke fungsi Lambda

Transisi umum berubah dari Amazon API Gateway ke fungsi Lambda untuk integrasi penyedia identitas kustom. Perubahan ini memungkinkan Anda untuk menyederhanakan arsitektur Anda sambil mempertahankan logika otentikasi yang sama.

Pertimbangan utama untuk transisi ini:

- Fungsi yang sama, izin yang berbeda — Anda dapat menggunakan fungsi Lambda yang sama untuk API Gateway dan integrasi Lambda langsung, tetapi kebijakan sumber daya harus diperbarui.
- Persyaratan kebijakan sumber daya — Saat mengubah integrasi Lambda langsung, kebijakan sumber daya fungsi harus memberikan `transfer.amazonaws.com` izin untuk menjalankan fungsi, sebagai tambahan. `apigateway.amazonaws.com`

Untuk membuat perubahan ini

1. Perbarui kebijakan sumber daya fungsi Lambda Anda `transfer.amazonaws.com` untuk memungkinkan menjalankan fungsi.
2. Di AWS Transfer Family konsol, ubah penyedia identitas dari API Gateway ke fungsi Lambda.
3. Pilih fungsi Lambda yang ada.
4. Uji konfigurasi untuk memastikan otentikasi berfungsi dengan benar.

Contoh kebijakan sumber daya untuk integrasi Lambda langsung:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Pelestarian pengguna selama transisi penyedia identitas

Saat mengubah di antara jenis penyedia identitas, konfigurasi pengguna yang ada dipertahankan dalam skenario tertentu untuk memungkinkan rollback yang efisien jika terjadi masalah:

- Service-managed ke penyedia identitas kustom dan kembali — Jika Anda mengubah dari penyedia identitas khusus yang dikelola layanan ke penyedia identitas khusus dan kemudian kembali ke layanan yang dikelola, semua pengguna dipertahankan dalam konfigurasi terakhir mereka yang diketahui.
- AWS Directory Service ke penyedia identitas kustom dan kembali — Jika Anda mengubah dari AWS Directory Service ke penyedia identitas khusus dan kemudian kembali ke AWS Directory Service, semua definisi untuk grup Akses Delegasi dipertahankan dalam konfigurasi terakhir yang diketahui.

Perilaku pelestarian ini memungkinkan Anda menguji konfigurasi penyedia identitas kustom dengan aman dan memutar kembali ke pengaturan sebelumnya tanpa kehilangan konfigurasi akses pengguna.

Pertimbangan penting saat mengganti penyedia identitas

- Migrasi pengguna — Saat mengubah jenis penyedia identitas, konfigurasi pengguna yang ada tidak dimigrasikan secara otomatis. Anda harus mengatur pengguna di sistem penyedia identitas baru.
- Pengujian - Uji konfigurasi penyedia identitas baru secara menyeluruh sebelum membuat perubahan di lingkungan produksi.
- Izin — Pastikan bahwa penyedia identitas baru memiliki izin dan peran IAM yang diperlukan yang dikonfigurasi sebelum melakukan perubahan.

Kelola kunci host untuk SFTP-enabled server Anda

Kunci host server adalah kunci pribadi yang digunakan oleh server Transfer Family untuk memberikan identitas unik kepada penelepon, dan untuk menjamin bahwa itu adalah server yang benar. Jaminan itu diberlakukan dengan adanya kunci publik yang benar dalam file penelepon. `known_hosts` (`known_hostsFile` ini adalah fitur standar yang digunakan oleh sebagian besar klien SSH untuk menyimpan kunci publik untuk server yang telah Anda sambungkan.) Anda dapat

mengambil kunci publik yang sesuai dengan kunci host server Anda dengan menjalankan ssh-keyscan server Anda.

 Important

Mengubah kunci host server secara tidak sengaja dapat mengganggu. Bergantung pada bagaimana klien SFTP Anda dikonfigurasi, klien dapat langsung gagal, dengan pesan bahwa tidak ada kunci host tepercaya, atau menyajikan petunjuk yang mengancam. Jika ada skrip untuk mengotomatisasi koneksi, kemungkinan besar akan gagal juga.

Secara default, AWS Transfer Family menghasilkan kunci host untuk SFTP-enabled server Anda. Anda dapat mengimpor kunci host server untuk mempertahankan identitas host dan menghindari memperbarui toko kepercayaan klien. [Kapan harus mengimpor kunci host](#) daftar beberapa alasan Anda mungkin ingin melakukan ini. Jika Anda tidak memberikan kunci host, yang baru akan dibuat untuk Anda.

AWS Transfer Family mendukung beberapa kunci host dari berbagai jenis (RSA, ECDSA, dan ED25519) untuk memberikan kompatibilitas dengan berbagai algoritma tanda tangan host klien yang lebih luas. Jenis kunci yang berbeda memungkinkan algoritme tertentu: Kunci RSA mengaktifkan algoritma rsa-*, kunci ECDSA mengaktifkan algoritma ecdsa-*, dan kunci ED25519 mengaktifkan algoritme ed25519. Rencanakan jenis kunci Anda pada waktu pembuatan server, karena memperkenalkan jenis kunci tambahan setelah klien mulai berinteraksi dengan server dapat mengganggu beberapa klien dan mungkin sama bermasalahnya dengan mengganti kunci host yang ada.

Untuk mencegah pengguna diminta untuk memverifikasi keaslian SFTP-enabled server Anda lagi, impor kunci host untuk server lokal Anda ke server. SFTP-enabled Melakukan hal ini juga mencegah pengguna Anda mendapatkan peringatan tentang potensi serangan man-in-the-middle.

Anda juga dapat memutar kunci host secara berkala, sebagai langkah keamanan tambahan. Lihat perinciannya di [Putar kunci host server](#).

 Note

Kunci host server digunakan oleh server yang mendukung protokol SFTP.

Kapan harus mengimpor kunci host

Meskipun AWS Transfer Family dapat menghasilkan kunci host secara otomatis, ada beberapa skenario di mana mengimpor kunci host Anda sendiri memberikan manfaat operasional:

- Migrasi server - Anda bermigrasi dari server yang ada ke AWS Transfer Family dan ingin menghindari memperbarui penyimpanan kepercayaan klien (`known_hostsfile`) untuk klien yang ada.
- Pemulihan bencana dan failover - Anda memiliki beberapa AWS Transfer Family server (misalnya, satu di AS Timur (Ohio) dan satu di AS Barat (Oregon)) yang memiliki nama DNS publik yang sama. Menggunakan kunci host yang sama di kedua server memastikan failover mulus tanpa kegagalan otentikasi klien.
- Kontinuitas operasional - Anda ingin materi kunci host tersedia untuk digunakan dengan server lain (AWS Transfer Family atau sebaliknya) di masa depan untuk mempertahankan identitas server yang konsisten di seluruh infrastruktur Anda.
- Kontrol algoritma - Anda menginginkan kompatibilitas klien yang lebih besar dengan menyediakan lebih banyak Algoritma Kunci Host, atau Anda ingin mengontrol algoritma mana yang dapat digunakan klien dengan hanya menawarkan kunci yang kompatibel dengan algoritme tertentu.

Topik berikut memberikan prosedur terperinci untuk mengelola kunci host server:

- [Tambahkan kunci host server tambahan](#)- Tambahkan kunci host tambahan ke server Anda
- [Hapus kunci host server](#)- Hapus kunci host dari server Anda
- [Putar kunci host server](#)- Putar kunci host untuk keamanan yang ditingkatkan
- [Informasi kunci host server tambahan](#)- Lihat dan kelola detail kunci host

Tambahkan kunci host server tambahan

Di AWS Transfer Family konsol, Anda dapat menambahkan kunci host server tambahan.

Menambahkan kunci host tambahan dari format yang berbeda dapat berguna untuk mengidentifikasi server ketika klien terhubung dengannya, serta meningkatkan profil keamanan Anda. Misalnya, jika kunci asli Anda adalah kunci RSA, Anda dapat menambahkan kunci ECDSA tambahan.

Note

Klien SFTP akan terhubung menggunakan kunci tertua dalam konfigurasi yang cocok dengan algoritma kunci. Kunci tertua untuk setiap jenis kunci (RSA, ECDSA, atau ED25519) adalah kunci aktif untuk server untuk jenis itu.

Catatan keamanan ketika server Transfer Family memiliki beberapa jenis kunci host

Jika server memiliki beberapa jenis kunci host, klien SFTP dapat menetapkan preferensi berdasarkan jenis. Jadi, ketika ada kunci host RSA, ECDSA, dan ED25519 untuk server, pilihan didorong oleh preferensi berdasarkan jenis.

Klien SFTP modern lebih memilih kunci host ECDSA dan ED25519 ketika ada. Ini menjadi penting jika Anda ingin menambahkan kunci ECDSA atau ED25519 ketika server sebelumnya hanya memiliki kunci RSA. Penambahan kunci ECDSA atau ED25519 baru berpotensi bermanifestasi sebagai peringatan keamanan untuk klien.

Untuk klien, kunci akan muncul sebagai telah berubah, padahal sebenarnya itu tidak berubah: kunci baru ditambahkan selain kunci RSA yang ada. Ingatlah hal ini jika Anda memutuskan untuk menambahkan jenis kunci host server baru.

Untuk menambahkan kunci host server tambahan

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Di panel navigasi kiri, pilih Server, lalu pilih server yang menggunakan protokol SFTP.
3. Pada halaman detail server, gulir ke bawah ke bagian Kunci host Server.

Server host keys (2)

ActionsAdd host key

Find resources

☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

4. Pilih Tambahkan kunci host.

Halaman kunci Add server host ditampilkan.

5. Di bagian Server Host Key, masukkan kunci pribadi RSA, ECDSA, atau ED25519 yang digunakan untuk mengidentifikasi server Anda ketika klien terhubung ke server. SFTP-enabled

Note

Saat Anda membuat kunci host server, pastikan untuk menentukan `-N ""` (tidak ada frasa sandi). Lihat [Membuat kunci SSH di macOS, Linux, atau Unix](#) untuk detail tentang cara menghasilkan pasangan kunci.

- (Opsional) Tambahkan deskripsi untuk membedakan antara beberapa kunci host server. Anda juga dapat menambahkan tag untuk kunci Anda.
- Pilih Tambah kunci. Anda dikembalikan ke halaman detail Server.

Untuk menambahkan kunci host dengan menggunakan AWS Command Line Interface (AWS CLI), gunakan operasi [ImportHostKey](#) API dan berikan kunci host baru. Jika Anda membuat SFTP-enabled server baru, Anda memberikan kunci host sebagai parameter dalam operasi [CreateServer](#) API. Anda juga dapat menggunakan AWS CLI untuk memperbarui deskripsi untuk kunci host yang ada.

Contoh `import-host-key` AWS CLI perintah berikut mengimpor kunci host untuk SFTP-enabled server tertentu.

```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

Hapus kunci host server

Di AWS Transfer Family konsol, Anda dapat menghapus kunci host server.

Untuk menghapus kunci host server

- Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
- Di panel navigasi kiri, pilih Server, lalu pilih server yang menggunakan protokol SFTP.
- Pada halaman detail server, gulir ke bawah ke bagian Kunci host Server.

Server host keys (2)							Actions ▾	Add host key
Find resources							< 1 >	
☐	Name ↗	Host key ID ▾	Fingerprint Info	Description ▾	Key type ▾	Date imported ▾		
☐	Default host key	hostkey-██████████	SHA256:██████████	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-██████████	SHA256:██████████	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

- Di bagian Server Host Keys, pilih kunci, dan kemudian di bawah Tindakan, pilih Hapus.

5. Di kotak dialog konfirmasi yang muncul, masukkan kata **delete**, lalu pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus kunci host.

Kunci host dihapus dari halaman Server.

Untuk menghapus kunci host dengan menggunakan AWS CLI, gunakan operasi [DeleteHostKey](#) API dan berikan ID server dan ID kunci host.

Contoh `delete-host-key` AWS CLI perintah berikut menghapus kunci host untuk SFTP-enabled server tertentu.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Putar kunci host server

Secara berkala, Anda dapat memutar kunci host server Anda. Topik ini menjelaskan bagaimana server memilih kunci mana yang akan diterapkan, dan prosedur untuk memutar kunci ini.

Bagaimana klien memilih kunci host server

Cara Transfer Family memilih kunci server mana yang akan diterapkan tergantung pada kondisi untuk klien SFTP, seperti yang dijelaskan di sini. Asumsinya adalah bahwa ada satu kunci lama dan satu kunci yang lebih baru.

- Klien SFTP tidak memiliki kunci host publik sebelumnya untuk server. Pertama kali klien terhubung ke server, salah satu dari berikut ini terjadi:
 - Klien gagal koneksi, jika dikonfigurasi untuk melakukannya.
 - Atau, klien memilih kunci pertama yang cocok dengan algoritme yang mungkin tersedia dan bertanya kepada pengguna apakah kunci itu dapat dipercaya. Jika demikian, klien memperbarui file secara otomatis (atau `known_hosts` file konfigurasi lokal atau sumber daya apa pun yang digunakan klien untuk merekam keputusan kepercayaan) dan memasukkan kunci itu.
- Klien SFTP memiliki kunci yang lebih lama dalam file-nya `known_hosts`. Klien lebih suka menggunakan kunci ini, bahkan jika ada kunci yang lebih baru, baik untuk algoritma kunci ini atau algoritma lain. Ini karena klien memiliki tingkat kepercayaan yang lebih tinggi untuk kunci yang ada di `known_hosts` file-nya.
- Klien SFTP memiliki kunci baru (dalam salah satu algoritma yang tersedia) dalam file `known_hosts`. Klien mengabaikan kunci lama karena tidak dipercaya dan menggunakan kunci baru.

- Klien SFTP memiliki kedua kunci dalam file-nyaknown_hosts. Klien memilih kunci pertama berdasarkan indeks yang cocok dengan daftar kunci yang tersedia yang ditawarkan oleh server.

Transfer Family lebih suka klien SFTP memiliki semua kunci dalam known_hosts file-nya, karena ini memungkinkan fleksibilitas paling besar saat menghubungkan ke server Transfer Family. Rotasi kunci didasarkan pada fakta bahwa beberapa entri dapat ada dalam known_hosts file untuk server Transfer Family yang sama.

Putar prosedur kunci host server

Sebagai contoh, asumsikan bahwa Anda telah menambahkan set kunci host server berikut ke server Transfer Family Anda.

Kunci host server

Jenis kunci host	Tanggal ditambahkan ke server
RSA	1 April 2020
ECDSA	Februari 1, 2020
ED25519	1 Desember, 2019
RSA	1 Oktober 2019
ECDSA	1 Juni 2019
ED25519	Maret 1, 2019

Untuk memutar kunci host server

1. Tambahkan kunci host server baru. Prosedur ini dijelaskan dalam [Tambahkan kunci host server tambahan](#).
2. Hapus satu atau beberapa kunci host dari jenis yang sama yang telah Anda tambahkan sebelumnya. Prosedur ini dijelaskan dalam [Hapus kunci host server](#).
3. Semua kunci terlihat, dan dapat aktif, tunduk pada perilaku yang dijelaskan sebelumnya di [Bagaimana klien memilih kunci host server](#).

Informasi kunci host server tambahan

Anda dapat memilih kunci host untuk menampilkan detail kunci tersebut.

Transfer Family > Servers > s-3fe215d89f074ed2a > Hostkey: hostkey-a6fed60bcb704ea9b

hostkey-a6fed60bcb704ea9b

Delete

Host key configuration

Edit

Name

ecdsa-521

Fingerprint

SHA256: [redacted]

Description

ECDSA host key

Key type

ecdsa-sha2-nistp521

Date imported

Thu, 13 Jun 2024 17:08:59 GMT

Amazon Resource Name (ARN)

arn:aws:transfer:us-east-1:[redacted]:host-key/[redacted]/hostkey-a-[redacted]

Anda dapat menghapus kunci host, atau mengedit deskripsinya dari menu Tindakan di layar Detail Server. Pilih tombol host, lalu pilih tindakan yang sesuai dari menu.

Server host keys (2)

Find resources

Actions

Edit

Delete

Add host key

< 1 >

	Name	Host key ID	Fingerprint	Description	Key type	Date imported
	Default host key	hostkey-[redacted]	SHA256:[redacted]	Default	ssh-rsa	2023-06-30
	ecdsa-521	hostkey-[redacted]	SHA256:[redacted]	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

Memantau penggunaan di konsol

Anda bisa mendapatkan informasi tentang metrik server Anda di halaman detail Servernya. Ini memberi Anda satu tempat untuk memantau beban kerja transfer file Anda. Anda dapat melacak berapa banyak file yang telah Anda tukarkan dengan mitra Anda dan melacak penggunaannya dengan cermat menggunakan dasbor terpusat. Lihat perinciannya di [Lihat detail server SFTP, FTPS, dan FTP](#). Tabel berikut menjelaskan metrik yang tersedia untuk Transfer Family.

Namespace	Metrik	Deskripsi
AWS/Transfer	BytesIn	Jumlah total byte yang ditransfer ke server.
Kriteria pelaporan:		

Namespace	Metrik	Deskripsi
		• Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses Unit: Hitung Periode: 5 menit
	BytesOut	Jumlah total byte yang ditransfer keluar dari server. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menelepon <code>StartFileTransfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses. Unit: Hitung Periode: 5 menit

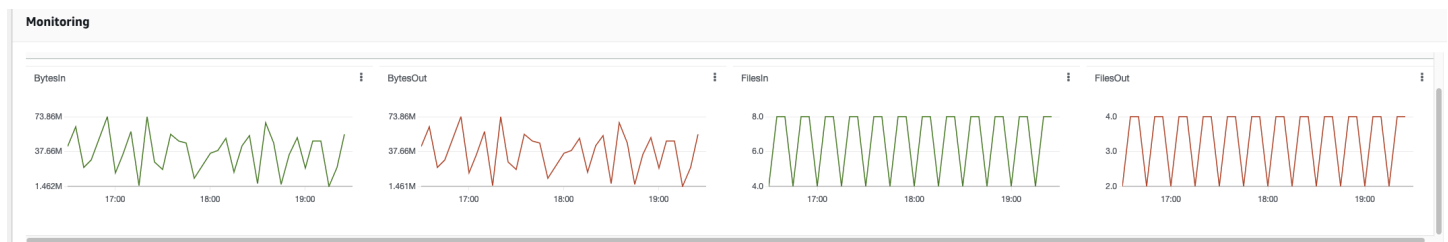
Namespace	Metrik	Deskripsi
	FilesIn	Jumlah total file yang ditransfer ke server. Untuk server yang menggunakan protokol AS2, metrik ini mewakili jumlah pesan yang diterima. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses. Unit: Hitung Periode: 5 menit
	FilesOut	Jumlah total file yang ditransfer keluar dari server. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menelepon StartFile Transfer dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses. Unit: Hitung Periode: 5 menit

Namespace	Metrik	Deskripsi
	InboundMessage	Jumlah total pesan AS2 yang berhasil diterima dari mitra dagang. Kriteria pelaporan: Ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses dengan sukses Unit: Hitung Periode: 5 menit
	InboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil diterima dari mitra dagang. Artinya, mitra dagang mengirim pesan, tetapi server Transfer Family tidak berhasil memprosesnya. Kriteria pelaporan: Ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses tidak berhasil Unit: Hitung Periode: 5 menit
	OnUploadExecutionsStarted	Jumlah total eksekusi alur kerja dimulai di server. Kriteria pelaporan: Dipicu setiap kali eksekusi dimulai Unit: Hitung Periode: 1 menit

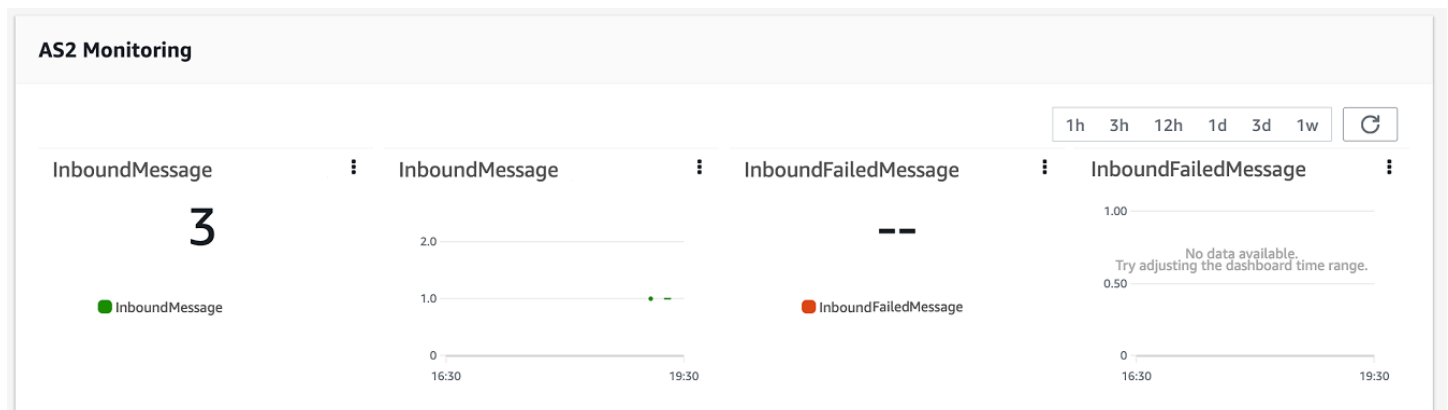
Namespace	Metrik	Deskripsi
	OnUploadExecutionsSuccess	Jumlah total eksekusi alur kerja yang berhasil di server. Kriteria pelaporan: Dipicu setiap kali eksekusi berhasil selesai Unit: Hitung Periode: 1 menit
	OnUploadExecutionsFailed	Jumlah total eksekusi alur kerja yang gagal di server. Kriteria pelaporan: Dipicu setiap kali eksekusi tidak berhasil diselesaikan Unit: Hitung Periode: 1 menit
	OutboundMessage	Jumlah total pesan AS2 yang berhasil dikirim ke mitra dagang. Kriteria pelaporan: Ketika pelanggan menelepon <code>StartFileTransfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses dengan sukses Unit: Hitung Periode: 5 menit

Namespace	Metrik	Deskripsi
	OutboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil dikirim ke mitra dagang. Kriteria pelaporan: Ketika pelanggan menelepon <code>StartFileTransfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses tidak berhasil Unit: Hitung Periode: 5 menit

Bagian Monitoring berisi empat grafik individual. Grafik ini menunjukkan byte masuk, byte keluar, file masuk, dan file keluar.



Untuk server yang memiliki protokol AS2 diaktifkan, ada bagian Pemantauan AS2 di bawah informasi Pemantauan. Bagian ini berisi detail untuk jumlah pesan masuk, baik yang berhasil maupun yang gagal.



Untuk membuka grafik yang dipilih di jendelanya sendiri, pilih ikon perluas



).

Anda juga dapat mengklik ikon elipsis vertikal grafik



)

untuk membuka menu tarik-turun dengan item berikut:

- Memperbesar — Membuka grafik yang dipilih di jendelanya sendiri.
- Refresh — Muat ulang grafik dengan data terbaru.
- Lihat dalam metrik — Membuka detail metrik yang sesuai di Amazon. CloudWatch
- Lihat log - Membuka grup log yang sesuai di CloudWatch.

Mengelola kontrol akses

Anda dapat mengontrol akses pengguna ke AWS Transfer Family sumber daya dengan menggunakan kebijakan AWS Identity and Access Management (IAM). Kebijakan IAM adalah pernyataan, biasanya dalam format JSON, yang memungkinkan tingkat akses tertentu ke sumber daya. Anda menggunakan kebijakan IAM untuk menentukan operasi file apa yang Anda ingin mengizinkan pengguna Anda untuk melakukan dan tidak melakukan. Anda juga dapat menggunakan kebijakan IAM untuk menentukan bucket atau bucket Amazon S3 yang ingin Anda akses kepada pengguna. Untuk menentukan kebijakan ini bagi pengguna, Anda membuat peran IAM AWS Transfer Family yang memiliki kebijakan IAM dan hubungan kepercayaan yang terkait dengannya.

Setiap pengguna diberi peran IAM. Jenis peran IAM yang AWS Transfer Family digunakan disebut peran layanan. Saat pengguna masuk ke server Anda, AWS Transfer Family asumsikan peran IAM yang dipetakan ke pengguna. Untuk mempelajari cara membuat peran IAM yang menyediakan akses pengguna ke bucket Amazon S3, [lihat Membuat peran untuk mendelegasikan izin ke AWS](#) layanan di Panduan Pengguna IAM.

Anda dapat memberikan akses hanya tulis ke objek Amazon S3 dengan menggunakan izin tertentu dalam kebijakan IAM. Lihat perinciannya di [Memberikan kemampuan untuk hanya menulis dan membuat daftar file](#).

Blog AWS Penyimpanan berisi posting yang merinci cara mengatur akses hak istimewa paling sedikit. Untuk detailnya, lihat [Menerapkan akses hak istimewa terkecil dalam AWS Transfer Family alur kerja](#).

Note

Jika bucket Amazon S3 dienkripsi menggunakan AWS Key Management Service (AWS KMS), Anda harus menentukan izin tambahan dalam kebijakan Anda. Lihat perinciannya di [Perlindungan data dan enkripsi](#). Selain itu, Anda dapat melihat informasi selengkapnya tentang [kebijakan sesi](#) di Panduan Pengguna IAM.

Topik

- [Mengizinkan akses baca dan tulis ke bucket Amazon S3](#)
- [Membuat kebijakan sesi untuk bucket Amazon S3](#)

- [Pendekatan manajemen izin dinamis](#)

Mengizinkan akses baca dan tulis ke bucket Amazon S3

Bagian ini menjelaskan cara membuat kebijakan IAM yang memungkinkan akses baca dan tulis ke bucket Amazon S3 tertentu. Menetapkan peran IAM yang memiliki kebijakan IAM ini kepada pengguna Anda memberi pengguna tersebut read/write akses ke bucket Amazon S3 yang ditentukan.

Kebijakan berikut menyediakan akses baca, tulis, dan penandaan terprogram ke bucket Amazon S3. PutObjectACL Pernyataan GetObjectACL dan pernyataan hanya diperlukan jika Anda perlu mengaktifkan Akses Lintas Akun. Artinya, server Transfer Family Anda perlu mengakses bucket di akun yang berbeda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

```
]
}
```

ListBucketTindakan tersebut membutuhkan izin untuk ember itu sendiri.

DELETETindakanPUT,GET, dan memerlukan izin objek. Karena ini adalah sumber daya yang berbeda, mereka ditentukan menggunakan Nama Sumber Daya Amazon (ARN) yang berbeda.

Untuk lebih membatasi akses pengguna hanya ke home awalan bucket Amazon S3 yang ditentukan, lihat. [Membuat kebijakan sesi untuk bucket Amazon S3](#)

Membuat kebijakan sesi untuk bucket Amazon S3

Kebijakan sesi adalah kebijakan AWS Identity and Access Management (IAM) yang membatasi pengguna pada bagian tertentu dari bucket Amazon S3. Ia melakukannya dengan mengevaluasi akses secara real time.

Note

Kebijakan sesi hanya digunakan dengan Amazon S3. Untuk Amazon EFS, Anda menggunakan izin file POSIX untuk membatasi akses.

Anda dapat menggunakan kebijakan sesi saat Anda perlu memberikan akses yang sama ke sekelompok pengguna ke bagian tertentu dari bucket Amazon S3 Anda. Misalnya, sekelompok pengguna mungkin hanya memerlukan akses ke home direktori. Kelompok pengguna itu berbagi peran IAM yang sama.

Note

Panjang maksimum kebijakan sesi adalah 2048 karakter. Untuk detail selengkapnya, lihat [parameter Permintaan kebijakan](#) untuk CreateUser tindakan dalam referensi API.

Untuk membuat kebijakan sesi, gunakan variabel kebijakan berikut dalam kebijakan IAM Anda:

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`

- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

Anda tidak dapat menggunakan variabel sebelumnya dalam Kebijakan Terkelola. Anda juga tidak dapat menggunakannya sebagai variabel kebijakan dalam definisi peran IAM. Anda membuat variabel-variabel ini dalam kebijakan IAM dan menyediakannya secara langsung saat menyiapkan pengguna Anda. Selain itu, Anda tidak dapat menggunakan `${aws:Username}` variabel dalam kebijakan sesi ini. Variabel ini mengacu pada nama pengguna IAM dan bukan nama pengguna yang diperlukan oleh AWS Transfer Family.

Contoh kebijakan sesi

Kode berikut menunjukkan contoh kebijakan sesi.

```
{
  "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

Contoh kebijakan sebelumnya mengasumsikan bahwa pengguna memiliki direktori home mereka diatur untuk menyertakan garis miring, untuk menandakan bahwa itu adalah direktori. Jika, di sisi lain, Anda menetapkan pengguna HomeDirectory tanpa garis miring, maka Anda harus memasukkannya sebagai bagian dari kebijakan Anda.

Dalam contoh kebijakan sebelumnya, perhatikan penggunaan parameter `transfer:HomeFolder`, `transfer:HomeBucket`, dan `transfer:HomeDirectory` kebijakan. Parameter ini diatur untuk HomeDirectory yang dikonfigurasi untuk pengguna, seperti yang dijelaskan dalam [HomeDirectory](#) dan [Menerapkan metode API Gateway Anda](#). Parameter ini memiliki definisi berikut:

- `transfer:HomeBucketParameter` diganti dengan komponen pertama dari `HomeDirectory`.
- `transfer:HomeFolderParameter` diganti dengan bagian `HomeDirectory` parameter yang tersisa.
- `transfer:HomeDirectoryParameter` memiliki garis miring depan (/) yang dihapus sehingga dapat digunakan sebagai bagian dari Nama Sumber Daya Amazon S3 (ARN) dalam sebuah pernyataan. Resource

Note

Jika Anda menggunakan direktori logik—yaitu, pengguna adalah LOGICAL —parameter kebijakan ini (`HomeBucket`, `HomeDirectory`, dan `HomeFolder`) tidak didukung.

`homeDirectoryType`

Misalnya, asumsikan bahwa `HomeDirectory` parameter yang dikonfigurasi untuk pengguna Transfer Family adalah `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` diatur ke `/home`.
- `transfer:HomeFolder` diatur ke `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` menjadi `home/bob/amazon/stuff/`.

Yang pertama "Sid" memungkinkan pengguna untuk membuat daftar semua direktori mulai dari `/home/bob/amazon/stuff/`.

Yang kedua "Sid" membatasi pengguna put dan get akses ke jalur yang sama, `/home/bob/amazon/stuff/`.

Dengan kebijakan sebelumnya, saat pengguna masuk, mereka hanya dapat mengakses objek di direktori home mereka. Pada waktu koneksi, AWS Transfer Family ganti variabel-variabel ini dengan nilai yang sesuai untuk pengguna. Melakukan hal ini memudahkan penerapan dokumen kebijakan yang sama ke beberapa pengguna. Pendekatan ini mengurangi overhead peran IAM dan manajemen kebijakan untuk mengelola akses pengguna ke bucket Amazon S3 Anda.

Anda juga dapat menggunakan kebijakan sesi untuk menyesuaikan akses untuk setiap pengguna berdasarkan kebutuhan bisnis Anda. Untuk informasi selengkapnya, lihat [Izin untuk AssumeRole](#), [AssumeRoleWithSAML](#), dan [AssumeRoleWithWebIdentity](#) di Panduan Pengguna IAM.

Note

AWS Transfer Family menyimpan kebijakan JSON, bukan Nama Sumber Daya Amazon (ARN) kebijakan. Jadi, ketika Anda mengubah kebijakan di konsol IAM, Anda harus kembali ke AWS Transfer Family konsol dan memperbarui pengguna Anda dengan konten kebijakan terbaru. Anda dapat memperbarui pengguna pada tab Info Kebijakan di bagian Konfigurasi pengguna.

Jika Anda menggunakan AWS CLI, Anda dapat menggunakan perintah berikut untuk memperbarui kebijakan.

```
aws transfer update-user --server-id server --user-name user --policy \  
    "$(aws iam get-policy-version --policy-arn policy --version-id version --  
    output json)"
```

Substitusi bersarang untuk kebijakan sesi

Substitusi bersarang tidak dilakukan dalam kebijakan sesi Transfer Family. Kebijakan sesi dapat menggunakan variabel bersarang, seperti `${transfer:HomeDirectory}`. Ketika kebijakan diproses, variabel luar (misalnya, `${transfer:HomeDirectory}`) mungkin diganti dengan nilai yang berisi variabel lain (misalnya, `{amzn-s3-demo-bucket}/${transfer:UserName}`). Namun, variabel bersarang tidak diganti lebih lanjut dengan nama pengguna yang sebenarnya (misalnya, johndoe).

Ini berarti bahwa saat membuat kebijakan sesi untuk Transfer Family, Anda perlu memperhitungkan perilaku ini dan memastikan bahwa struktur kebijakan dan penggunaan variabel dirancang sesuai dengan itu. Variabel bersarang mungkin tidak diselesaikan seperti yang diharapkan, dan kebijakan mungkin tidak memberikan izin yang dimaksudkan. Sangat penting untuk menguji dan memvalidasi kebijakan sesi secara menyeluruh untuk memastikan mereka bekerja seperti yang diharapkan. Perilaku ini menjadi pertimbangan utama saat menerapkan kontrol akses dan izin untuk lingkungan Transfer Family Anda.

Salah satu solusi untuk masalah ini adalah dengan menggunakan nama bucket Amazon S3 yang sebenarnya dalam kebijakan sesi Anda. Jadi, misalnya, daripada menentukan `${transfer:HomeDirectory}` dalam kebijakan sesi Anda, gunakan yang berikut ini, di mana `amzn-s3-demo-bucket` adalah bucket Anda yang sebenarnya: `${amzn-s3-demo-bucket}/${transfer:UserName}`

Pendekatan manajemen izin dinamis

Memahami arsitektur izin Transfer Family

AWS Transfer Family mendukung manajemen izin dinamis melalui kebijakan sesi, yang memungkinkan Anda membatasi izin efektif peran IAM saat runtime. Pendekatan ini berfungsi untuk

pengguna yang dikelola layanan dan pengguna penyedia identitas khusus, tetapi hanya didukung saat mentransfer file ke atau dari Amazon S3 (bukan Amazon EFS).

Setiap AWS Transfer Family pengguna beroperasi dengan model izin yang terdiri dari:

1. Peran IAM dasar - Mendefinisikan izin dasar untuk pengguna
2. Kebijakan sesi opsional - Membatasi (cakupan ke bawah) izin dasar saat runtime

Izin efektif adalah persimpangan izin peran dasar dan izin kebijakan sesi. Kebijakan sesi hanya dapat membatasi izin; mereka tidak dapat memberikan izin tambahan di luar apa yang diizinkan oleh peran dasar.

Arsitektur ini berlaku untuk kedua tipe pengguna:

- Service-managed pengguna - Kebijakan sesi dapat dikonfigurasi langsung di pengaturan pengguna
- Pengguna penyedia identitas kustom - Kebijakan sesi dapat dikembalikan sebagai bagian dari respons otentikasi atau disimpan di AWS Secrets Manager

Dua pendekatan untuk manajemen izin

Saat merancang izin untuk pengguna Transfer Family yang membutuhkan pola akses unik, Anda dapat memilih di antara dua pendekatan utama:

Satu peran per pengguna

Buat peran IAM terpisah untuk setiap pengguna Transfer Family dengan izin khusus yang disesuaikan dengan kebutuhan pengguna tersebut. Gunakan pendekatan ini ketika:

- Setiap pengguna memerlukan izin yang sangat berbeda
- Administrasi izin ditangani oleh orang yang berbeda di organisasi Anda
- Anda memerlukan kontrol halus atas akses pengguna individu

Peran bersama dengan kebijakan sesi

Gunakan satu peran IAM dengan izin luas (seperti akses ke seluruh bucket Amazon S3 yang berisi beberapa direktori home pengguna) dan terapkan kebijakan sesi untuk membatasi setiap pengguna ke area spesifik mereka. Pendekatan ini secara signifikan mengurangi overhead

administratif dibandingkan dengan mengelola peran terpisah untuk setiap pengguna. Gunakan pendekatan ini ketika:

- Pengguna membutuhkan jenis akses yang serupa tetapi ke sumber daya yang berbeda (misalnya, semua pengguna memerlukan read/write akses, tetapi masing-masing hanya ke folder mereka sendiri)
- Anda ingin menyederhanakan manajemen peran dan menghindari membuat lusinan atau ratusan peran individu
- Pengguna hanya boleh mengakses direktori beranda yang ditunjuk dalam bucket bersama
- Administrasi izin terpusat di dalam organisasi Anda

Misalnya, alih-alih membuat peran terpisah untuk pengguna “alice”, “bob”, dan “charlie”, Anda dapat membuat satu peran dengan akses ke seluruh `s3://company-transfers/` bucket, lalu menggunakan kebijakan sesi untuk membatasi alice ke `s3://company-transfers/alice/`, bob ke `s3://company-transfers/bob/`, dan sebagainya.

Menerapkan kebijakan sesi

Kebijakan sesi berfungsi dengan membatasi izin efektif dari peran IAM dasar yang ditetapkan kepada pengguna. Izin terakhir adalah persimpangan izin peran dan izin kebijakan sesi.

Anda dapat menerapkan kebijakan sesi dinamis dengan dua cara:

Substitusi variabel

Gunakan variabel kebijakan Transfer Family seperti `${transfer:Username}`, `${transfer:HomeDirectory}`, dan `${transfer:HomeBucket}` dalam kebijakan sesi Anda. Variabel ini secara otomatis diganti dengan nilai aktual saat runtime. Untuk informasi lebih lanjut tentang variabel-variabel ini, lihat [Membuat kebijakan sesi untuk bucket Amazon S3](#).

Generasi dinamis

Untuk penyedia identitas kustom, buat kebijakan sesi dengan cepat sebagai bagian dari respons autentikasi dari fungsi Lambda atau metode API Gateway Anda. Pendekatan ini memungkinkan Anda membuat kebijakan yang sangat disesuaikan berdasarkan atribut pengguna, keanggotaan grup, atau sumber data eksternal pada waktu otentikasi.

Anda juga dapat menyimpan kebijakan sesi yang telah dibuat sebelumnya AWS Secrets Manager dengan menyertakan kunci yang diberi nama `Policy` dengan kebijakan sesi JSON sebagai

nilainya. Ini memungkinkan Anda untuk menggunakan peran IAM luas yang sama di beberapa pengguna sambil mempertahankan kontrol akses khusus pengguna.

Note

Kebijakan sesi hanya didukung untuk transfer file ke dan dari Amazon S3. Mereka tidak berlaku untuk sistem file Amazon EFS. Untuk Amazon EFS, izin diatur oleh UID/GID dan bit izin diterapkan dalam sistem file itu sendiri.

Implementasi menurut tipe pengguna

Service-managed pengguna

Untuk pengguna yang dikelola layanan, Anda dapat menentukan kebijakan sesi secara langsung dalam konfigurasi pengguna melalui AWS Transfer Family konsol, API, atau CLI. Untuk informasi selengkapnya, lihat [Bekerja dengan pengguna yang dikelola layanan](#).

Pengguna penyedia identitas khusus

Untuk pengguna penyedia identitas kustom, Anda dapat memberikan kebijakan sesi dengan dua cara:

- Melalui AWS Secrets Manager dengan menyertakan kunci bernama `Policy` dengan kebijakan sesi sebagai nilai
- Langsung di respons fungsi Lambda atau respons API Gateway sebagai bagian dari hasil otentikasi

Untuk informasi selengkapnya, lihat [Solusi penyedia identitas khusus](#).

Contoh: Menyederhanakan manajemen peran dengan kebijakan sesi

Contoh ini menunjukkan bagaimana manajemen izin dinamis dapat secara signifikan mengurangi overhead administratif sambil menjaga keamanan.

Skenario

Organisasi Anda memiliki 50 pengguna yang memerlukan akses SFTP untuk mentransfer file. Setiap pengguna hanya boleh mengakses folder mereka sendiri dalam bucket Amazon S3 bersama yang disebut `company-transfers`. Tanpa kebijakan sesi, Anda perlu membuat 50 peran IAM terpisah.

Pendekatan tradisional (tanpa kebijakan sesi)

- Buat 50 peran IAM: `TransferRole-Alice`, `TransferRole-Bob`, `TransferRole-Charlie`, dll.
- Setiap peran memiliki izin khusus hanya untuk folder pengguna tersebut
- Mengelola izin memerlukan pembaruan peran individual
- Menambahkan pengguna baru membutuhkan pembuatan peran baru

Pendekatan dinamis (dengan kebijakan sesi)

- Buat 1 peran IAM: `TransferRole-Shared` dengan izin luas ke seluruh bucket
- Gunakan kebijakan sesi untuk membatasi setiap pengguna ke folder spesifik mereka saat runtime
- Mengelola izin memerlukan pembaruan satu peran atau templat kebijakan sesi
- Menambahkan pengguna baru tidak memerlukan peran baru, hanya konfigurasi pengguna

Implementasi

Inilah cara Anda menerapkan pendekatan dinamis (menggunakan `company-transfers` bucket sebagai contoh untuk diganti dengan bucket Amazon S3 Anda yang sebenarnya):

Untuk menerapkan manajemen izin dinamis

1. Buat satu peran IAM bersama dengan izin Amazon S3 yang luas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
```

```

    "Resource": "arn:aws:s3:::company-transfers"
  }
]
}

```

2. Buat templat kebijakan sesi yang membatasi akses ke folder pengguna:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${transfer:Username}*"
        }
      }
    }
  ]
}

```

3. Konfigurasi setiap pengguna dengan:

- Peran IAM bersama
- Kebijakan sesi diterapkan sebagai berikut:
 - Service-managed pengguna: Gunakan API atau CLI untuk menerapkan JSON melalui parameter Kebijakan saat membuat atau memodifikasi pengguna (konsol hanya menawarkan opsi kebijakan yang telah ditentukan sebelumnya)

- Pengguna penyedia identitas khusus: Baik mengembalikannya sebagai bagian dari respons fungsi Lambda selama autentikasi, atau simpan AWS Secrets Manager sebagai kunci bernama “Kebijakan” di samping kredensial pengguna
- Direktori rumah: `/company-transfers/${transfer:Username}/`

AWS CloudTrail penebangan untuk AWS Transfer Family

AWS Transfer Family terintegrasi dengan keduanya AWS CloudTrail dan Amazon CloudWatch. CloudTrail dan CloudWatch melayani tujuan yang berbeda tetapi saling melengkapi.

- Topik ini mencakup integrasi dengan CloudTrail, AWS layanan yang membuat catatan tindakan yang diambil dalam diri Anda Akun AWS. Ini terus memantau dan merekam operasi API untuk aktivitas seperti login konsol, AWS Command Line Interface perintah, dan SDK/API operasi. Ini memungkinkan Anda untuk menyimpan log siapa yang mengambil tindakan apa, kapan, dan dari mana. CloudTrail membantu audit, manajemen akses, dan kepatuhan terhadap peraturan dengan memberikan riwayat semua aktivitas di AWS lingkungan Anda. Untuk detailnya, lihat [Panduan AWS CloudTrail Pengguna](#).
- [Amazon CloudWatch logging untuk AWS Transfer Family server](#) mencakup integrasi dengan CloudWatch, layanan pemantauan untuk AWS sumber daya dan aplikasi. Ini mengumpulkan metrik dan log untuk memberikan visibilitas ke pemanfaatan sumber daya, kinerja aplikasi, dan kesehatan sistem secara keseluruhan. CloudWatch membantu tugas operasional seperti pemecahan masalah, pengaturan alarm, dan penskalaan otomatis. Untuk detailnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari operasi API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Transfer Family, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)

- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Semua AWS Transfer Family tindakan dicatat oleh CloudTrail dan didokumentasikan dalam [ActionsAPI reference](#). Misalnya, panggilan ke `CreateServer`, `ListUsers` dan `StopServer` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan root atau kredensi AWS Identity and Access Management pengguna.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk AWS Transfer Family. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Transfer Family, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Topik

- [Aktifkan AWS CloudTrail pencatatan](#)
- [Contoh entri log untuk membuat server](#)
- [Contoh log akses data](#)

Aktifkan AWS CloudTrail pencatatan

Anda dapat memantau operasi AWS Transfer Family API menggunakan AWS CloudTrail. Dengan memantau operasi API, Anda bisa mendapatkan informasi keamanan dan operasional yang berguna. Jika Anda [mengaktifkan pencatatan level objek Amazon S3](#), RoleSessionName terdapat dalam bidang Peminta sebagai. [AWS:Role Unique Identifier]/username.sessionid@server-id Untuk informasi selengkapnya tentang pengidentifikasi unik peran AWS Identity and Access Management (IAM), lihat [Pengidentifikasi unik di Panduan](#) Pengguna.AWS Identity and Access Management

Important

Panjang maksimum RoleSessionName adalah 64 karakter. Jika RoleSessionName lebih panjang, server-id akan terpotong.

Mengaktifkan peristiwa data Amazon S3

Untuk melacak operasi file yang dilakukan melalui AWS Transfer Family bucket Amazon S3, Anda perlu mengaktifkan peristiwa data untuk bucket tersebut. Peristiwa data menyediakan aktivitas API tingkat objek dan sangat berguna untuk melacak unggahan file, unduhan, dan operasi lain yang dilakukan oleh pengguna. AWS Transfer Family

Untuk mengaktifkan peristiwa data Amazon S3 untuk server Anda AWS Transfer Family :

1. Buka CloudTrail konsol di <https://console.aws.amazon.com/cloudtrail/>.
2. Di panel navigasi, pilih Jalur, lalu pilih jejak yang ada atau buat yang baru.
3. Di bawah Peristiwa data, pilih Edit.
4. Untuk tipe peristiwa Data, pilih S3.
5. Pilih bucket Amazon S3 untuk mencatat peristiwa data. Anda dapat mencatat peristiwa data untuk semua bucket atau menentukan masing-masing bucket.
6. Pilih apakah akan mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.
7. Pilih Simpan perubahan.

Setelah mengaktifkan peristiwa data, Anda dapat mengakses log ini di bucket Amazon S3 yang dikonfigurasi untuk CloudTrail jejak Anda. Log mencakup detail seperti pengguna yang melakukan

tindakan, stempel waktu tindakan, objek tertentu yang terpengaruh, dan onBehalfOf bidang yang membantu melacak tindakan userId yang dilakukan. AWS Transfer Family

Contoh entri log untuk membuat server

Contoh berikut menunjukkan entri CloudTrail log (dalam format JSON) yang menunjukkan tindakan. 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"
}

```

Contoh log akses data

Saat mengaktifkan peristiwa data Amazon S3 untuk CloudTrail jejak Anda, Anda dapat melacak operasi file yang dilakukan. AWS Transfer Family Log ini membantu Anda memantau siapa yang mengakses data apa, kapan, dan bagaimana.

Contoh entri log untuk akses data yang berhasil

Contoh berikut menunjukkan entri CloudTrail log untuk operasi pengunduhan file yang berhasil melalui AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {

```

```

    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/
TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
    "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ="
  },
  "requestID": "EXAMPLE123456789",
  "eventID": "example12-3456-7890-abcd-ef1234567890",

```

```

    "readOnly": true,
    "resources": [
      {
        "type": "AWS::S3::Object",
        "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-report-2025-Q2.pdf"
      },
      {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::my-transfer-bucket"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "requestParameters": {
      "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
    }
  }
}

```

Dalam contoh ini, perhatikan bidang-bidang penting berikut:

- `eventName`: Menunjukkan operasi API S3 yang dilakukan (GetObject untuk pengunduhan file).
- `requestParameters.bucketName` dan `requestParameters.key`: Tampilkan objek S3 mana yang diakses.
- `additionalEventData.bytesTransferredOut`: Menunjukkan ukuran file yang diunduh dalam byte.
- `requestParameters.x-amz-onBehalfOf`: Berisi AWS Transfer Family nama pengguna dan ID sesi, memungkinkan Anda melacak AWS Transfer Family pengguna mana yang melakukan tindakan.

`x-amz-onBehalfOf` Bidang ini sangat penting karena menautkan panggilan kembali API S3 ke AWS Transfer Family pengguna tertentu yang memulai tindakan. Bidang ini mengikuti format `username.sessionid@server-id`, di mana:

- `username` adalah nama AWS Transfer Family pengguna.
- `sessionid` adalah pengenal unik untuk sesi pengguna.

- `server-id` adalah ID AWS Transfer Family server.

Operasi akses data umum

Saat memantau akses data AWS Transfer Family, Anda biasanya akan melihat operasi API S3 berikut di CloudTrail log Anda:

Operasi S3 umum di log AWS Transfer Family

Operasi API S3	AWS Transfer Family Aksi	Deskripsi
GetObject	Unduhan berkas	Pengguna mengunduh file dari server
PutObject	Unggahan file	Pengguna mengunggah file ke server
DeleteObject	Penghapusan file	Pengguna menghapus file dari server
ListObjects atau ListObjectsV2	Daftar direktori	File terdaftar pengguna dalam direktori
CopyObject	Salinan berkas	Pengguna menyalin file di dalam server

Dengan memantau operasi ini di CloudTrail log Anda, Anda dapat melacak semua aktivitas file yang dilakukan melalui AWS Transfer Family server Anda, membantu Anda memenuhi persyaratan kepatuhan dan mendeteksi akses yang tidak sah.

Amazon CloudWatch logging untuk AWS Transfer Family server

Amazon CloudWatch adalah layanan pemantauan dan observabilitas yang kuat yang memberikan visibilitas komprehensif ke AWS sumber daya Anda, termasuk. AWS Transfer Family

- Real-time pemantauan: CloudWatch memantau sumber daya dan aplikasi Transfer Family secara real-time, memungkinkan Anda melacak dan menganalisis kinerjanya.
- Koleksi metrik: CloudWatch mengumpulkan dan melacak berbagai metrik untuk sumber daya dan aplikasi Anda, yang merupakan variabel yang dapat Anda ukur dan gunakan untuk analisis.
- CloudWatch Halaman beranda: CloudWatch Halaman beranda secara otomatis menampilkan metrik tentang Transfer Family dan AWS layanan lain yang Anda gunakan, memberikan tampilan terpusat dari data pemantauan Anda.
- Dasbor khusus: Anda dapat membuat dasbor khusus CloudWatch untuk menampilkan metrik khusus untuk aplikasi khusus Anda dan sumber daya yang Anda pilih untuk dipantau.
- Alarm dan notifikasi: CloudWatch memungkinkan Anda membuat alarm yang memantau metrik Anda dan memicu pemberitahuan atau tindakan otomatis ketika ambang batas tertentu dilanggar. Ini dapat berguna untuk memantau aktivitas transfer file di server Transfer Family Anda dan menskalakan sumber daya yang sesuai.
- Optimalisasi biaya: Anda dapat menggunakan data yang dikumpulkan oleh CloudWatch untuk mengidentifikasi sumber daya yang kurang dimanfaatkan dan mengambil tindakan, seperti menghentikan atau menghapus instance, untuk mengoptimalkan biaya Anda.

Secara keseluruhan, kemampuan pemantauan yang komprehensif CloudWatch menjadikannya alat yang berharga untuk mengelola dan mengoptimalkan infrastruktur Transfer Family Anda dan aplikasi yang berjalan di dalamnya.

Detail untuk CloudWatch pencatatan untuk aplikasi web Transfer Family tersedia di [CloudTrail log untuk aplikasi web Transfer Family](#).

Jenis CloudWatch pencatatan untuk Transfer Family

Transfer Family menyediakan dua cara untuk mencatat peristiwa ke CloudWatch:

- Pencatatan terstruktur JSON

- Logging melalui peran logging

Untuk server Transfer Family, Anda dapat memilih mekanisme logging yang Anda inginkan. Untuk konektor dan alur kerja, hanya peran logging yang didukung.

Pencatatan terstruktur JSON

Untuk mencatat peristiwa server, sebaiknya gunakan logging terstruktur JSON. Ini menyediakan format logging yang lebih komprehensif yang memungkinkan kueri CloudWatch log. Untuk jenis logging ini, kebijakan IAM untuk pengguna yang membuat server (atau mengedit konfigurasi logging server) harus berisi izin berikut:

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

Berikut ini adalah contoh kebijakan .

```
{
  "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": "*"
  }
]
}

```

Untuk detail tentang pengaturan logging terstruktur JSON, lihat [Membuat, memperbarui, dan melihat logging untuk server](#).

Peran logging

Untuk mencatat peristiwa untuk alur kerja terkelola yang dilampirkan ke server, serta untuk konektor, Anda perlu menentukan peran logging. Untuk menetapkan akses, Anda membuat kebijakan IAM berbasis sumber daya dan peran IAM yang menyediakan informasi akses tersebut. Berikut ini adalah contoh kebijakan untuk Akun AWS yang dapat mencatat peristiwa server.

```

{
  "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/*"
    }
  ]
}

```

Untuk detail tentang mengonfigurasi peran logging untuk mencatat peristiwa alur kerja, lihat [Mengelola logging untuk alur kerja](#)

Membuat, memperbarui, dan melihat logging untuk server

Untuk semua AWS Transfer Family server, kami menyediakan logging terstruktur. Kami menyarankan Anda menggunakan logging terstruktur untuk semua server Transfer Family yang baru dan yang sudah ada. Manfaat menggunakan logging terstruktur meliputi:

- Menerima log dalam format JSON terstruktur.
- Kueri log Anda dengan Amazon CloudWatch Logs Insights, yang secara otomatis menemukan bidang berformat JSON.
- Bagikan grup log di seluruh AWS Transfer Family sumber daya memungkinkan Anda menggabungkan aliran log dari beberapa server ke dalam satu grup log, sehingga memudahkan pengelolaan konfigurasi pemantauan dan pengaturan penyimpanan log.
- Buat metrik dan visualisasi agregat yang dapat ditambahkan ke dasbor. CloudWatch
- Lacak data penggunaan dan kinerja dengan menggunakan grup log untuk membuat metrik log, visualisasi, dan dasbor terkonsolidasi.

Untuk mengaktifkan pencatatan alur kerja yang dilampirkan ke server, Anda harus menggunakan peran logging.

 Note

Saat Anda menambahkan peran logging, grup logging selalu `/aws/transfer/your-serverID`, dan tidak dapat diubah. Ini berarti, bahwa kecuali Anda mengirim log server terstruktur Anda ke grup yang sama, Anda akan masuk ke dua grup logging terpisah. Jika Anda tahu bahwa Anda akan mengaitkan alur kerja dengan server Anda, dan karenanya perlu menambahkan peran logging, Anda dapat mengatur logging terstruktur untuk masuk ke grup log default. `/aws/transfer/your-serverID`
Untuk mengubah grup logging Anda, lihat [StructuredLogDestinations](#) di Referensi AWS Transfer Family API.

Jika Anda membuat server baru menggunakan konsol Transfer Family, logging diaktifkan secara default. Setelah membuat server, Anda dapat menggunakan operasi `UpdateServer` API untuk mengubah konfigurasi logging Anda. Lihat perinciannya di [StructuredLogDestinations](#).

Saat ini, untuk alur kerja, jika ingin logging diaktifkan, Anda harus menentukan peran logging:

- Jika Anda mengaitkan alur kerja dengan server, menggunakan operasi `CreateServer` atau `UpdateServer` API, sistem tidak secara otomatis membuat peran logging. Jika Anda ingin mencatat peristiwa alur kerja Anda, Anda perlu melampirkan peran logging secara eksplisit ke server.

- Jika Anda membuat server menggunakan konsol Transfer Family dan melampirkan alur kerja, log akan dikirim ke grup log yang berisi ID server dalam nama. Formatnya `/aws/transfer/server-id`, misalnya, `/aws/transfer/s-1111aaaa2222bbbb3`. Log server dapat dikirim ke grup log yang sama atau yang lain.

Pertimbangan log untuk membuat dan mengedit server di konsol

- Server baru yang dibuat melalui konsol hanya mendukung logging JSON terstruktur, kecuali alur kerja dilampirkan ke server.
- Tidak ada logging bukanlah opsi untuk server baru yang Anda buat di konsol.
- Server yang ada dapat mengaktifkan logging JSON terstruktur melalui konsol kapan saja.
- Mengaktifkan logging JSON terstruktur melalui konsol menonaktifkan metode logging yang ada, agar tidak menagih pelanggan dua kali lipat. Pengecualiannya adalah jika alur kerja dilampirkan ke server.
- Jika Anda mengaktifkan logging JSON terstruktur, Anda tidak dapat menonaktifkannya nanti melalui konsol.
- Jika Anda mengaktifkan logging JSON terstruktur, Anda dapat mengubah tujuan grup log melalui konsol kapan saja.
- Jika Anda mengaktifkan logging JSON terstruktur, Anda tidak dapat mengedit peran logging melalui konsol jika Anda telah mengaktifkan kedua jenis logging melalui API. Pengecualiannya adalah jika server Anda memiliki alur kerja yang terpasang. Namun, peran logging terus muncul di Detail tambahan.

Pertimbangan logging untuk membuat dan mengedit server menggunakan API atau SDK

- Jika Anda membuat server baru melalui API, Anda dapat mengonfigurasi salah satu atau kedua jenis logging, atau memilih tidak ada logging.
- Untuk server yang ada, aktifkan dan nonaktifkan logging JSON terstruktur kapan saja.
- Anda dapat mengubah grup log melalui API kapan saja.
- Anda dapat mengubah peran logging melalui API kapan saja.

Untuk mengaktifkan logging terstruktur, Anda harus masuk ke akun dengan izin berikut

- `logs:CreateLogDelivery`

- logs:DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

Contoh kebijakan tersedia di bagian ini [Konfigurasi peran CloudWatch logging](#).

Topik

- [Membuat logging untuk server](#)
- [Memperbarui logging untuk server](#)
- [Melihat konfigurasi server](#)

Membuat logging untuk server

Saat Anda membuat server baru, pada halaman Konfigurasi detail tambahan, Anda dapat menentukan grup log yang ada, atau membuat yang baru.

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

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

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

Jika Anda memilih Buat grup log, CloudWatch konsol (<https://console.aws.amazon.com/cloudwatch/>) terbuka ke halaman Buat grup log. Untuk detailnya, lihat [Membuat grup log di CloudWatch Log](#).

Memperbarui logging untuk server

Detail untuk pencatatan bergantung pada skenario pembaruan Anda.

Note

Saat Anda memilih logging JSON terstruktur, mungkin ada penundaan, dalam kasus yang jarang terjadi, di mana Transfer Family berhenti masuk dalam format lama, tetapi membutuhkan waktu untuk mulai masuk dalam format JSON yang baru. Hal ini dapat mengakibatkan peristiwa yang tidak masuk log. Tidak akan ada gangguan layanan, tetapi Anda harus berhati-hati mentransfer file selama satu jam pertama setelah mengubah metode logging Anda, karena log dapat dihapus.

Jika Anda mengedit server yang ada, opsi Anda bergantung pada status server.

- Server sudah mengaktifkan peran logging, tetapi tidak mengaktifkan logging JSON Terstruktur.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- Server tidak memiliki logging yang diaktifkan.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



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

- Server sudah mengaktifkan logging JSON Terstruktur, tetapi tidak memiliki peran logging yang ditentukan.

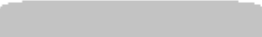
Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/  ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



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

- Server sudah mengaktifkan logging JSON Terstruktur, dan juga memiliki peran logging yang ditentukan.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

ⓘ Workflows events will be delivered to a log group labelled with the server ID.

Melihat konfigurasi server

Detail untuk halaman konfigurasi server bergantung pada skenario Anda:

Bergantung pada skenario Anda, halaman konfigurasi server mungkin terlihat seperti salah satu contoh berikut:

- Tidak ada logging yang diaktifkan.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- Pencatatan JSON terstruktur diaktifkan.

Additional details
Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- Peran logging diaktifkan, tetapi logging JSON terstruktur tidak diaktifkan.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted] execution-role [redacted]	Passive IP -

- Kedua jenis logging (peran logging dan logging JSON terstruktur) diaktifkan.

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 -

Mengelola logging untuk alur kerja

CloudWatch menyediakan audit dan pencatatan terkonsolidasi untuk kemajuan dan hasil alur kerja. Selain itu, AWS Transfer Family menyediakan beberapa metrik untuk alur kerja. Anda dapat melihat metrik berapa banyak eksekusi alur kerja yang dimulai, diselesaikan dengan sukses, dan gagal pada menit sebelumnya. Semua CloudWatch metrik untuk Transfer Family dijelaskan dalam [Menggunakan CloudWatch metrik untuk server Transfer Family](#).

Lihat CloudWatch log Amazon untuk alur kerja

1. Buka CloudWatch konsol Amazon di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi kiri, pilih Log, lalu pilih Grup log.
3. Pada halaman Grup log, pada bilah navigasi, pilih Wilayah yang benar untuk AWS Transfer Family server Anda.
4. Pilih grup log yang sesuai dengan server Anda.

Misalnya, jika ID server Anda `-1234567890abcdef0`, grup log Anda adalah `/aws/transfer/s-1234567890abcdef0`.

5. Pada halaman detail grup log untuk server Anda, aliran log terbaru ditampilkan. Ada dua aliran log untuk pengguna yang Anda jelajahi:

- Satu untuk setiap sesi Secure Shell (SSH) File Transfer Protocol (SFTP).

- Satu untuk alur kerja yang sedang dijalankan untuk server Anda. Format untuk aliran log untuk alur kerja adalah `username.workflowID.uniqueStreamSuffix`.

Misalnya, jika pengguna Andamary-major, Anda memiliki aliran log berikut:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

Pengidentifikasi alfanumerik 16 digit yang tercantum dalam contoh ini adalah fiktif. Nilai yang Anda lihat di Amazon CloudWatch berbeda.

Halaman peristiwa Log untuk `mary-major-usa-east.1234567890abcdef0` menampilkan detail untuk setiap sesi pengguna, dan aliran `mary.w-abcdef01234567890.021345abcdef6789` log berisi detail untuk alur kerja.

Berikut ini adalah contoh aliran log untuk `mary.w-abcdef01234567890.021345abcdef6789`, berdasarkan alur kerja (`w-abcdef01234567890`) yang berisi langkah salin.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
}
```

```

},
{
  "type": "StepStarted",
  "details": {
    "input": {
      "fileLocation": {
        "backingStore": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    },
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepCompleted",
  "details": {
    "output": {},
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "ExecutionCompleted",
  "details": {},
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",

```

```
"transferDetails":{
  "serverId":"s-server-id",
  "username":"mary",
  "sessionId":"session-id"
}
```

Konfigurasi peran CloudWatch logging

Untuk menetapkan akses, Anda membuat kebijakan IAM berbasis sumber daya dan peran IAM yang menyediakan informasi akses tersebut.

Untuk mengaktifkan CloudWatch pencatatan Amazon, Anda mulai dengan membuat kebijakan IAM yang memungkinkan CloudWatch pencatatan log. Anda kemudian membuat peran IAM dan melampirkan kebijakan ke dalamnya. Anda dapat melakukan ini ketika Anda [membuat server](#) atau dengan [mengedit server yang ada](#). Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) dan [Apa itu CloudWatch log Amazon?](#) di Panduan CloudWatch Pengguna Amazon.

Gunakan contoh berikut kebijakan IAM untuk mengizinkan CloudWatch pencatatan.

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": "*"
      }
    ]
  }
}

```

Dalam contoh kebijakan sebelumnya, untuk **Resource**, ganti *region-id* dan *Akun AWS* dengan nilai Anda. Sebagai contoh, **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**.

Anda kemudian membuat peran dan melampirkan kebijakan CloudWatch Log yang Anda buat.

Untuk membuat peran IAM dan melampirkan kebijakan

1. Di panel navigasi, pilih Peran, lalu pilih Buat peran.

Pada halaman Buat peran, pastikan bahwa AWS layanan dipilih.

2. Pilih Transfer dari daftar layanan, lalu pilih Berikutnya: Izin. Ini membangun hubungan kepercayaan antara AWS Transfer Family dan peran IAM. Selain itu, tambahkan `aws:SourceAccount` dan `aws:SourceArn` kondisikan kunci untuk melindungi diri Anda dari masalah wakil yang membingungkan. Lihat dokumentasi berikut untuk lebih jelasnya:

- Prosedur untuk membangun hubungan kepercayaan dengan AWS Transfer Family: [Untuk membangun hubungan kepercayaan](#)
- Deskripsi untuk masalah wakil yang bingung: [masalah wakil yang bingung](#)

3. Di bagian Lampirkan kebijakan izin, cari dan pilih kebijakan CloudWatch Log yang baru saja Anda buat, lalu pilih Berikutnya: Tag.
4. (Opsional) Masukkan kunci dan nilai untuk tag, dan pilih Berikutnya: Tinjau.
5. Pada halaman Tinjauan, masukkan nama dan deskripsi untuk peran baru Anda, lalu pilih Buat peran.
6. Untuk melihat log, pilih ID Server untuk membuka halaman konfigurasi server, dan pilih Lihat log. Anda diarahkan ke CloudWatch konsol tempat Anda dapat melihat aliran log Anda.

Pada CloudWatch halaman server Anda, Anda dapat melihat catatan otentikasi pengguna (keberhasilan dan kegagalan), unggahan data (PUToperasi), dan unduhan data (GEToperasi).

Melihat aliran log Transfer Family

Untuk melihat log server Transfer Family

1. Arahkan ke halaman detail untuk server.
2. Pilih Lihat log. Ini membuka Amazon CloudWatch.
3. Grup log untuk server yang Anda pilih akan ditampilkan.

CloudWatch ×

CloudWatch > Log groups > /aws/transfer/s-

/aws/transfer/s- Actions View in Logs Insights Search log group

Log group details

ARN arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-:*	Metric filters 0 Subscription filters 0 Contributor Insights rules -	Data protection - new Inactive Sensitive data found - new - KMS key ID -
Creation time 2 years ago		
Retention Never expire		
Stored bytes 39.39 MB		

Log streams Metric filters Subscription filters Contributor Insights Tags Data protection - new

Log streams (10) [Refresh] [Delete] [Create log stream] [Search all log streams]

Q Filter log streams or try prefix search ☐ Exact match ☐ Show expired [Info](#) < 1 > [Settings]

☐	Log stream	Last event
☐	ERRORS	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-

4. Anda dapat memilih aliran log untuk menampilkan detail dan entri individual untuk aliran.
- Jika ada daftar untuk ERROR, Anda dapat memilihnya untuk melihat detail kesalahan terbaru untuk server.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

1m 30m 1h 12h Custom

▶	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...	Copy
▼	2023-03-23T16:12:56.857-04:00	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=	Copy
▶	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Pilih entri lain untuk melihat contoh aliran log.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

1m 30m 1h 12h Custom

▶	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			

- Jika server Anda memiliki alur kerja terkelola yang terkait dengannya, Anda dapat melihat log untuk menjalankan alur kerja.

Note

Format untuk aliran log untuk alur kerja adalah `username.workflowId.uniqueStreamSuffix`. Misalnya, `decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` bisa menjadi nama aliran log untuk pengguna dan alur kerja. **decrypt-user w-a1111222233334444**

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
	There are older events to load. Load more .
2023-03-21T13:37:57.795-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt-</code>
2023-03-21T14:12:02.850-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt- <pre> { "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "", "key": "decrypt-user/test.json.gpg", "versionId": "", "etag": "" } }, "stepType": "DECRYPT", "stepName": "decrypt-step" }, "workflowId": "w-", "executionId": "", "transferDetails": { "serverId": "s-", "username": "decrypt-user", "sessionId": "" } } </pre> </code>
2023-03-21T14:12:03.464-04:00	<code>{"type": "StepCompleted", "details": {"output": {}}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-</code>

Note

Untuk entri log yang diperluas, Anda dapat menyalin entri ke clipboard dengan memilih Salin. Untuk detail selengkapnya tentang CloudWatch log, lihat [Melihat data log](#).

Membuat CloudWatch alarm Amazon

Contoh berikut menunjukkan cara membuat CloudWatch alarm Amazon menggunakan AWS Transfer Family metrik,FilesIn.

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Mencatat operasi API Amazon S3 ke log akses S3

Note

Bagian ini tidak berlaku untuk aplikasi web Transfer Family.

Jika Anda [menggunakan log akses Amazon S3 untuk mengidentifikasi permintaan S3](#) yang dibuat atas nama pengguna transfer file Anda, RoleSessionName digunakan untuk menampilkan peran IAM mana yang diasumsikan untuk melayani transfer file. Ini juga menampilkan informasi tambahan seperti nama pengguna, id sesi, dan server-id yang digunakan untuk transfer. Formatnya adalah [AWS:Role Unique Identifier]/username.sessionid@server-id dan terkandung dalam bidang Pemohon. Misalnya, berikut ini adalah konten untuk bidang Peminta sampel dari log akses S3 untuk file yang disalin ke bucket S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/  
username.sessionid@server-id
```

Di bidang Pemohon di atas, ini menunjukkan Peran IAM yang disebut. IamRoleName Untuk informasi selengkapnya tentang pengidentifikasi unik peran IAM, lihat [Pengidentifikasi unik di Panduan Pengguna AWS Identity and Access Management](#)

Contoh untuk membatasi masalah wakil yang membingungkan

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Untuk detail selengkapnya, lihat [Cross-service pencegahan wakil bingung](#).

Note

Dalam contoh berikut, ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

Dalam contoh ini, Anda dapat menghapus detail ARN untuk alur kerja jika server Anda tidak memiliki alur kerja yang melekat padanya.

Contoh logging/invoke kebijakan berikut memungkinkan setiap server (dan alur kerja) dalam akun untuk mengambil peran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

Contoh logging/invoke kebijakan berikut memungkinkan server tertentu (dan alur kerja) untuk mengambil peran.

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

```
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-  
id"
        ]
      }
    }
  }
}
```

CloudWatch struktur log untuk Transfer Family

Topik ini menjelaskan bidang yang diisi dalam log Transfer Family: baik untuk entri log terstruktur JSON maupun entri log lama.

Topik

- [Log terstruktur JSON untuk Transfer Family](#)
- [Log lama untuk Transfer Family](#)

Log terstruktur JSON untuk Transfer Family

Tabel berikut berisi rincian untuk bidang entri log untuk SFTP/FTP/FTPS tindakan Transfer Family, dalam format log terstruktur JSON yang baru.

Bidang	Deskripsi	Entri contoh
jenis aktivitas	Tindakan oleh pengguna	Jenis kegiatan yang tersedia adalah sebagai berikut:AUTH_FAIL URE ,CONNECTED ,DISCONN

Bidang	Deskripsi	Entri contoh
		TED ,ERROR,EXIT_REAS ON ,CLOSE,CREATE_SY MLINK ,DELETE,MKDIR,OPEN,PARTIA LOSE ,RENAME,RMDIR,SETSTAT,TLS_ E_FAILURE .
bytes-in	Jumlah byte yang diunggah oleh pengguna	29238420042
bytes-out	Jumlah byte yang diunduh oleh pengguna	23094032490328
cipher	Menentukan cipher SSH dinegosiasikan untuk koneksi (cipher yang tersedia tercantum dalam) Algoritma kriptografi	aes256-gcm@openssh.com
klien	Perangkat lunak klien pengguna	SSH-2.0-OpenSSH_7.4
rumah-dir	Direktori tempat pengguna akhir mendarat saat mereka terhubung ke titik akhir jika jenis direktori home mereka adalahPATH: jika mereka memiliki direktori home logis, nilai ini selalu /	/pengguna-rumah-- bucket/test
kex	Menentukan pertukaran kunci SSH yang dinegosiasikan (KEX) untuk koneksi (KEX tersedia tercantum dalam) Algoritma kriptografi	diffie-hellman-group14-sha256

Bidang	Deskripsi	Entri contoh
pesan	Memberikan informasi lebih lanjut terkait dengan kesalahan	<i><string></i>
metode	Metode otentikasi	kunci publik
Mode	Menentukan bagaimana klien membuka file	BUAT MEMOTONG TULIS
operation	Operasi klien pada file	BUKA TUTUP
path	Jalur file aktual terpengaruh	bucket/test/amzn-s3-demo- - file-1.pdf
ssh-kunci publik	Badan kunci publik untuk pengguna yang terhubung	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl
sidik jari kunci publik ssh-publik	Sidik jari kunci publik, seperti yang ditunjukkan di konsol untuk pengguna yang dikelola layanan saat mencantumkan kunci pengguna mereka.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0

 Note

Di konsol, sidik jari ditampilkan dengan karakter padding (jika ada): dari 0 hingga 3 tanda yang sama (=) di akhir. Dalam entri log, padding ini dilucuti dari output.

Bidang	Deskripsi	Entri contoh
tipe kunci publik ssh-publik	Jenis kunci publik: Transfer Family mendukung RSA-, ECDSA-, dan kunci ED25519-formatted	ssh-ed25519
sumber daya-arn	Pengidentifikasi unik yang ditetapkan sistem untuk sumber daya tertentu (misalnya, server)	arn:aws:transfer: ap-timur laut-1:12346789012: -1234567890akeu2js2 server/s
peran	Peran IAM pengguna	arn:aws:iam: :0293883675: -peran role/testuser
session-id	Pengidentifikasi unik yang ditetapkan sistem untuk satu sesi	9ca9a0e1cec6ad9d
sumber-ip	Alamat IP Klien	18.323.0.129
user	Nama pengguna akhir	myname192
kebijakan pengguna	Izin yang ditentukan untuk pengguna akhir: bidang ini diisi jika kebijakan pengguna adalah kebijakan sesi.	Kode JSON untuk kebijakan sesi yang sedang digunakan

Log lama untuk Transfer Family

Tabel berikut berisi rincian untuk entri log untuk berbagai tindakan Transfer Family.

Note

Entri ini tidak dalam format log terstruktur JSON yang baru.

Tabel berikut berisi rincian untuk entri log untuk berbagai tindakan Transfer Family, dalam format log terstruktur JSON yang baru.

Tindakan	Log yang sesuai dalam CloudWatch Log Amazon
Kegagalan otentikasi	ERROR AUTH_FAILURE METHOD=PublicKey User="RSA+b7 +a+hxg0c7l1jiZ0" sourceIP=3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE
COPY/TAG/DELETE/DECRYPT alur kerja	<pre>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/lhr/regex.py"}}, "stepType": "TAG", "stepName": "successful_tag_step", "workflowId": "w-1111a-aaa222bbb3", "ExecutionID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": {"serverID": "s-1234abcd5678efghi", "username": "lhr", "sessionId": "1234567890abcdef0"}}</pre>
Alur kerja langkah kustom	<pre>{"type": "CustomStepInvoked", "details": {"output": {"token": ""}, "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "workflowId": "MzM4Mjg5YWUtYTEzMy00YjZlLWI3OGMtYzU4OGI2ZjQyMzE5", "ExecutionID": "w-9283e49d33297c3f7", "ExecutionId": "1234abcd-1234-efgh-58-678-ijklmnopqr90", "transferDetails": {"serverID": "s-zzzz1111aaaa22223", "username": "lhr", "sessionId": "1234567890abcdef0"}}</pre>
Menghapus	lhr.33a8fb495ffb383b HAPUS Path=/ /123.jpg bucket/user
Unduh	lhr.33a8fb495ffb383b JALUR TERBUKA =/ /123.jpg mode=Baca bucket/user

Tindakan	Log yang sesuai dalam CloudWatch Log Amazon
	lhr.33a8fb495ffb383b JALUR TUTUP =/ /123.jpg =3618546 bucket/user BytesOut
Logins/Logouts	user.914984e553bcddb6 SUMBER TERHUBUNG = 1.22.111.222 pengguna = LHR = Klien LOGIS = _7.4 peran = Arn:aws: :iam: :123456789012: -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcddb6 TERPUTUS
Mengganti nama	lhr.33a8fb495ffb383b GANTI NAMA Path=/ / lambo.png =/ /ferrari.png bucket/user NewPath bucket/user
Contoh log kesalahan alur kerja	{"type": "StepErrored ", "details": {"ErrorType": "BAD_REQUEST", "ErrorMessage": "Tidak dapat menandai berkas Efs", "stepType": "stepName": "successful_tag_step"}, "workflowid": "w-1234abcd5678efghi", "ExecutionID": "81234abcd5678efghi", "ExecutionID": "81234abcd5678efghi": "ExecutionID": "81234abcd5678efghi": "ExecutionID": "81234abcd5678efghi": "ExecutionID": "81234abcd534abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": {"serverID": "s-1234abcd5678efghi", "nama pengguna": "lhr", "sessionID": "1234567890abcdef0"}}}
Symlink	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs- /pqr.jpg =abc.jpg LinkPath 12345678/lhr TargetPath

Tindakan	Log yang sesuai dalam CloudWatch Log Amazon
Unggahan	lhr.33a8fb495ffb383b JALUR TERBUKA =/ mode /123.jpg =buat terpotong tuliskan bucket/user lhr.33a8fb495ffb383b JALUR TUTUP =/ /123.jpg =3618546 bucket/user BytesIn
Alur kerja	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initial": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "filePath": "lhr/regex.py" } }, "workflowId": "w-1111a-aaa22bbb3", "executionId": "123434-abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-zzzz1111aaaaa22223", "userName": "lhr", "sessionId": "1234567890abcdef0" } } }</pre> <pre>{ "type": "StepStarted", "details": { "input": { "filePath": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "filePath": "lhr/regex.py" }, "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "workType": "efs-s3_copy_2", "workType": "stepName": "efs-s3_copy_2", "workType": "wid": "w-9283e49d33297c3f7", "ExecutionID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-18ca49dce5d842e0b", "username": "lhr", "sessions5d842e0b id": "1234567890abcdef0" } } } }</pre>

Contoh entri CloudWatch log

Topik ini menyajikan contoh entri log.

Topik

- [Contoh entri log sesi transfer](#)
- [Contoh entri log untuk konektor SFTP](#)
- [Contoh entri log untuk konektor VPC Lattice](#)
- [Contoh entri log untuk kegagalan algoritma pertukaran Kunci](#)

Contoh entri log sesi transfer

Dalam contoh ini, pengguna SFTP terhubung ke server Transfer Family, mengunggah file, lalu memutuskan sambungan dari sesi.

Entri log berikut mencerminkan pengguna SFTP yang terhubung ke server Transfer Family.

```
{
  "role": "arn:aws:iam::500655546075:role/transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "home-dir": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrQDPY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Entri log berikut mencerminkan pengguna SFTP yang mengunggah file ke bucket Amazon S3 mereka.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

```
}
```

Entri log berikut mencerminkan pengguna SFTP yang terputus dari sesi SFTP mereka. Pertama, klien menutup koneksi ke bucket, dan kemudian klien memutuskan sesi SFTP.

```
{
  "path": "/test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "bytes-in": "121",
  "session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Note

Jenis kegiatan yang tersedia adalah sebagai

berikut: AUTH_FAILURE, CONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK

Contoh entri log untuk konektor SFTP

Bagian ini berisi contoh log untuk transfer yang berhasil dan tidak berhasil. Log dihasilkan ke grup log bernama `/aws/transfer/connector-id`, di mana *connector-id* adalah pengenal untuk konektor SFTP Anda. Entri log untuk konektor SFTP dihasilkan saat Anda menjalankan perintah atau perintah. `StartFileTransfer` `StartDirectoryListing`

Entri log ini untuk transfer yang berhasil diselesaikan.

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T16:33:27.373720Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
```

```

    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "COMPLETED",
    "start-time": "2023-10-25T16:33:26.945481Z",
    "end-time": "2023-10-25T16:33:27.159823Z",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "local-directory-path": "/connectors-localbucket",
    "bytes": 514,
    "egress-type": "SERVICE_MANAGED"
  }

```

Entri log ini untuk transfer yang waktunya habis, dan dengan demikian tidak berhasil diselesaikan.

```

{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T22:33:47.625703Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "FAILED",
  "failure-code": "TIMEOUT_ERROR",
  "failure-message": "Transfer request timeout.",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

Entri log ini untuk operasi SEND yang berhasil.

```

{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",

```



```

    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

Deskripsi untuk beberapa bidang kunci dalam contoh log sebelumnya.

- `timestamp` mewakili saat log ditambahkan ke CloudWatch. `start-time` dan `end-time` sesuai dengan kapan konektor benar-benar memulai dan menyelesaikan transfer.
- `transfer-id` adalah pengidentifikasi unik yang ditetapkan untuk setiap `start-file-transfer` permintaan. Jika pengguna melewati beberapa jalur file dalam satu operasi `start-file-transfer` API, semua file berbagi yang sama `transfer-id`.
- `file-transfer-id` adalah nilai unik yang dihasilkan untuk setiap file yang ditransfer. Perhatikan bahwa bagian awal `file-transfer-id` adalah sama dengan `transfer-id`.

Contoh entri log untuk konektor VPC Lattice

Bagian ini berisi contoh log untuk konektor VPC Lattice. Untuk konektor VPC Lattice, log menyertakan bidang tambahan yang memberikan informasi tentang konfigurasi konektor dan pengaturan jaringan.

Entri log ini untuk operasi KIRIM konektor VPC Lattice yang berhasil diselesaikan.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",
  "start-time": "2025-09-05T14:20:19.434072509Z",
  "end-time": "2025-09-05T14:20:19.481453346Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",

```

```

"remote-directory-path": "/test-bucket/test-folder/",
"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-
id:resourceconfiguration/resource-configuration-arn-id,
"vpc-lattice-port-number": 22
}

```

Log konektor VPC Lattice mencakup bidang tambahan berikut:

- `egress-type`- Jenis konfigurasi jalan keluar untuk konektor
- `vpc-lattice-resource-configuration-arn`- ARN dari Konfigurasi Sumber Daya Kisi VPC yang mendefinisikan lokasi server SFTP target
- `vpc-lattice-port-number`- Nomor port untuk menghubungkan ke server SFTP melalui VPC Lattice

Contoh entri log untuk kegagalan algoritma pertukaran Kunci

Bagian ini berisi contoh log di mana algoritma pertukaran Kunci (KEX) gagal. Ini adalah contoh dari aliran log ERRORS untuk log terstruktur.

Entri log ini adalah contoh di mana ada kesalahan jenis kunci host.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-99999999999999999999",
  "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"
}

```

Entri log ini adalah contoh di mana ada ketidakcocokan KEX.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-99999999999999999999",

```

```

    "message": "no matching key exchange method found",
    "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group14-sha256"
  }

```

Menggunakan CloudWatch metrik untuk server Transfer Family

Note

Anda juga bisa mendapatkan metrik untuk Transfer Family dari dalam konsol Transfer Family itu sendiri. Untuk detailnya, lihat [Memantau penggunaan di konsol](#)

Anda bisa mendapatkan informasi tentang server Anda menggunakan CloudWatch metrik. Metrik mewakili kumpulan titik data yang diurutkan waktu yang dipublikasikan ke CloudWatch. [Saat menggunakan metrik, Anda harus menentukan namespace Transfer Family, nama metrik, dan dimensi.](#) Untuk informasi selengkapnya tentang metrik, lihat [Metrik](#) di CloudWatch Panduan Pengguna Amazon.

Tabel berikut menjelaskan CloudWatch metrik untuk Transfer Family.

Namespace	Metrik	Deskripsi
AWS/Transfer	BytesIn	Jumlah total byte yang ditransfer ke server. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses Unit: Hitung Periode: 5 menit

Namespace	Metrik	Deskripsi
	BytesOut	Jumlah total byte yang ditransfer keluar dari server. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menelepon <code>StartFile Transfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses. Unit: Hitung Periode: 5 menit
	FilesIn	Jumlah total file yang ditransfer ke server. Untuk server yang menggunakan protokol AS2, metrik ini mewakili jumlah pesan yang diterima. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses. Unit: Hitung Periode: 5 menit

Namespace	Metrik	Deskripsi
	FilesOut	Jumlah total file yang ditransfer keluar dari server. Kriteria pelaporan: • Untuk SFTP/FTP/FTPS: dipancarkan setiap 5 menit saat koneksi dibuat ke server Transfer Family. Jika tidak ada file atau byte yang ditransfer dalam periode tersebut, "0" dipancarkan. • Untuk AS2: ketika pelanggan menelepon StartFile Transfer dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses. Unit: Hitung Periode: 5 menit
	InboundMessage	Jumlah total pesan AS2 yang berhasil diterima dari mitra dagang. Kriteria pelaporan: Ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses dengan sukses Unit: Hitung Periode: 5 menit

Namespace	Metrik	Deskripsi
	InboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil diterima dari mitra dagang. Artinya, mitra dagang mengirim pesan, tetapi server Transfer Family tidak berhasil memprosesnya. Kriteria pelaporan: Ketika pelanggan menerima pesan di server AS2 mereka dan dipancarkan segera setelah pesan masuk selesai diproses tidak berhasil Unit: Hitung Periode: 5 menit
	OnUploadExecutionsStarted	Jumlah total eksekusi alur kerja dimulai di server. Kriteria pelaporan: Dipicu setiap kali eksekusi dimulai Unit: Hitung Periode: 1 menit
	OnUploadExecutionsSuccess	Jumlah total eksekusi alur kerja yang berhasil di server. Kriteria pelaporan: Dipicu setiap kali eksekusi berhasil selesai Unit: Hitung Periode: 1 menit
	OnUploadExecutionsFailed	Jumlah total eksekusi alur kerja yang gagal di server. Kriteria pelaporan: Dipicu setiap kali eksekusi tidak berhasil diselesaikan Unit: Hitung Periode: 1 menit

Namespace	Metrik	Deskripsi
	OutboundMessage	Jumlah total pesan AS2 yang berhasil dikirim ke mitra dagang. Kriteria pelaporan: Ketika pelanggan menelepon <code>StartFileTransfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses dengan sukses Unit: Hitung Periode: 5 menit
	OutboundFailedMessage	Jumlah total pesan AS2 yang tidak berhasil dikirim ke mitra dagang. Kriteria pelaporan: Ketika pelanggan menelepon <code>StartFileTransfer</code> dari konektor AS2 mereka dan dipancarkan segera setelah pesan keluar selesai diproses tidak berhasil Unit: Hitung Periode: 5 menit

Dimensi Transfer Family

Dimensi adalah name/value pasangan yang merupakan bagian dari identitas metrik. Untuk informasi selengkapnya tentang dimensi, lihat [Dimensi](#) di Panduan CloudWatch Pengguna Amazon.

Tabel berikut menjelaskan CloudWatch dimensi untuk Transfer Family.

Dimensi	Deskripsi
ServerId	ID unik dari server.
ConnectorId	ID unik konektor. Digunakan untuk AS2, untuk OutboundMessage dan OutboundFailedMessage

Menggunakan Notifikasi Pengguna AWS dengan AWS Transfer Family

Untuk mendapatkan pemberitahuan tentang AWS Transfer Family acara, Anda dapat menggunakan [Notifikasi Pengguna AWS](#) untuk mengatur berbagai saluran pengiriman. Jika acara cocok dengan aturan yang Anda tentukan, Anda menerima pemberitahuan.

Anda dapat menerima pemberitahuan untuk acara melalui beberapa saluran, termasuk email, [Pengembang Amazon Q dalam pemberitahuan obrolan aplikasi](#) obrolan, atau pemberitahuan [AWS Console Mobile Application](#) push. Anda juga dapat melihat notifikasi di [Pusat Pemberitahuan Konsol](#). Notifikasi Pengguna mendukung agregasi, yang dapat mengurangi jumlah pemberitahuan yang Anda terima selama acara tertentu.

Untuk informasi selengkapnya, lihat [Menyesuaikan pemberitahuan pengiriman file menggunakan posting blog alur kerja AWS Transfer Family terkelola](#), dan [Apa itu? Notifikasi Pengguna AWS](#) dalam Notifikasi Pengguna AWS User Guide.

Menggunakan kueri untuk memfilter entri log

Anda dapat menggunakan CloudWatch kueri untuk memfilter dan mengidentifikasi entri log untuk Transfer Family. Bagian ini berisi beberapa contoh.

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Anda dapat membuat kueri atau aturan.
 - Untuk membuat kueri Wawasan Log, pilih Wawasan Log dari panel navigasi kiri, lalu masukkan detail untuk kueri Anda.
 - Untuk membuat aturan Contributor Insights, pilih Insights > Contributor Insights dari panel navigasi kiri, lalu masukkan detail untuk aturan Anda.
3. Jalankan kueri atau aturan yang Anda buat.

Lihat kontributor kegagalan otentikasi teratas

Dalam log terstruktur Anda, entri log kegagalan otentikasi terlihat mirip dengan yang berikut:

```
{
```



```

"method": "password",
"activity-type": "AUTH_FAILURE",
"source-ip": "999.999.999.999",
"resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
"message": "Invalid user name or password",
"user": "exampleUser"
}

```

Jalankan kueri berikut untuk melihat kontributor teratas untuk kegagalan otentikasi.

```

filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10

```

Daripada menggunakan Wawasan CloudWatch Log, Anda dapat membuat aturan Wawasan CloudWatch Kontributor untuk melihat kegagalan autentikasi. Buat aturan yang mirip dengan yang berikut ini.

```

{
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$.activity-type",
        "In": [
          "AUTH_FAILURE"
        ]
      }
    ],
    "Keys": [
      "$.user"
    ]
  },
  "LogFormat": "JSON",
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupARNs": [
    "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
  ]
}

```

```
]
}
```

Lihat entri log tempat file dibuka

Dalam log terstruktur Anda, entri log baca file terlihat mirip dengan yang berikut ini:

```
{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id": "0049cd844c7536c06a89"
}
```

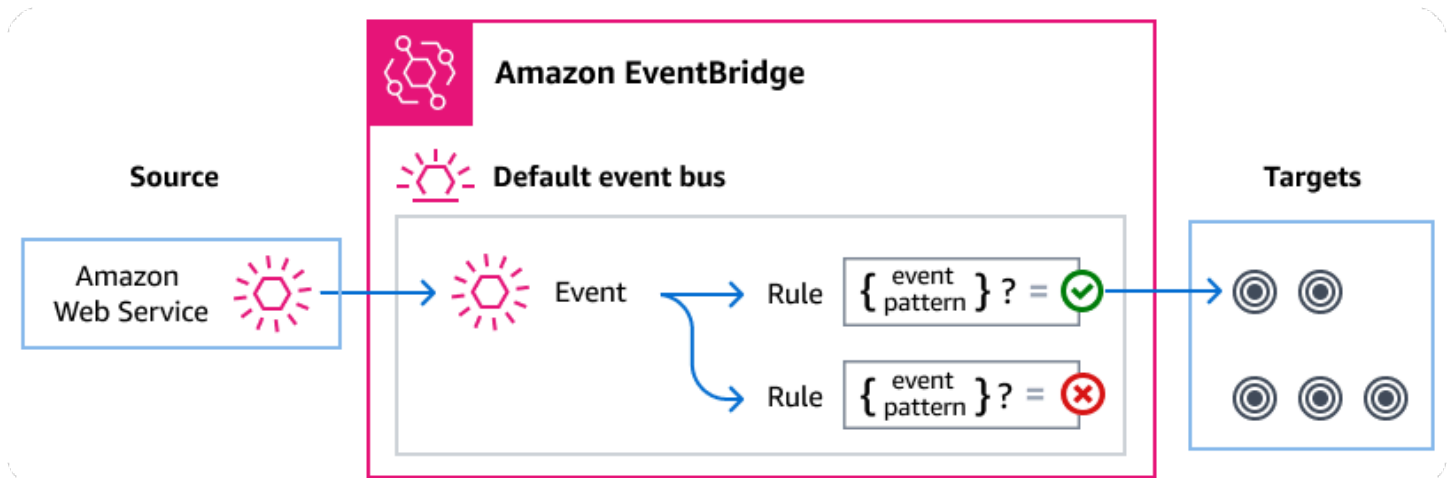
Jalankan kueri berikut untuk melihat entri log yang menunjukkan file dibuka.

```
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path
```

Mengelola Transfer Family acara menggunakan Amazon EventBridge

Amazon EventBridge adalah layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, yang dapat memudahkan Anda membangun aplikasi berbasis peristiwa yang dapat diskalakan. Event-driven Arsitektur adalah gaya membangun sistem perangkat lunak yang digabungkan secara longgar yang bekerja sama dengan memancarkan dan menanggapi peristiwa. Peristiwa mewakili perubahan dalam sumber daya atau lingkungan.

Seperti banyak AWS layanan, Transfer Family menghasilkan dan mengirim acara ke bus acara Amazon EventBridge default. Perhatikan bahwa bus acara default secara otomatis disediakan di setiap AWS akun. Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Anda menentukan aturan untuk bus acara yang mengevaluasi peristiwa saat mereka tiba. Setiap aturan memeriksa apakah suatu peristiwa cocok dengan pola acara aturan. Jika acara cocok, bus acara mengirimkan acara ke satu atau lebih target yang ditentukan.



Topik

- [Transfer Family peristiwa](#)
- [Mengirim Transfer Family peristiwa dengan menggunakan EventBridge aturan](#)
- [Amazon EventBridge izin](#)
- [Tambahkan EventBridge sumber daya](#)
- [Transfer Family referensi detail acara](#)

Transfer Family peristiwa

Transfer Family secara otomatis mengirimkan acara ke bus EventBridge acara default. Anda dapat membuat aturan pada bus acara di mana setiap aturan mencakup pola acara dan satu atau lebih target.

Peristiwa yang cocok dengan pola peristiwa aturan dikirimkan ke target yang ditentukan baik dengan upaya terbaik atau tahan lama (perhatikan bahwa beberapa peristiwa mungkin dikirim rusak). Tingkat pengiriman ini dijelaskan dalam [tingkat Pengiriman untuk peristiwa AWS layanan](#) di Referensi EventBridge Acara Amazon.

- Server-level acara untuk server SFTP, FTPS dan FTP disampaikan atas dasar upaya terbaik.
- Acara konektor SFTP dikirimkan secara tahan lama.
- Acara AS2 disampaikan secara tahan lama.

Peristiwa berikut dihasilkan oleh Transfer Family. Untuk informasi selengkapnya, lihat [EventBridge peristiwa](#) di Panduan Amazon EventBridge Pengguna.

Acara server SFTP, FTPS, dan FTP

Tabel berikut mencantumkan peristiwa untuk server SFTP, FTPS, dan FTP, yang diselenggarakan berdasarkan jenis acara.

Upload file dan download acara

Jenis detail acara	Deskripsi
Unduhan File Server FTP Selesai	Sebuah file telah berhasil diunduh untuk protokol FTP.
Unduhan File Server FTP Gagal	Upaya untuk mengunduh file gagal untuk protokol FTP.
Unggahan File Server FTP Selesai	Sebuah file telah berhasil diunggah untuk protokol FTP.
Unggahan File Server FTP Gagal	Upaya untuk mengunggah file gagal untuk protokol FTP.

Jenis detail acara	Deskripsi
Unduhan File Server FTPS Selesai	File telah berhasil diunduh untuk protokol FTPS.
Unduhan File Server FTPS Gagal	Upaya untuk mengunduh file gagal untuk protokol FTPS.
Unggahan File Server FTPS Selesai	Sebuah file telah berhasil diunggah untuk protokol FTPS.
Unggahan File Server FTPS Gagal	Upaya untuk mengunggah file gagal untuk protokol FTPS.
Unduhan File Server SFTP Selesai	Sebuah file telah berhasil diunduh untuk protokol SFTP.
Unduhan File Server SFTP Gagal	Upaya untuk mengunduh file gagal untuk protokol SFTP.
Unggahan File Server SFTP Selesai	Sebuah file telah berhasil diunggah untuk protokol SFTP.
Unggahan File Server SFTP Gagal	Upaya untuk mengunggah file gagal untuk protokol SFTP.

Acara operasi file lainnya

Jenis detail acara	Deskripsi
Direktori Server FTP Membuat Selesai	Direktori telah berhasil dibuat untuk protokol FTP.
Membuat Direktori Server FTP Gagal	Upaya untuk membuat direktori gagal untuk protokol FTP.
Penghapusan Direktori Server FTP Selesai	Direktori telah berhasil dihapus untuk protokol FTP.

Jenis detail acara	Deskripsi
Penghapusan Direktori Server FTP Gagal	Upaya untuk menghapus direktori telah gagal untuk protokol FTP.
Penghapusan File Server FTP Selesai	Sebuah file telah berhasil dihapus untuk protokol FTP.
Penghapusan File Server FTP Gagal	Upaya untuk menghapus file telah gagal untuk protokol FTP.
Ganti Nama File Server FTP Selesai	Sebuah file telah berhasil diganti namanya untuk protokol FTP.
Gagal Mengganti Nama File Server FTP	Upaya untuk mengganti nama file telah gagal untuk protokol FTP.
Direktori Server FTPS Membuat Selesai	Direktori telah berhasil dibuat untuk protokol FTPS.
Pembuatan Direktori Server FTPS Gagal	Upaya untuk membuat direktori gagal untuk protokol FTPS.
Penghapusan Direktori Server FTPS Selesai	Direktori telah berhasil dihapus untuk protokol FTPS.
Penghapusan Direktori Server FTPS Gagal	Upaya untuk menghapus direktori telah gagal untuk protokol FTPS.
Penghapusan File Server FTPS Selesai	Sebuah file telah berhasil dihapus untuk protokol FTPS.
Penghapusan File Server FTPS Gagal	Upaya untuk menghapus file gagal untuk protokol FTPS.
Ganti Nama File Server FTPS Selesai	Sebuah file telah berhasil diganti namanya untuk protokol FTPS.
Gagal Mengganti Nama File Server FTPS	Upaya untuk mengganti nama file telah gagal untuk protokol FTPS.

Jenis detail acara	Deskripsi
Direktori Server SFTP Membuat Selesai	Direktori telah berhasil dibuat untuk protokol SFTP.
Pembuatan Direktori Server SFTP Gagal	Upaya untuk membuat direktori gagal untuk protokol SFTP.
Penghapusan Direktori Server SFTP Selesai	Direktori telah berhasil dihapus untuk protokol SFTP.
Penghapusan Direktori Server SFTP Gagal	Upaya untuk menghapus direktori telah gagal untuk protokol SFTP.
Penghapusan File Server SFTP Selesai	Sebuah file telah berhasil dihapus untuk protokol SFTP.
Penghapusan File Server SFTP Gagal	Upaya untuk menghapus file gagal untuk protokol SFTP.
Ganti Nama File Server SFTP Selesai	Sebuah file telah berhasil diganti namanya untuk protokol SFTP.
Gagal Mengganti Nama File Server SFTP	Upaya untuk mengganti nama file telah gagal untuk protokol SFTP.

Acara konektor SFTP

Note

Acara ini dikirimkan ke EventBridge tingkat tahan lama, seperti yang dijelaskan dalam [tingkat Pengiriman untuk acara AWS layanan](#) di Referensi EventBridge Acara Amazon.

Jenis detail acara	Deskripsi
Kirim File Konektor SFTP Selesai	Transfer file dari konektor ke server SFTP jarak jauh telah berhasil diselesaikan.
Kirim File Konektor SFTP Gagal	Transfer file dari konektor ke server SFTP jarak jauh telah gagal.
Pengambilan File Konektor SFTP Selesai	Transfer file dari server SFTP jarak jauh ke konektor telah berhasil diselesaikan.
Pengambilan File Konektor SFTP Gagal	Transfer file dari server SFTP jarak jauh ke konektor gagal.
Daftar Direktori Konektor SFTP Selesai	Panggilan daftar direktori file mulai yang telah selesai dengan sukses.
Daftar Direktori Konektor SFTP Gagal	Daftar direktori file awal yang gagal.
Konektor SFTP Remote Move Selesai	File atau direktori telah dipindahkan atau diganti namanya dengan sukses di server jarak jauh.
Pindah Jarak Jauh Konektor SFTP Gagal	File atau direktori gagal dipindahkan atau diganti namanya di server jarak jauh.
Penghapusan Jarak Jauh Konektor SFTP Selesai	File atau direktori telah berhasil dihapus di server jarak jauh.
Penghapusan Jarak Jauh Konektor SFTP Gagal	File atau direktori gagal dihapus di server jarak jauh.

Acara AS2

Note

Acara ini dikirimkan ke EventBridge tingkat tahan lama, seperti yang dijelaskan dalam [tingkat Pengiriman untuk acara AWS layanan](#) di Referensi EventBridge Acara Amazon.

Jenis detail acara	Deskripsi
Terima Muatan AS2 Selesai	Muatan untuk pesan AS2 telah diterima.
Penerimaan Muatan AS2 Gagal	Muatan untuk pesan AS2 belum diterima.
Kirim Muatan AS2 Selesai	Payload untuk pesan AS2 telah berhasil dikirim.
Kirim Muatan AS2 Gagal	Muatan untuk pesan AS2 gagal dikirim.
AS2 MDN Terima Selesai	Pemberitahuan disposisi pesan untuk pesan AS2 telah diterima.
AS2 MDN Menerima Gagal	Pemberitahuan disposisi pesan untuk pesan AS2 belum diterima.
AS2 MDN Kirim Selesai	Pemberitahuan disposisi pesan untuk pesan AS2 telah berhasil dikirim.
AS2 MDN Kirim Gagal	Pemberitahuan disposisi pesan untuk pesan AS2 gagal dikirim.

Mengirim Transfer Family peristiwa dengan menggunakan EventBridge aturan

Jika Anda ingin bus acara EventBridge default mengirim Transfer Family acara ke target, Anda harus membuat aturan yang berisi pola peristiwa yang cocok dengan data dalam Transfer Family acara yang Anda inginkan.

Untuk menangkap AWS Transfer Family peristiwa di Amazon EventBridge

1. Masuk ke Konsol Manajemen AWS dan buka EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, pilih Aturan, lalu pilih Buat aturan.
3. Masukkan nama deskriptif untuk aturan, dan secara opsional masukkan deskripsi.
4. Untuk jenis Aturan, pilih Aturan dengan pola acara lalu pilih Berikutnya.
5. Di bagian Sumber acara, pilih AWS acara atau acara EventBridge mitra.
6. Di bagian Metode pembuatan, pilih Gunakan formulir pola.

7. Di bagian Pola acara, berikan informasi berikut.

- a. Untuk Sumber peristiwa, pilih Layanan AWS .
- b. Untuk AWS layanan, pilih Transfer.
- c. Untuk jenis Acara, pilih jenis acara Transfer Family yang ingin memicu aturan Anda.

Tergantung pada pilihan jenis Acara Anda, Anda mungkin akan disajikan dengan bagian Spesifikasi Jenis Acara 1.

- d. Jika Anda melihat bagian Spesifikasi Jenis Acara 1, pilih peristiwa tertentu yang ingin Anda ambil (atau pilih Setiap peristiwa untuk menangkap semua acara untuk jenis acara yang Anda pilih).
 - e. (Opsional) Gunakan editor pola acara untuk menentukan filter untuk detail acara.
 - f. Pilih Berikutnya.
8. Pilih target dari pilihan yang tersedia di Pilih target. Pilih dari target yang tersedia berikut.

- AWS layanan. Opsi populer adalah fungsi Lambda untuk komputasi tanpa server, antrian Amazon SQS untuk pemrosesan pesan, topik Amazon SNS untuk notifikasi, dan untuk mengatur alur kerja. AWS Step Functions
- EventBridge Tujuan API. Jika Anda ingin mengirim peristiwa ke titik akhir HTTP di luar AWS, Anda dapat menggunakan API Destination sebagai target Anda.
- EventBridge bus acara. Anda dapat mengirim acara ke bus acara lain, baik di akun dan wilayah yang sama atau di akun atau wilayah yang berbeda.

Untuk petunjuk komprehensif tentang cara membuat aturan bus acara, lihat [Membuat aturan yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon.

Untuk bantuan dalam memilih target, lihat [Pilih target](#) di Panduan EventBridge Pengguna Amazon.

9. Konfigurasikan opsi tambahan apa pun untuk target Anda lalu pilih Berikutnya.
10. (Opsional) Tambahkan tag ke aturan Anda dan pilih Berikutnya.
11. Di layar Tinjau dan buat, jika semuanya terlihat bagus, pilih Buat aturan.

Membuat pola acara untuk Transfer Family peristiwa

Saat Transfer Family mengirimkan acara ke bus acara default, EventBridge gunakan pola acara yang ditentukan untuk setiap aturan untuk menentukan apakah acara harus dikirim ke target aturan. Pola peristiwa cocok dengan data dalam Transfer Family peristiwa yang diinginkan. Setiap pola acara adalah objek JSON yang berisi berikut:

- `sourceAtribut` yang mengidentifikasi layanan yang mengirim acara. Untuk Transfer Family acara, sumbernya adalah `aws.transfer`.
- (Opsional) `detail-type Atribut` yang berisi array dari jenis acara untuk dicocokkan.
- (Opsional) `detail Atribut` yang berisi data peristiwa lain yang cocok.

Misalnya, pola acara berikut cocok dengan semua peristiwa dari Transfer Family:

```
{
  "source": ["aws.transfer"]
}
```

Contoh pola peristiwa berikut cocok dengan semua peristiwa konektor SFTP:

```
{
  "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"]
}
```

Contoh pola acara berikut cocok dengan semua peristiwa gagal Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

Contoh pola peristiwa berikut cocok dengan unduhan SFTP yang berhasil untuk pengguna:

username

```
{
```

```
"source": ["aws.transfer"],
"detail-type": ["SFTP Server File Download Completed"],
"detail": {
  "username": [username]
}
}
```

Untuk informasi selengkapnya tentang penulisan pola acara, lihat [Pola acara](#) di Panduan EventBridge Pengguna.

Menguji pola acara untuk Transfer Family peristiwa di EventBridge

Anda dapat menggunakan EventBridge Sandbox untuk mendefinisikan dan menguji pola peristiwa dengan cepat, tanpa harus menyelesaikan proses pembuatan atau pengeditan aturan yang lebih luas. Menggunakan Sandbox, Anda dapat menentukan pola peristiwa dan menggunakan contoh peristiwa untuk mengonfirmasi bahwa pola tersebut cocok dengan peristiwa yang diinginkan. EventBridge memberi Anda pilihan untuk membuat aturan baru dengan menggunakan pola acara itu langsung dari kotak pasir.

Untuk informasi selengkapnya, lihat [Menguji pola peristiwa menggunakan EventBridge Kotak Pasir](#) di Panduan EventBridge Pengguna.

Amazon EventBridge izin

Transfer Family tidak memerlukan izin tambahan untuk mengirimkan acara ke Amazon EventBridge.

Target yang Anda tentukan mungkin memerlukan izin atau konfigurasi tertentu. Untuk detail selengkapnya tentang penggunaan layanan khusus untuk target, lihat [Amazon EventBridge target](#) di Panduan Amazon EventBridge Pengguna.

Tambahan EventBridge sumber daya

Lihat topik-topik berikut di [Panduan Amazon EventBridge Pengguna](#) untuk informasi lebih lanjut tentang cara menggunakan EventBridge untuk memproses dan mengelola acara.

- Untuk informasi rinci tentang cara kerja bus acara, lihat [bus Amazon EventBridge acara](#).
- Untuk informasi tentang struktur acara, lihat [Acara](#).
- Untuk informasi tentang membuat pola peristiwa untuk EventBridge digunakan saat mencocokkan peristiwa dengan aturan, lihat [Pola acara](#).

- Untuk informasi tentang membuat aturan untuk menentukan EventBridge proses peristiwa, lihat [Aturan](#).
- Untuk informasi tentang cara menentukan layanan atau tujuan lain yang EventBridge mengirimkan peristiwa yang cocok, lihat [Target](#).

Transfer Family referensi detail acara

Semua peristiwa dari AWS layanan memiliki seperangkat bidang umum yang berisi metadata tentang acara tersebut. Metadata ini dapat mencakup AWS layanan yang merupakan sumber acara, waktu acara dibuat, akun dan Wilayah tempat acara berlangsung, dan lainnya. Untuk definisi bidang umum ini, lihat [Referensi struktur acara](#) di Panduan Amazon EventBridge Pengguna.

Selain itu, setiap acara memiliki detail bidang yang berisi data khusus untuk peristiwa tertentu. Referensi berikut mendefinisikan bidang detail untuk berbagai Transfer Family acara.

Saat Anda menggunakan EventBridge untuk memilih dan mengelola Transfer Family acara, pertimbangkan hal berikut:

- `sourceBidang` untuk semua acara dari Transfer Family diatur ke `aws.transfer`.
- `detail-typeBidang` menentukan jenis acara.

Misalnya, `FTP Server File Download Completed`.

- `detailBidang` berisi data yang spesifik untuk peristiwa tertentu.

Untuk informasi tentang membuat pola peristiwa yang memungkinkan aturan untuk mencocokkan Transfer Family peristiwa, lihat [Pola acara](#) di Panduan Amazon EventBridge Pengguna.

Untuk informasi selengkapnya tentang peristiwa dan cara EventBridge memprosesnya, lihat [Amazon EventBridge peristiwa](#) di Panduan Amazon EventBridge Pengguna.

Topik

- [Acara server SFTP, FTPS, dan FTP](#)
- [Acara konektor SFTP](#)
- [Acara AS2](#)

Acara server SFTP, FTPS, dan FTP

Berikut ini adalah bidang detail untuk acara server SFTP, FTPS, dan FTP:

- Direktori Server FTP Membuat Selesai
- Membuat Direktori Server FTP Gagal
- Penghapusan Direktori Server FTP Selesai
- Penghapusan Direktori Server FTP Gagal
- Penghapusan File Server FTP Selesai
- Penghapusan File Server FTP Gagal
- Unduhan File Server FTP Selesai
- Unduhan File Server FTP Gagal
- Ganti Nama File Server FTP Selesai
- Gagal Mengganti Nama File Server FTP
- Unggahan File Server FTP Selesai
- Unggahan File Server FTP Gagal
- Direktori Server FTPS Membuat Selesai
- Pembuatan Direktori Server FTPS Gagal
- Penghapusan Direktori Server FTPS Selesai
- Penghapusan Direktori Server FTPS Gagal
- Penghapusan File Server FTPS Selesai
- Penghapusan File Server FTPS Gagal
- Unduhan File Server FTPS Selesai
- Unduhan File Server FTPS Gagal
- Ganti Nama File Server FTPS Selesai
- Gagal Mengganti Nama File Server FTPS
- Unggahan File Server FTPS Selesai
- Unggahan File Server FTPS Gagal
- Direktori Server SFTP Membuat Selesai
- Pembuatan Direktori Server SFTP Gagal
- Penghapusan Direktori Server SFTP Selesai

- Penghapusan Direktori Server SFTP Gagal
- Penghapusan File Server SFTP Selesai
- Penghapusan File Server SFTP Gagal
- Unduhan File Server SFTP Selesai
- Unduhan File Server SFTP Gagal
- Ganti Nama File Server SFTP Selesai
- Gagal Mengganti Nama File Server SFTP
- Unggahan File Server SFTP Selesai
- Unggahan File Server SFTP Gagal

detail-typeBidang source dan disertakan di bawah ini karena mengandung nilai khusus untuk Transfer Family acara. Untuk definisi bidang metadata lain yang disertakan dalam semua peristiwa, lihat [Referensi struktur acara](#) di Amazon EventBridge Panduan Pengguna.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

detail-type

Mengidentifikasi jenis acara.

Untuk acara ini, nilainya adalah salah satu nama acara server SFTP, FTPS, atau FTP yang tercantum sebelumnya.

source

Mengidentifikasi layanan yang menghasilkan peristiwa. Untuk acara Transfer Family, nilai ini adalah `aws.transfer`.

detail

Objek JSON yang berisi informasi tentang peristiwa. Layanan yang menghasilkan acara menentukan konten bidang ini.

Untuk acara ini, data meliputi yang berikut:

failure-code

Kategori mengapa transfer gagal. Nilai: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

status-code

Apakah transfer berhasil. Nilai: `COMPLETED` | `FAILED`.

protocol

Protokol yang digunakan untuk transfer. Nilai: `SFTP` | `FTPS` | `FTP`

bytes

Jumlah byte yang ditransfer.

client-ip

Alamat IP untuk klien yang terlibat dalam transfer

failure-message

Untuk transfer yang gagal, detail mengapa transfer gagal.

end-timestamp

Untuk transfer yang berhasil, stempel waktu ketika file selesai diproses.

etag

Tag entitas (hanya digunakan untuk file Amazon S3).

file-path

Jalur ke file yang ditransfer, dihapus, atau dioperasikan.

original-file-path

Untuk acara ganti nama file, jalur asli file sebelum mengganti nama.

renamed-file-path

Untuk acara ganti nama file, jalur baru file setelah mengganti nama.

directory-path

Untuk direktori membuat dan menghapus peristiwa, jalur direktori.

server-id

ID unik untuk server Transfer Family.

username

Pengguna yang melakukan transfer.

session-id

Pengidentifikasi unik untuk sesi transfer.

start-timestamp

Untuk transfer yang berhasil, stempel waktu saat pemrosesan file dimulai.

Example Unduhan File Server SFTP Gagal contoh peristiwa

Contoh berikut menunjukkan peristiwa di mana unduhan gagal di server SFTP (Amazon EFS adalah penyimpanan yang digunakan).

```
{
  "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 Unggah File Server FTP Contoh acara selesai

Contoh berikut menunjukkan peristiwa di mana unggahan berhasil diselesaikan pada server FTP (Amazon S3 adalah penyimpanan yang digunakan).

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "FTP Server File Upload Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T16:31:43Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "FTP",
        "bytes": 1048576,
        "client-ip": "10.0.0.141",
        "end-timestamp": "2024-01-29T16:31:43.311866408Z",
    }
}

```

```

    "etag": "b6d81b360a5672d80c27430f39153e2c",
    "file-path": "/amzn-s3-demo-bucket/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}

```

Example Hapus File Server SFTP Contoh acara yang lengkap

Contoh berikut menunjukkan peristiwa di mana file berhasil dihapus pada server SFTP.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}

```

Example Ganti Nama File Server SFTP Contoh acara yang lengkap

Contoh berikut menunjukkan peristiwa di mana file berhasil diganti namanya pada server SFTP.

```

{
  "version": "0",

```

```

    "id": "event-ID",
    "detail-type": "SFTP Server File Rename Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T15:45:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T15:45:12.749749117Z",
        "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
        "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2025-05-15T15:45:11.706282454Z"
    }
}

```

Example Direktori Server SFTP Buat contoh acara Selesai

Contoh berikut menunjukkan peristiwa di mana direktori berhasil dibuat pada server SFTP.

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server Directory Create Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T16:20:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T16:20:05.749749117Z",
        "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
    }
}

```

```
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T16:20:04.706282454Z"
  }
}
```

Acara konektor SFTP

Note

Acara ini dikirimkan ke EventBridge tingkat tahan lama, seperti yang dijelaskan dalam [tingkat Pengiriman untuk acara AWS layanan](#) di Referensi EventBridge Acara Amazon.

Berikut ini adalah bidang detail untuk acara konektor SFTP:

- Kirim File Konektor SFTP Selesai
- Kirim File Konektor SFTP Gagal
- Pengambilan File Konektor SFTP Selesai
- Pengambilan File Konektor SFTP Gagal
- Daftar Direktori Konektor SFTP Selesai
- Daftar Direktori Konektor SFTP Gagal
- Konektor SFTP Remote Move Selesai
- Pindah Jarak Jauh Konektor SFTP Gagal
- Penghapusan Jarak Jauh Konektor SFTP Selesai
- Penghapusan Jarak Jauh Konektor SFTP Gagal

`detail-type` Bidang source dan disertakan di bawah ini karena mengandung nilai khusus untuk Transfer Family acara. Untuk definisi bidang metadata lain yang disertakan dalam semua peristiwa, lihat [Referensi struktur acara](#) di Amazon EventBridge Panduan Pengguna.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
}
```

```

. . .,
"detail": {
  "operation" : "string",
  "max-items" : "number",
  "connector-id" : "string",
  "output-directory-path" : "string",
  "listing-id" : "string",
  "transfer-id" : "string",
  "file-transfer-id" : "string",
  "url" : "string",
  "file-path" : "string",
  "status-code" : "string",
  "failure-code" : "string",
  "failure-message" : "string",
  "start-timestamp" : "string",
  "end-timestamp" : "string",
  "local-directory-path" : "string",
  "remote-directory-path" : "string",
  "item-count" : "number",
  "truncated" : "boolean",
  "bytes" : "number",
  "egress-type" : "string",
  "vpc-lattice-resource-configuration-arn" : "string",
  "vpc-lattice-port-number" : "number",
  "local-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  },
  "output-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  }
}
}
}

```

detail-type

Mengidentifikasi jenis acara.

Untuk acara ini, nilainya adalah salah satu nama acara konektor SFTP yang tercantum sebelumnya.

source

Mengidentifikasi layanan yang menghasilkan peristiwa. Untuk Transfer Family acara, nilai ini adalah `aws.transfer`.

detail

Objek JSON yang berisi informasi tentang peristiwa. Layanan yang menghasilkan acara menentukan konten bidang ini.

Untuk acara ini, data meliputi yang berikut:

max-items

Jumlah maksimum directory/file nama untuk dikembalikan.

operation

Apakah `StartFileTransfer` permintaan mengirim atau mengambil file. Nilai: `SEND` | `RETRIEVE`.

connector-id

Pengidentifikasi unik untuk konektor SFTP yang digunakan.

output-directory-path

Jalur (bucket dan awalan) di Amazon S3 untuk menyimpan hasil listing. file/directory

listing-id

Pengidentifikasi unik untuk operasi `StartDirectoryListing` API. Pengenal ini dapat digunakan untuk memeriksa CloudWatch log untuk melihat status permintaan daftar.

transfer-id

Pengenal unik untuk acara transfer (`StartFileTransfer` permintaan).

file-transfer-id

Pengidentifikasi unik untuk file yang ditransfer.

url

URL titik akhir AS2 atau SFTP mitra.

file-path

Lokasi dan file yang sedang dikirim atau diambil.

status-code

Apakah transfer berhasil. Nilai:FAILED | COMPLETED.

failure-code

Untuk transfer yang gagal, kode alasan mengapa transfer gagal. Nilai:ASSUME_ROLE_ERROR | UNSUPPORTED_OPERATION_ERROR | CONNECTION_ERROR | READ_FILE_ERROR | WRITE_FILE_ERROR | TIMEOUT_ERROR | LIST_DIRECTORY_ERROR | SEND_FILE_NOT_FOUND | RETRIEVE_FILE_NOT_FOUND | DIRECTORY_NOT_FOUND | FILE_NOT_FOUND | PATH_NOT_FOUND | RENAME_ERROR | DELETE_ERROR | INTERNAL_ERROR | UNKNOWN_ERROR.

failure-message

Untuk transfer yang gagal, detail mengapa transfer gagal.

start-timestamp

Untuk transfer yang berhasil, stempel waktu saat pemrosesan file dimulai.

end-timestamp

Untuk transfer yang berhasil, stempel waktu saat pemrosesan file selesai.

local-directory-path

Untuk RETRIEVE permintaan, lokasi di mana untuk menempatkan file yang diambil.

remote-directory-path

Untuk SEND permintaan, direktori file tempat menempatkan file di server SFTP mitra. Ini adalah nilai untuk RemoteDirectoryPath yang diteruskan pengguna ke StartFileTransfer permintaan. Anda dapat menentukan direktori default di server SFTP mitra. Jika demikian, bidang ini kosong.

item-count

Jumlah item (direktori dan file) yang dikembalikan untuk permintaan daftar.

truncated

Apakah output daftar berisi semua item yang terkandung dalam direktori jarak jauh atau tidak.

bytes

Jumlah byte yang ditransfer. Nilainya adalah 0 untuk transfer yang gagal.

`egress-type`

Jenis konfigurasi jalan keluar untuk konektor. Nilai: `SERVICE_MANAGED` atau `VPC_LATTICE`.

`vpc-lattice-resource-configuration-arn`

ARN dari Konfigurasi Sumber Daya `VPC_LATTICE` yang mendefinisikan lokasi server SFTP target. Bidang ini adalah nol untuk konektor yang dikelola layanan.

`vpc-lattice-port-number`

Nomor port untuk menghubungkan ke server SFTP melalui `VPC_LATTICE`.

`local-file-location`

Parameter ini berisi rincian lokasi file AWS penyimpanan.

`domain`

Penyimpanan yang digunakan. Saat ini, satu-satunya nilai adalah `S3`.

`bucket`

Wadah untuk objek di Amazon S3.

`key`

Nama yang ditetapkan untuk objek di Amazon S3.

`output-file-location`

Parameter ini berisi rincian lokasi tempat menyimpan hasil daftar direktori dalam AWS penyimpanan.

`domain`

Penyimpanan yang digunakan. Saat ini, satu-satunya nilai adalah `S3`.

`bucket`

Wadah untuk objek di Amazon S3.

`key`

Nama yang ditetapkan untuk objek di Amazon S3.

Example SFTP Connector File Kirim contoh peristiwa gagal

Contoh berikut menunjukkan peristiwa di mana konektor SFTP gagal saat mencoba mengirim file ke server SFTP jarak jauh.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Send Failed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T19:30:45Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "SEND",
    "connector-id": "c-f1111aaaa2222bbbb3",
    "transfer-id": "transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/testfile.txt",
    "status-code": "FAILED",
    "failure-code": "CONNECTION_ERROR",
    "failure-message": "Unknown Host",
    "remote-directory-path": "",
    "bytes": 0,
    "start-timestamp": "2024-01-24T18:29:33.658729Z",
    "end-timestamp": "2024-01-24T18:29:33.993196Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}
```

Example File Konektor SFTP Mengambil contoh acara yang lengkap

Contoh berikut menunjukkan peristiwa di mana konektor SFTP berhasil mengambil file yang dikirim dari server SFTP jarak jauh.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Retrieve Completed",
  "source": "aws.transfer",
```

```

"account": "123456789012",
"time": "2024-01-24T18:28:08Z",
"region": "us-east-1",
"resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
],
"detail": {
    "operation": "RETRIEVE",
    "connector-id": "c-fc68000012345aa18",
    "transfer-id": "file-transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "testfile.txt",
    "status-code": "COMPLETED",
    "local-directory-path": "/amzn-s3-demo-bucket",
    "bytes": 63533,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "local-file-location": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "testfile.txt"
    }
}
}

```

Example Daftar Direktori Konektor SFTP Contoh acara lengkap

Contoh berikut menunjukkan peristiwa di mana panggilan daftar direktori awal diambil file daftar dari server SFTP jarak jauh.

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector Directory Listing Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {

```

```
{
  "max-items": 10000,
  "connector-id": "c-fc68000012345aa18",
  "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
  "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
  "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

  "status-code": "COMPLETED",
  "remote-directory-path": "/home",
  "item-count": 10000,
  "truncated": true,
  "start-timestamp": "2024-01-24T18:28:07.632388Z",
  "end-timestamp": "2024-01-24T18:28:07.774898Z",
  "output-file-location": {
    "domain": "S3",
    "bucket": "amzn-s3-demo-bucket",
    "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
  }
}
```

Acara AS2

Note

Acara ini dikirimkan ke EventBridge tingkat tahan lama, seperti yang dijelaskan dalam [tingkat Pengiriman untuk acara AWS layanan](#) di Referensi EventBridge Acara Amazon.

Berikut ini adalah bidang detail untuk acara AS2:

- Terima Muatan AS2 Selesai
- Penerimaan Muatan AS2 Gagal
- Kirim Muatan AS2 Selesai
- Kirim Muatan AS2 Gagal
- AS2 MDN Terima Selesai
- AS2 MDN Menerima Gagal
- AS2 MDN Kirim Selesai
- AS2 MDN Kirim Gagal

detail-typeBidang source dan disertakan di bawah ini karena mengandung nilai khusus untuk Transfer Family acara. Untuk definisi bidang metadata lain yang disertakan dalam semua peristiwa, lihat [Referensi struktur acara](#) di Amazon EventBridge Panduan Pengguna.

```
{
  . . . ,
  "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

Mengidentifikasi jenis acara.

Untuk acara ini, nilainya adalah salah satu peristiwa AS2 yang tercantum sebelumnya.

`source`

Mengidentifikasi layanan yang menghasilkan peristiwa. Untuk Transfer Family acara, nilai ini adalah `aws.transfer`.

`detail`

Objek JSON yang berisi informasi tentang peristiwa. Layanan yang menghasilkan acara menentukan konten bidang ini.

`s3-attributes`

Mengidentifikasi bucket dan kunci Amazon S3 untuk file yang ditransfer. Untuk acara MDN, ini juga mengidentifikasi bucket dan kunci untuk file MDN.

`file-bucket`

Wadah untuk objek di Amazon S3.

`file-key`

Nama yang ditetapkan untuk objek di Amazon S3.

`json-bucket`

Untuk transfer SELESAI atau GAGAL, wadah untuk file JSON.

`json-key`

Untuk transfer SELESAI atau GAGAL, nama yang ditetapkan ke file JSON di Amazon S3.

`mdn-bucket`

Untuk acara MDN, wadah untuk file MDN.

`mdn-key`

Untuk peristiwa MDN, nama ditetapkan ke file MDN di Amazon S3.

`mdn-subject`

Untuk acara MDN, deskripsi teks untuk disposisi pesan.

`mdn-message-id`

Untuk acara MDN, ID unik untuk pesan MDN.

disposition

Untuk acara MDN, kategori untuk disposisi.

bytes

Jumlah byte dalam pesan.

as2-from

Mitra dagang AS2 yang mengirim pesan.

as2-message-id

Pengidentifikasi unik untuk pesan AS2 yang ditransfer.

as2-to

Mitra dagang AS2 yang menerima pesan.

connector-id

Untuk pesan AS2 yang dikirim dari server Transfer Family ke mitra dagang, pengenalan unik untuk konektor AS2 digunakan.

client-ip

Untuk kejadian server (transfer dari mitra dagang ke server Transfer Family), alamat IP untuk klien yang terlibat dalam transfer.

agreement-id

Untuk peristiwa server, pengenalan unik untuk perjanjian AS2.

server-id

Untuk kejadian server, ID unik hanya untuk server Transfer Family.

requester-file-name

Untuk acara payload, nama asli untuk file yang diterima selama transfer.

message-subject

Deskripsi teks untuk subjek pesan.

start-timestamp

Untuk transfer yang berhasil, stempel waktu saat pemrosesan file dimulai.

end-timestamp

Untuk transfer yang berhasil, stempel waktu saat pemrosesan file selesai.

status-code

Kode yang sesuai dengan keadaan proses transfer pesan AS2. Nilai yang valid: COMPLETED | FAILED | PROCESSING.

failure-code

Untuk transfer yang gagal, kategori mengapa transfer gagal.

failure-message

Untuk transfer yang gagal, detail mengapa transfer gagal.

transfer-id

Pengidentifikasi unik untuk acara transfer.

Example AS2 Payload Receive Contoh acara Selesai

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 Payload Receive Completed",
  "source": "aws.transfer",
  "account": "076722215406",
  "time": "2024-02-07T06:47:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/
c-1111aaaa2222bbbb3"],
  "detail": {
    "s3-attributes": {
      "file-key": "/inbound/processed/testAs2Message.dat",
      "file-bucket": "amzn-s3-demo-bucket"
    },
    "client-ip": "client-IP-address",
    "requester-file-name": "testAs2MessageVerifyFile.dat",
    "end-timestamp": "2024-02-07T06:47:06.040031Z",
    "as2-from": "as2-from-ID",
    "as2-message-id": "as2-message-ID",
    "message-subject": "Message from AS2 tests",
    "start-timestamp": "2024-02-07T06:47:05.410Z",
```



```

    "status-code": "PROCESSING",
    "bytes": 63,
    "as2-to": "as2-to-ID",
    "agreement-id": "a-1111aaaa2222bbbb3",
    "server-id": "s-1234abcd5678efghi"
  }
}

```

Example AS2 MDN Menerima contoh peristiwa Gagal

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
  "detail": {
    "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde to partner ijklmnop987654",
    "s3-attributes": {
      "json-bucket": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-bucket2",
      "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
    },
    "mdn-message-id": "MDN-message-ID",
    "end-timestamp": "2024-02-06T22:05:09.479878Z",
    "as2-from": "PartnerA",
    "as2-message-id": "as2-message-ID",
    "connector-id": "c-1234abcd5678efghj",
    "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
    "start-timestamp": "2024-02-06T22:05:03Z",
    "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
    "status-code": "FAILED",
    "as2-to": "MyCompany",
    "failure-message": "No public certificate matching message signature could be found in profile: p-1234abcd5678efghj",
    "transfer-id": "transfer-ID"
  }
}

```

Keamanan di AWS Transfer Family

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#).

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi AWS Keamanan](#).

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Transfer Family. Topik berikut menunjukkan cara mengonfigurasi AWS Transfer Family untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Transfer Family sumber daya Anda.

Kami menawarkan lokakarya yang menyediakan panduan preskriptif dan lab langsung tentang bagaimana Anda dapat membangun arsitektur transfer file yang terukur dan aman AWS tanpa perlu memodifikasi aplikasi yang ada atau mengelola infrastruktur server. Anda dapat melihat detail untuk lokakarya ini [di sini](#).

Topik

- [Manfaat keamanan konektivitas VPC](#)
- [Kebijakan keamanan untuk AWS Transfer Family server](#)
- [Kebijakan keamanan untuk AWS Transfer Family Konektor SFTP](#)
- [Menggunakan pertukaran kunci pasca-kuantum hibrida dengan AWS Transfer Family](#)
- [Perlindungan data dan enkripsi](#)

- [Mengelola kunci SSH dan PGP di Transfer Family](#)
- [Identitas dan manajemen akses untuk AWS Transfer Family](#)
- [Validasi kepatuhan untuk AWS Transfer Family](#)
- [Ketahanan di AWS Transfer Family](#)
- [Buat koneksi pribadi antara VPC dan AWS Transfer Family API](#)
- [Keamanan infrastruktur di AWS Transfer Family](#)
- [Tambahkan firewall aplikasi web](#)
- [Cross-service pencegahan wakil bingung](#)
- [AWS kebijakan terkelola untuk AWS Transfer Family](#)

Manfaat keamanan konektivitas VPC

Konektor SFTP dengan tipe jalan keluar VPC memberikan manfaat keamanan yang ditingkatkan melalui Akses Sumber Daya: Cross-VPC

- Isolasi jaringan: Semua lalu lintas tetap berada dalam lingkungan VPC Anda, menyediakan isolasi jaringan lengkap dari internet publik untuk koneksi titik akhir pribadi.
- Kontrol IP sumber: Server SFTP jarak jauh hanya melihat alamat IP dari rentang CIDR VPC Anda, memberi Anda kontrol penuh atas alamat IP sumber yang digunakan untuk koneksi.
- Akses endpoint pribadi: Sambungkan langsung ke server SFTP di VPC Anda menggunakan alamat IP pribadi, menghilangkan paparan ke internet publik.
- Konektivitas hibrida: Akses server SFTP lokal dengan aman melalui koneksi VPN atau Direct Connect yang sudah mapan tanpa eksposur internet tambahan.
- Kontrol keamanan VPC: Manfaatkan grup keamanan VPC, NACL, dan kebijakan perutean yang ada untuk mengontrol dan memantau lalu lintas konektor SFTP.

Model keamanan VPC Lattice

Konektivitas VPC untuk konektor SFTP menggunakan AWS VPC Lattice dengan jaringan layanan untuk menyediakan akses multi-tenant yang aman:

- Pencegahan wakil yang membingungkan: Pemeriksaan otentikasi dan otorisasi memastikan bahwa konektor hanya dapat mengakses sumber daya spesifik tempat mereka dikonfigurasi, mencegah akses penyewa silang yang tidak sah.

- IPv6-only jaringan layanan: Menggunakan pengalamatan IPv6 untuk menghindari potensi konflik alamat IP dan meningkatkan isolasi keamanan.
- Forward Access Session (FAS): Penanganan kredensial sementara menghilangkan kebutuhan akan penyimpanan kredensial jangka panjang atau berbagi sumber daya manual.
- Resource-level kontrol akses: Setiap konektor dikaitkan dengan Konfigurasi Sumber Daya tertentu, memastikan kontrol akses granular ke server SFTP individual.

Praktik terbaik keamanan untuk konektivitas VPC

Saat menggunakan konektor tipe jalan keluar VPC, ikuti praktik terbaik keamanan berikut:

- Grup keamanan: Konfigurasikan grup keamanan untuk memungkinkan lalu lintas SFTP (port 22) hanya di antara sumber daya yang diperlukan. Batasi rentang IP sumber dan tujuan ke minimum yang diperlukan.
- Penempatan Resource Gateway: Terapkan Resource Gateways di subnet pribadi bila memungkinkan, dan pastikan mereka menjangkau setidaknya dua Availability Zone untuk ketersediaan tinggi.
- Pemantauan jaringan: Gunakan VPC Flow Logs dan Amazon CloudWatch untuk memantau pola lalu lintas jaringan dan mendeteksi aktivitas anomali.
- Pencatatan akses: Aktifkan pencatatan konektor untuk melacak aktivitas transfer file dan memelihara jejak audit untuk persyaratan kepatuhan.
- Manajemen Konfigurasi Sumber Daya: Secara teratur meninjau dan memperbarui Konfigurasi Sumber Daya untuk memastikan mereka menunjuk ke server SFTP yang benar dan menggunakan pengaturan jaringan yang sesuai.

Kebijakan keamanan untuk AWS Transfer Family server

Kebijakan keamanan server AWS Transfer Family memungkinkan Anda untuk membatasi set algoritma kriptografi (kode otentikasi pesan (MAC), pertukaran kunci (KEX), cipher suite, cipher enkripsi konten, dan algoritma hash) yang terkait dengan server Anda.

AWS Transfer Family mendukung kebijakan keamanan pasca-kuantum yang menggunakan algoritma pertukaran kunci hibrida, menggabungkan metode kriptografi tradisional dengan algoritma pasca-kuantum untuk memberikan keamanan yang ditingkatkan terhadap ancaman komputasi kuantum masa depan. Untuk informasi selengkapnya, lihat [Menggunakan pertukaran kunci pasca-kuantum hibrida dengan AWS Transfer Family](#).

Untuk daftar algoritma kriptografi yang didukung, lihat [Algoritma kriptografi](#). Untuk daftar algoritme kunci yang didukung untuk digunakan dengan kunci host server dan kunci pengguna yang dikelola layanan, lihat [Mengelola kunci SSH dan PGP di Transfer Family](#).

 Note

Mulai tahun 2025, semua kebijakan AWS Transfer Family keamanan baru mencakup dukungan kriptografi pasca-kuantum menggunakan algoritma pertukaran kunci hibrida. Untuk informasi lebih lanjut tentang keamanan pasca-kuantum, lihat [Menggunakan pertukaran kunci pasca-kuantum hibrida dengan AWS Transfer Family](#).

 Note

Kami sangat menyarankan untuk memperbarui server Anda ke kebijakan keamanan terbaru kami.

- `TransferSecurityPolicy-2024-01` adalah kebijakan keamanan default yang dilampirkan ke server Anda saat membuat server menggunakan konsol, API, atau CLI.
- Jika Anda membuat server Transfer Family menggunakan CloudFormation dan menerima kebijakan keamanan default, server akan ditetapkan `TransferSecurityPolicy-2018-11`.

Jika Anda khawatir tentang kompatibilitas klien, harap sebutkan kebijakan keamanan mana yang ingin Anda gunakan saat membuat atau memperbarui server daripada menggunakan kebijakan default, yang dapat berubah sewaktu-waktu. Untuk mengubah kebijakan keamanan server, lihat [Edit kebijakan keamanan](#).

 Note

Kebijakan kuantum pasca sebelumnya (`TransferSecurityPolicy-PQ-SSH-Experimental-2023-04` dan `TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04`) tidak digunakan lagi. Kami menyarankan Anda menggunakan kebijakan baru sebagai gantinya.

Untuk informasi selengkapnya tentang keamanan di Transfer Family, lihat postingan blog berikut ini:

- [Enam tips untuk meningkatkan keamanan AWS Transfer Family server Anda](#)
- [Bagaimana Transfer Family dapat membantu Anda membangun solusi transfer file terkelola yang aman dan sesuai](#)

Topik

- [Algoritma kriptografi](#)
- [Detail kebijakan keamanan](#)

Algoritma kriptografi

Untuk kunci host, kami mendukung algoritma berikut:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

Selain itu, kebijakan keamanan berikut memungkinkan `ssh-rsa`:

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`
- `TransferSecurityPolicy-FIPS-2023-05`
- `TransferSecurityPolicy-FIPS-2024-01`

Note

Penting untuk memahami perbedaan antara tipe kunci RSA — yang selalu `ssh-rsa` — dan algoritma kunci host RSA, yang dapat berupa salah satu algoritma yang didukung.

Berikut ini adalah daftar algoritma kriptografi yang didukung untuk setiap kebijakan keamanan.

 Note

Dalam tabel dan kebijakan berikut, perhatikan penggunaan jenis algoritma berikut.

- Server SFTP hanya menggunakan algoritma di SshCiphers, SshKexs, dan bagian. SshMacs
- Server FTPS hanya menggunakan algoritma di bagian ini. TlsCiphers
- Server FTP, karena mereka tidak menggunakan enkripsi, tidak menggunakan algoritme ini.
- Server AS2 hanya menggunakan algoritma di bagian ContentEncryptionCiphers dan HashAlgorithms. Bagian ini mendefinisikan algoritma yang digunakan untuk mengenkripsi dan menandatangani konten file.
- Kebijakan FIPS-2024-05 dan FIPS-2024-01 keamanan identik, kecuali yang FIPS-2024-05 tidak mendukung `ssh-rsa` algoritma.
- Transfer Family telah memperkenalkan kebijakan terbatas baru yang paralel erat dengan kebijakan yang ada:
 - Kebijakan TransferSecurityPolicy-Restricted-2018-11 dan TransferSecurityPolicy-2018-11 keamanan identik, kecuali bahwa kebijakan terbatas tidak mendukung `chacha20-poly1305@openssh.com` cipher.
 - Kebijakan TransferSecurityPolicy-Restricted-2020-06 dan TransferSecurityPolicy-2020-06 keamanan identik, kecuali bahwa kebijakan terbatas tidak mendukung `chacha20-poly1305@openssh.com` cipher.

* Dalam tabel berikut, `chacha20-poly1305@openssh.com` sandi disertakan dalam kebijakan yang tidak dibatasi saja,

652

Kebijakan Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer	Transfer
keamanan	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	Security	SecurityPo
	licy-2025-03	licy-2025-08	licy-2025-08	licy-2025-07	licy-2024-01	licy-2024-01	licy-2023-05	licy-2023-05	licy-2020-06	licy-2020-06	licy-2020-06	licy-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditComes	restricted		-2024-01/		-2023-05		dan	-2020-06	dan
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11

SshKexs												
mlkem768x	◆			◆								
25519-sha256												
mlkem768n	◆			◆								
istp256-s												
ha256												
mlkem1024	◆			◆								
nistp384-sha384												
kurva25519-sha256		◆	◆	◆		◆		◆				◆
curve25519-sha256@libssh.org		◆	◆	◆		◆		◆				◆

Kebijakan keamanan	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2022-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11	TransferSecurityPolicy-2018-11
			Compliant-2025-02	Restricted-2025-07		TransferSecurityPolicy-2024-05			dan TransferSecurityPolicy-2020-06	dan TransferSecurityPolicy-2020-06	dan TransferSecurityPolicy-2018-11	dan TransferSecurityPolicy-2018-11
diffie-he												◆
lman-gro												
up14-sha1												
diffie-he									◆	◆	◆	
lman-gro												
up14-sha2												
56												
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
lman-gro												
up16-sha5												
12												

Kebijakan keamanan	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-Comes	TransferSecurityPolicy-Restricted-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-FIPS-2024-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up18-sha512														
diffie-he	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up-exchan														
ge-sha256														
ecdh-sha2	◆	◆		◆	◆	◆				◆	◆	◆	◆	◆
-nistp256														

Kebijakan Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03
keamanan	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03	Transfer Security Policy-2025-03
	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11	
	-2025-03	ditComes	stricted	-2025-07	-2024-01/	TransferS	-2023-05	dan	-2020-06	dan	-2018	
		iant-2025-02			TransferS	ecurityPo		TransferS	ecurityPo	TransferS	ecurityPo	
					licy-	FIPS		licy-	Rest	licy-	Rest	
					-2024-05			ricted-20	20-06	ricted-20	18-11	
ecdh-sha2-nistp384	◆	◆	◆	◆	◆			◆	◆	◆		
ecdh-sha2-nistp521	◆	◆	◆	◆	◆			◆	◆	◆		
SshMacs												
hmac-sha1											◆	
hmac-sha1											◆	
etm@openssh.com												
hmac-sha2-256							◆	◆	◆	◆		

Kebijakan keamanan	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
			Restricted							dan		dan
			TransferS				TransferS			TransferS		TransferS
			ecurityPo				ecurityPo			ecurityPo		ecurityPo
			licy-				licy-			licy-		licy-
			FIPS				FIPS			Rest		Rest
							-2024-05			ricted-20		ricted-20
										20-06		18-11
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512									◆	◆	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com										◆		◆
umac-128@openssh.com										◆		◆

Kebijakan Transfer Security Policy-2025-03	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-07	Transfer Security Policy-2025-07	Transfer Security Policy-2024-01	Transfer Security Policy-2024-05	Transfer Security Policy-2023-05	Transfer Security Policy-2023-06	Transfer Security Policy-2020-06	Transfer Security Policy-2020-11	Transfer Security Policy-2018-11
umac-64- e tm@openssh.com											◆
umac-64@openssh.com											◆
ContentEncryptionCiphers											
aes256-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes128-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
3des-cbc	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
HashAlgorithms											
sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Kebijakan keamanan	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2022-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-2024-05			dan TransferSecurityPolicy-2020-06		dan TransferSecurityPolicy-2018-11
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆
TlsCiphers											
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Kebijakan keamanan	Transfer Security Policy-2025-03	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-07	Transfer Security Policy-2024-01	Transfer Security Policy-2023-05	Transfer Security Policy-2023-05	Transfer Security Policy-2023-06	Transfer Security Policy-2020-06	Transfer Security Policy-2020-06	Transfer Security Policy-2018-11
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	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Kebijakan keamanan	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256											◆
TLS_RSA_WITH_AES_128_CBC_SHA256											◆

Detail kebijakan keamanan

Bagian berikut berisi representasi JSON dari setiap kebijakan keamanan.

TransferSecurityPolicy-2025-03

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2025-03 keamanan.

```
{
  "SecurityPolicy": {
```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2025-03",
"SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2025-03

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-FIPS-2025-03 keamanan.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [

```

```

        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Kebijakan keamanan ini dirancang untuk transfer file AS2 yang memerlukan peningkatan keamanan dengan mengecualikan algoritma kriptografi lama. Ini mendukung enkripsi AES modern dan algoritma SHA-2 hash sambil menghapus dukungan untuk algoritma yang lebih lemah seperti 3DES dan SHA-1

Note

Kebijakan keamanan ini identik dengan TransferSecurityPolicy-2025-03, kecuali tidak mendukung 3DES (in ContentEncryptionCiphers) dan tidak mendukung SHA1 (in

HashAlgorithms). Ini mencakup semua algoritma dari 2025-03, termasuk algoritma kriptografi pasca-kuantum (mlkem* KEXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512"
    ],
    "TlsCiphers": [
```

```

        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-SshAuditCompliant-2025-02 keamanan.

Note

Kebijakan keamanan ini dirancang berdasarkan rekomendasi yang diberikan oleh ssh-audit alat, dan 100% sesuai dengan alat itu.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
  },
}

```

```

    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER"
  }
}

```

TransferSecurityPolicy-2024-01

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2024-01 keamanan.

```

{
  "SecurityPolicy": {

```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2024-01",
"SshCiphers": [
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```



```
    ]
  }
}
```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

Berikut ini menunjukkan TransferSecurityPolicy-FIPS-2024-01 dan kebijakan TransferSecurityPolicy-FIPS-2024-05 keamanan.

Note

Titik akhir layanan FIPS TransferSecurityPolicy-FIPS-2024-01 dan kebijakan TransferSecurityPolicy-FIPS-2024-05 keamanan hanya tersedia di beberapa AWS Wilayah. Untuk informasi selengkapnya, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS

Satu-satunya perbedaan antara kedua kebijakan keamanan ini adalah yang TransferSecurityPolicy-FIPS-2024-01 mendukung ssh-rsa algoritma, dan TransferSecurityPolicy-FIPS-2024-05 tidak.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
```

```

        "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2023-05 keamanan.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
    "SshCiphers": [
        "aes256-gcm@openssh.com",
        "aes128-gcm@openssh.com",
        "aes256-ctr",
        "aes192-ctr"
    ],
    "SshKexs": [
        "curve25519-sha256",

```

```

        "curve25519-sha256@libssh.org",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

Detail sertifikasi FIPS untuk AWS Transfer Family dapat ditemukan di <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-FIPS-2023-05 keamanan.

 Note

Titik akhir layanan FIPS dan kebijakan TransferSecurityPolicy-FIPS-2023-05 keamanan hanya tersedia di beberapa AWS Wilayah. Untuk informasi selengkapnya, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
```

```

        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-2022-03

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2022-03 keamanan.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [

```

```

    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2020-06 dan TransferSecurityPolicy-Restricted-2020-06

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2020-06 keamanan.

Note

Kebijakan TransferSecurityPolicy-Restricted-2020-06 dan TransferSecurityPolicy-2020-06 keamanan identik, kecuali bahwa kebijakan terbatas tidak mendukung `chacha20-poly1305@openssh.com` cipher.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
  },
}

```

```
"SshKexs": [  
  "ecdh-sha2-nistp256",  
  "ecdh-sha2-nistp384",  
  "ecdh-sha2-nistp521",  
  "diffie-hellman-group-exchange-sha256",  
  "diffie-hellman-group16-sha512",  
  "diffie-hellman-group18-sha512",  
  "diffie-hellman-group14-sha256"  
],  
"SshMacs": [  
  "umac-128-etm@openssh.com",  
  "hmac-sha2-256-etm@openssh.com",  
  "hmac-sha2-512-etm@openssh.com",  
  "umac-128@openssh.com",  
  "hmac-sha2-256",  
  "hmac-sha2-512"  
],  
"ContentEncryptionCiphers": [  
  "aes256-cbc",  
  "aes192-cbc",  
  "aes128-cbc",  
  "3des-cbc"  
],  
"HashAlgorithms": [  
  "sha256",  
  "sha384",  
  "sha512",  
  "sha1"  
],  
"TlsCiphers": [  
  "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",  
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",  
  "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",  
  "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",  
  "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",  
  "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",  
  "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",  
  "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"  
]  
}  
}
```

TransferSecurityPolicy-FIPS-2020-06

Detail sertifikasi FIPS untuk AWS Transfer Family dapat ditemukan di <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-FIPS-2020-06 keamanan.

Note

Titik akhir layanan FIPS dan kebijakan TransferSecurityPolicy-FIPS-2020-06 keamanan hanya tersedia di beberapa AWS Wilayah. Untuk informasi lebih lanjut, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
```



```

    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2018-11 dan TransferSecurityPolicy-Restricted-2018-11

Berikut ini menunjukkan kebijakan TransferSecurityPolicy-2018-11 keamanan.

Note

Kebijakan TransferSecurityPolicy-Restricted-2018-11 dan TransferSecurityPolicy-2018-11 keamanan identik, kecuali bahwa kebijakan terbatas tidak mendukung chacha20-poly1305@openssh.com cipher.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "aes128-ctr",

```

```
"aes192-ctr",
"aes256-ctr",
"aes128-gcm@openssh.com",
"aes256-gcm@openssh.com"
],
"SshKexs": [
  "curve25519-sha256",
  "curve25519-sha256@libssh.org",
  "ecdh-sha2-nistp256",
  "ecdh-sha2-nistp384",
  "ecdh-sha2-nistp521",
  "diffie-hellman-group-exchange-sha256",
  "diffie-hellman-group16-sha512",
  "diffie-hellman-group18-sha512",
  "diffie-hellman-group14-sha256",
  "diffie-hellman-group14-sha1"
],
"SshMacs": [
  "umac-64-etm@openssh.com",
  "umac-128-etm@openssh.com",
  "hmac-sha2-256-etm@openssh.com",
  "hmac-sha2-512-etm@openssh.com",
  "hmac-sha1-etm@openssh.com",
  "umac-64@openssh.com",
  "umac-128@openssh.com",
  "hmac-sha2-256",
  "hmac-sha2-512",
  "hmac-sha1"
],
"ContentEncryptionCiphers": [
  "aes256-cbc",
  "aes192-cbc",
  "aes128-cbc",
  "3des-cbc"
],
"HashAlgorithms": [
  "sha256",
  "sha384",
  "sha512",
  "sha1"
],
"TlsCiphers": [
  "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
```

```

    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256"
  ]
}
}

```

Kebijakan keamanan untuk AWS Transfer Family Konektor SFTP

Kebijakan keamanan konektor SFTP AWS Transfer Family memungkinkan Anda membatasi rangkaian algoritme kriptografi (kode otentikasi pesan (MAC), pertukaran kunci (KEX), dan rangkaian sandi) yang terkait dengan konektor SFTP Anda. Berikut ini adalah daftar algoritma kriptografi yang didukung untuk setiap kebijakan keamanan konektor SFTP.

Note

`TransferSFTPConnectorSecurityPolicy-2024-03` adalah kebijakan keamanan default yang diterapkan pada konektor SFTP.

Anda dapat mengubah kebijakan keamanan untuk konektor Anda. Pilih Konektor dari panel navigasi kiri Transfer Family, dan pilih konektor Anda. Kemudian pilih Edit di bagian konfigurasi Sftp. Di bagian Opsi algoritma kriptografi, pilih kebijakan keamanan yang tersedia dari daftar dropdown di bidang Kebijakan Keamanan.

Algoritma kriptografi

Untuk kunci host, konektor SFTP mendukung semua algoritma yang didukung untuk server Transfer Family, kecuali untuk ed25519:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`

- `ecdsa-sha2-nistp521`

Selain itu, untuk kunci host, kami mendukung `ssh-rsa`, tetapi hanya untuk `TransferSFTPConnectorSecurityPolicy-2023-07`.

Untuk otentikasi, konektor SFTP mendukung jenis kunci berikut:

- `ssh-rsa`
- `ecdsa`

Rincian kebijakan keamanan konektor SFTP

Tabel berikut menunjukkan algoritma kriptografi spesifik yang didukung oleh setiap kebijakan keamanan konektor SFTP.

Kebijakan keamanan	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Ciphers			
<code>aes128-ctr</code>			◆
<code>aes128-gcm@openssh.com</code>	◆	◆	◆
<code>aes192-ctr</code>		◆	◆
<code>aes256-ctr</code>		◆	◆
<code>aes256-gcm@openssh.com</code>	◆	◆	◆
Kexs			
<code>kurva25519-sha256</code>		◆	◆
<code>curve25519-sha256@libssh.org</code>		◆	◆

Kebijakan keamanan	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
diffie-hellman-group14-sha1			◆
diffie-hellman-group16-sha512		◆	◆
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆
hmac-sha1-96			◆
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆

Kebijakan keamanan	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

Menggunakan pertukaran kunci pasca-kuantum hibrida dengan AWS Transfer Family

Transfer Family mendukung opsi pembentukan kunci pasca-kuantum hibrida untuk protokol Secure Shell (SSH). Post-quantum Pembentukan kunci diperlukan karena sudah mungkin untuk merekam lalu lintas jaringan dan menyimpannya untuk dekripsi di masa depan oleh komputer kuantum, yang disebut serangan store-now-harvest-later.

Anda dapat menggunakan opsi ini saat terhubung ke Transfer Family untuk transfer file aman ke dalam dan keluar dari penyimpanan Amazon Simple Storage Service (Amazon S3) atau Amazon Elastic File System (Amazon EFS). Post-quantum Pembentukan kunci hibrida di SSH memperkenalkan mekanisme pembentukan kunci pasca-kuantum, yang digunakannya bersama dengan algoritma pertukaran kunci klasik. Kunci SSH yang dibuat dengan cipher suite klasik aman dari serangan brute-force dengan teknologi saat ini. Namun, enkripsi klasik diperkirakan tidak akan tetap aman setelah munculnya komputasi kuantum skala besar di masa depan.

Jika organisasi Anda bergantung pada kerahasiaan data jangka panjang yang diteruskan melalui koneksi Transfer Family, Anda harus mempertimbangkan rencana untuk bermigrasi ke kriptografi pasca-kuantum sebelum komputer kuantum skala besar tersedia untuk digunakan.

Untuk melindungi data yang dienkripsi hari ini terhadap potensi serangan future, AWS berpartisipasi dengan komunitas kriptografi dalam pengembangan algoritma tahan kuantum atau pasca-kuantum. Kami telah menerapkan rangkaian cipher pertukaran kunci pasca-kuantum hibrida di Transfer Family yang menggabungkan elemen klasik dan pasca-kuantum.

Suite sandi hibrida ini tersedia untuk digunakan pada beban kerja produksi Anda di sebagian besar Wilayah. AWS Namun, karena karakteristik kinerja dan persyaratan bandwidth suite cipher hybrid berbeda dengan mekanisme pertukaran kunci klasik, kami sarankan Anda mengujinya pada koneksi Transfer Family Anda.

Cari tahu lebih lanjut tentang kriptografi pasca-kuantum di posting blog keamanan [Post-QuantumKriptografi](#).

Daftar Isi

- [Tentang pertukaran kunci hibrida pasca-kuantum di SSH](#)
- [Cara kerja pembentukan kunci hibrida pasca-kuantum di Transfer Family](#)
 - [Mengapa ML-KEM?](#)
 - [Post-quantum pertukaran kunci SSH hibrida dan persyaratan kriptografi \(FIPS 140\)](#)
- [Menguji pertukaran kunci hibrida pasca-kuantum di Transfer Family](#)
 - [Aktifkan pertukaran kunci hybrid pasca-kuantum di titik akhir SFTP Anda](#)
 - [Siapkan klien SFTP yang mendukung pertukaran kunci hybrid pasca-kuantum](#)
 - [Konfirmasikan pertukaran kunci hibrida pasca-kuantum di SFTP](#)

Tentang pertukaran kunci hibrida pasca-kuantum di SSH

Transfer Family mendukung suite cipher pertukaran kunci hibrida pasca-kuantum, yang menggunakan algoritme pertukaran kunci [Elliptic Curve Diffie-Hellman \(ECDH\)](#) klasik, dan. ML-KEM ML-KEM adalah enkripsi kunci publik pasca-kuantum dan algoritma pembentukan kunci yang telah ditetapkan oleh [National Institute for Standards and Technology \(NIST\)](#) sebagai algoritma perjanjian kunci pasca-kuantum standar pertama.

Klien dan server masih melakukan pertukaran kunci ECDH. Selain itu, server merangkum rahasia bersama pasca-kuantum ke kunci publik KEM pasca-kuantum klien, yang diiklankan dalam pesan pertukaran kunci SSH klien. Strategi ini menggabungkan jaminan tinggi pertukaran kunci klasik dengan keamanan pertukaran kunci pasca-kuantum yang diusulkan, untuk membantu memastikan bahwa jabat tangan dilindungi selama ECDH atau rahasia bersama pasca-kuantum tidak dapat dipatahkan.

Cara kerja pembentukan kunci hibrida pasca-kuantum di Transfer Family

AWS baru-baru ini mengumumkan dukungan untuk pertukaran kunci pasca-kuantum dalam transfer file SFTP di. AWS Transfer Family Transfer Family secara aman menskalakan transfer file bisnis-ke-

bisnis ke layanan AWS Penyimpanan menggunakan SFTP dan protokol lainnya. SFTP adalah versi yang lebih aman dari File Transfer Protocol (FTP) yang berjalan melalui SSH. Dukungan pertukaran kunci pasca-kuantum dari Transfer Family meningkatkan bilah keamanan untuk transfer data melalui SFTP.

Dukungan SFTP pertukaran kunci hibrida pasca-kuantum di Transfer Family termasuk menggabungkan algoritma pasca-kuantum ML-KEM-768, dan, dengan ECDH lebih dari kurva P256 ML-KEM-1024, P384, atau Curve25519. Metode pertukaran kunci SSH yang sesuai berikut ini ditentukan dalam draf pertukaran [kunci SSH hibrida pasca-kuantum](#).

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

Mengapa ML-KEM?

AWS berkomitmen untuk mendukung standar, algoritma interoperable. ML-KEM adalah satu-satunya algoritma pertukaran kunci pasca-kuantum yang distandarisasi dan disetujui oleh proyek Kriptografi [NIST Post-Quantum](#). Badan standar sudah terintegrasi ML-KEM ke dalam protokol. AWS sudah mendukung ML-KEM di TLS di beberapa titik akhir AWS API.

Sebagai bagian dari komitmen ini, AWS telah mengajukan draf proposal ke IETF untuk kriptografi pasca-kuantum yang menggabungkan ML-KEM dengan NIST-approved kurva seperti P256 untuk SSH. Untuk membantu meningkatkan keamanan bagi pelanggan kami, AWS implementasi pertukaran kunci pasca-kuantum di SFTP dan SSH mengikuti rancangan itu. Kami berencana untuk mendukung pembaruan masa depan sampai proposal kami diadopsi oleh IETF dan menjadi standar.

Metode pertukaran kunci baru (tercantum di bagian [Cara kerja pembentukan kunci hibrida pasca-kuantum di Transfer Family](#)) mungkin berubah saat draf berkembang menuju standardisasi.

Note

Post-quantum dukungan algoritme saat ini tersedia untuk pertukaran kunci hibrida pasca-kuantum di TLS untuk AWS KMS (lihat [Menggunakan TLS pasca-kuantum hibrida dengan AWS KMS](#)), AWS Certificate Manager, dan titik akhir API. AWS Secrets Manager

Post-quantum pertukaran kunci SSH hibrida dan persyaratan kriptografi (FIPS 140)

Untuk pelanggan yang memerlukan kepatuhan FIPS, Transfer Family menyediakan FIPS-approved kriptografi dalam SSH dengan menggunakan perpustakaan kriptografi open-source bersertifikat AWS FIPS 140, -LC. AWS Metode pertukaran kunci hibrida pasca-kuantum yang didukung TransferSecurityPolicy-FIPS-2025-03 dalam Transfer Family in disetujui FIPS menurut [SP 800-56Cr2 NIST](#) (bagian 2). Kantor Federal Jerman untuk Keamanan Informasi ([BSI](#)) dan Agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) Prancis juga merekomendasikan metode pertukaran kunci hibrida pasca-kuantum tersebut.

Menguji pertukaran kunci hibrida pasca-kuantum di Transfer Family

Bagian ini menjelaskan langkah-langkah yang Anda ambil untuk menguji pertukaran kunci hibrida pasca-kuantum.

1. [Aktifkan pertukaran kunci hybrid pasca-kuantum di titik akhir SFTP Anda.](#)
2. Gunakan klien SFTP (seperti [Siapkan klien SFTP yang mendukung pertukaran kunci hybrid pasca-kuantum](#)) yang mendukung pertukaran kunci hibrida pasca-kuantum dengan mengikuti panduan dalam spesifikasi draf yang disebutkan di atas.
3. Transfer file menggunakan server Transfer Family.
4. [Konfirmasikan pertukaran kunci hibrida pasca-kuantum di SFTP.](#)

Aktifkan pertukaran kunci hybrid pasca-kuantum di titik akhir SFTP Anda

Anda dapat memilih kebijakan SSH saat membuat endpoint server SFTP baru di Transfer Family, atau dengan mengedit opsi algoritma Cryptographic di endpoint SFTP yang ada. Snapshot berikut menunjukkan contoh Konsol Manajemen AWS tempat Anda memperbarui kebijakan SSH.

Cryptographic algorithm options [Info](#)

Security Policy

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

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 ▲

Find a security policy

TransferSecurityPolicy-2018-11
TransferSecurityPolicy-2020-06
TransferSecurityPolicy-2022-03
TransferSecurityPolicy-2023-05
TransferSecurityPolicy-2024-01
TransferSecurityPolicy-2025-03 ✓
TransferSecurityPolicy-Restricted-2018-11
TransferSecurityPolicy-Restricted-2020-06

to it. Addit

Nama kebijakan SSH yang mendukung pertukaran kunci pasca-kuantum adalah dan TransferSecurityPolicy-2025-03. TransferSecurityPolicy-FIPS-2025-03 Untuk detail selengkapnya tentang kebijakan Transfer Family, lihat [Kebijakan keamanan untuk AWS Transfer Family server](#).

Siapkan klien SFTP yang mendukung pertukaran kunci hybrid pasca-kuantum

Setelah memilih kebijakan SSH pasca-kuantum yang benar di titik akhir Transfer Family SFTP, Anda dapat bereksperimen dengan SFTP pasca-kuantum di Transfer Family. Instal klien OpenSSH terbaru (seperti versi 9.9) pada sistem lokal Anda untuk menguji.

Note

Pastikan klien Anda mendukung satu atau lebih ML-KEM algoritme yang tercantum sebelumnya. Anda dapat melihat algoritme yang didukung untuk versi OpenSSH Anda dengan menjalankan perintah ini: `ssh -Q kex`

Anda dapat menjalankan contoh klien SFTP untuk terhubung ke titik akhir SFTP Anda (misalnya, `s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`) dengan

menggunakan metode pertukaran kunci hybrid pasca-kuantum, seperti yang ditunjukkan pada perintah berikut.

```
sftp -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

Pada perintah sebelumnya, ganti item berikut dengan informasi Anda sendiri:

- Ganti *username_private_key_PEM_file* dengan file kunci pribadi pengguna SFTP PEM-encoded
- Ganti *username* dengan nama pengguna SFTP
- Ganti *server-id* dengan ID server Transfer Family
- Ganti *region-id* dengan wilayah sebenarnya tempat server Transfer Family Anda berada

Konfirmasikan pertukaran kunci hibrida pasca-kuantum di SFTP

Untuk mengonfirmasi bahwa pertukaran kunci hybrid pasca-kuantum digunakan selama koneksi SSH untuk SFTP ke Transfer Family, periksa output klien. Secara opsional, Anda dapat menggunakan program pengambilan paket. Jika Anda menggunakan klien OpenSSH 9.9, outputnya akan terlihat mirip dengan yang berikut (menghilangkan informasi yang tidak relevan untuk singkatnya):

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
```

```
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or
directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

Output menunjukkan bahwa negosiasi klien terjadi menggunakan mlkem768x25519-sha256 metode hibrida pasca-kuantum dan berhasil membuat sesi SFTP.

Perlindungan data dan enkripsi

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di AWS Transfer Family (Transfer Family). Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ privasi data](#). Untuk informasi tentang perlindungan data di Eropa, lihat [model tanggung jawab AWS bersama dan posting blog GDPR](#) di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi kredensial AWS akun dan mengatur akun pengguna individu dengan AWS IAM Identity Center. Dengan cara ini, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut ini:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mendukung TLS 1.2.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon Simple Storage Service (Amazon S3).
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, lihat [Standar pemrosesan informasi federal \(FIPS\) 140-2](#).

Kami sangat merekomendasikan agar Anda tidak memasukkan informasi identifikasi sensitif apapun, seperti nomor rekening pelanggan Anda, ke dalam kolom isian teks bebas seperti kolom Nama. Ini termasuk saat Anda bekerja dengan Transfer Family atau AWS layanan lain menggunakan konsol, API AWS CLI, atau AWS SDK. Data konfigurasi apa pun yang Anda masukkan ke dalam konfigurasi layanan Transfer Family, atau konfigurasi layanan lain, dapat diambil untuk dimasukkan dalam log diagnostik. Saat Anda memberikan URL ke server eksternal, jangan sertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Sebaliknya, data dari operasi unggah dan pengunduhan masuk dan keluar dari server Transfer Family diperlakukan sebagai sepenuhnya pribadi dan tidak pernah ada di luar saluran terenkripsi — seperti koneksi SFTP atau FTPS. Data ini hanya dapat diakses oleh orang yang berwenang.

Enkripsi data di Transfer Family

AWS Transfer Family menggunakan opsi enkripsi default yang Anda tetapkan untuk bucket Amazon S3 untuk mengenkripsi data Anda. Saat Anda mengaktifkan enkripsi pada bucket, semua objek dienkripsi saat disimpan di bucket. Objek dienkripsi dengan menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) atau AWS Key Management Service (KMS) kunci terkelola (KMS). Untuk informasi tentang enkripsi sisi server, lihat [Melindungi data menggunakan enkripsi sisi server](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Langkah-langkah berikut menunjukkan cara mengenkripsi data di AWS Transfer Family.

Untuk memungkinkan enkripsi di AWS Transfer Family

1. Aktifkan enkripsi default untuk bucket Amazon S3 Anda. Untuk petunjuknya, lihat [enkripsi default Amazon S3 untuk bucket S3 di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.
2. Perbarui kebijakan peran AWS Identity and Access Management (IAM) yang dilampirkan ke pengguna untuk memberikan izin required AWS Key Management Service (AWS KMS).
3. Jika Anda menggunakan kebijakan sesi untuk pengguna, kebijakan sesi harus memberikan AWS KMS izin yang diperlukan.

Contoh berikut menunjukkan kebijakan IAM yang memberikan izin minimum yang diperlukan saat menggunakan bucket Amazon S3 AWS Transfer Family yang diaktifkan untuk enkripsi. AWS KMS Sertakan kebijakan contoh ini dalam kebijakan peran IAM pengguna dan kebijakan sesi, jika Anda menggunakannya.

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:GetPublicKey",
    "kms:ListKeyPolicies"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

ID kunci KMS yang Anda tentukan dalam kebijakan ini harus sama dengan yang ditentukan untuk enkripsi default pada langkah 1.

Root, atau peran IAM yang digunakan untuk pengguna, harus diizinkan dalam kebijakan AWS KMS kunci. Untuk informasi tentang kebijakan AWS KMS utama, lihat [Menggunakan kebijakan utama di AWS KMS](#) di Panduan AWS Key Management Service Pengembang.

AWS Transfer Family enkripsi saat istirahat

Karena AWS Transfer Family merupakan layanan transfer file, itu tidak mengelola data penyimpanan Anda saat istirahat. Layanan penyimpanan dan sistem yang AWS Transfer Family mendukung bertanggung jawab untuk melindungi data dalam keadaan itu. Namun, ada beberapa data terkait layanan yang AWS Transfer Family mengelola saat istirahat.

Apa yang dienkripsi?

Satu-satunya data yang AWS Transfer Family menangani saat istirahat berkaitan dengan detail yang dibutuhkan untuk mengoperasikan server transfer file Anda dan memproses transfer. AWS Transfer Family menyimpan data berikut dengan enkripsi penuh saat istirahat di Amazon DynamoDB:

- Konfigurasi server (misalnya, pengaturan server, konfigurasi protokol, dan detail titik akhir).
- Data otentikasi pengguna, termasuk kunci publik SSH dan metadata pengguna.
- Rincian eksekusi alur kerja dan konfigurasi langkah.
- Konfigurasi konektor dan kredensial otentikasi untuk sistem pihak ketiga. Kredensial ini dienkripsi menggunakan AWS Transfer Family kunci enkripsi terkelola.

Manajemen kunci

Anda tidak dapat mengelola kunci enkripsi yang AWS Transfer Family digunakan untuk menyimpan informasi di DynamoDB yang terkait dengan menjalankan server Anda dan memproses transfer. Informasi ini mencakup konfigurasi server Anda, data otentikasi pengguna, detail alur kerja, dan kredensi konektor.

Apa yang tidak dienkripsi?

Meskipun AWS Transfer Family tidak mengontrol bagaimana data penyimpanan Anda dienkripsi saat istirahat, kami tetap menyarankan untuk mengonfigurasi lokasi penyimpanan Anda dengan tingkat keamanan tertinggi yang mereka dukung. Misalnya, Anda dapat mengenkripsi objek dengan kunci enkripsi terkelola Amazon S3 SSE-S3 () AWS KMS atau kunci SSE-KMS ().

Pelajari lebih lanjut tentang cara layanan AWS penyimpanan mengenkripsi data saat istirahat:

- [Amazon S3](#)
- [Amazon EFS](#)

Mengelola kunci SSH dan PGP di Transfer Family

Di bagian ini, Anda dapat menemukan informasi tentang kunci SSH, termasuk cara membuatnya dan cara memutarnya. Untuk detail tentang penggunaan Transfer Family with AWS Lambda to manage keys, lihat posting blog [Mengaktifkan manajemen kunci layanan mandiri pengguna dengan AWS Transfer Family](#) dan. AWS Lambda Untuk penerapan otomatis dan pengelolaan pengguna dengan beberapa kunci SSH, lihat. [Modul Transfer Family Terraform](#)

Note

AWS Transfer Family menerima kunci RSA, ECDSA, dan ED25519 untuk otentikasi SSH.

Bagian ini juga mencakup cara membuat dan mengelola kunci Pretty Good Privacy (PGP).

Untuk gambaran menyeluruh tentang semua enkripsi dan algoritme kunci yang didukung, termasuk rekomendasi untuk kasus penggunaan yang berbeda, lihat [Ikhtisar enkripsi dan algoritma kunci](#).

Ikhtisar enkripsi dan algoritma kunci

AWS Transfer Family mendukung berbagai jenis algoritma untuk tujuan yang berbeda. Memahami algoritme mana yang akan digunakan untuk kasus penggunaan spesifik Anda membantu memastikan transfer file yang aman dan kompatibel.

Referensi Cepat Algoritma

Kasus Penggunaan	Algoritma yang Direkomendasikan	Sesuai FIPS	Catatan
SSH/SFTP Otentikasi	RSA (rsa-sha2-256/512), ECDSA, atau ED25519	RSA: Ya, ECDSA: Ya, ED25519: Tidak	Kompatibel dengan semua klien SSH dan server
Generasi Kunci PGP	RSA atau ECC (NIST)	Ya	Untuk dekripsi alur kerja
Enkripsi File PGP	AES-256	Ya	Ditentukan oleh perangkat lunak PGP

Algoritma otentikasi SSH

Algoritma ini digunakan untuk SSH/SFTP otentikasi antara klien dan AWS Transfer Family server. Pilih salah satunya saat membuat pasangan kunci SSH untuk otentikasi pengguna atau kunci host server.

RSA (Direkomendasikan)

Kompatibel dengan semua klien SSH dan server, dan FIPS-compliant. Gunakan dengan SHA-2 hashing untuk meningkatkan keamanan:

- `rsa-sha2-256`- Direkomendasikan untuk sebagian besar kasus penggunaan
- `rsa-sha2-512`- Opsi keamanan yang lebih tinggi

ED25519

Modern dan efisien. Ukuran kunci yang lebih kecil dengan keamanan yang kuat:

- `ssh-ed25519`- Cepat dan aman, tapi tidak FIPS-compliant

ECDSA

Opsi kurva elips. Keseimbangan keamanan dan kinerja yang baik:

- `ecdsa-sha2-nistp256`- Kurva standar
- `ecdsa-sha2-nistp384`- Kurva keamanan yang lebih tinggi
- `ecdsa-sha2-nistp521`- Kurva keamanan tertinggi

Note

Kami mendukung `ssh-rsa` dengan SHA1 untuk kebijakan keamanan yang lebih lama. Lihat perinciannya di [Algoritma kriptografi](#).

Memilih algoritma SSH yang tepat

- Untuk sebagian besar pengguna: Gunakan RSA dengan `rsa-sha2-256` atau `rsa-sha2-512`
- Untuk kepatuhan FIPS: Gunakan algoritma RSA atau ECDSA
- Untuk lingkungan modern: ED25519 menawarkan keamanan dan kinerja yang sangat baik

Enkripsi PGP dan algoritma dekripsi

PGP (Pretty Good Privacy) menggunakan dua jenis algoritma yang bekerja sama untuk mengenkripsi dan mendekripsi file dalam alur kerja:

1. Algoritma pasangan kunci - Digunakan untuk menghasilkan pasangan public/private kunci untuk enkripsi dan tanda tangan digital
2. Algoritma simetris - Digunakan untuk mengenkripsi data file aktual (algoritma key pair mengenkripsi kunci simetris)

Algoritma key pair PGP

Pilih salah satu algoritme ini saat membuat pasangan kunci PGP untuk dekripsi alur kerja:

RSA (Direkomendasikan)

Direkomendasikan untuk sebagian besar pengguna. Didukung secara luas, mapan, dan FIPS-compliant. Memberikan keseimbangan keamanan dan kompatibilitas yang baik.

ECC (Kriptografi Kurva Elips)

Lebih efisien daripada RSA dengan ukuran kunci yang lebih kecil sambil mempertahankan keamanan yang kuat:

- Kurva NIST - Kurva standar didukung secara luas dan FIPS-compliant
- BrainPool kurva - Kurva alternatif untuk persyaratan kepatuhan tertentu
- Curve25519 - Kurva kinerja tinggi modern yang menawarkan keamanan yang kuat dengan komputasi yang efisien

ElGamal

Algoritma warisan. Didukung untuk kompatibilitas dengan sistem yang lebih lama. Gunakan RSA atau ECC untuk implementasi baru.

Untuk petunjuk rinci tentang menghasilkan kunci PGP, lihat. [Hasilkan kunci PGP](#)

Algoritma enkripsi simetris PGP

Algoritma ini mengenkripsi data file Anda yang sebenarnya. Algoritma yang digunakan tergantung pada bagaimana file PGP dibuat oleh perangkat lunak PGP Anda:

FIPS-compliant algoritma (direkomendasikan untuk lingkungan yang diatur)

- AES-128, AES-192, AES-256 - Standar Enkripsi Tingkat Lanjut (disarankan)
- 3DES - Triple Data Encryption Standard (lama, gunakan AES bila memungkinkan)

Algoritma lain yang didukung

- IDE, CAST5, Blowfish, DES,,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

Note

Anda tidak memilih algoritma simetris secara langsung saat menggunakan AWS Transfer Family alur kerja - itu ditentukan oleh perangkat lunak PGP yang digunakan untuk membuat file terenkripsi. Namun, Anda dapat mengonfigurasi perangkat lunak PGP Anda untuk memilih FIPS-compliant algoritma seperti. AES-256

Untuk informasi selengkapnya tentang algoritme simetris yang didukung, lihat [Algoritma enkripsi simetris yang didukung](#)

Buat kunci SSH untuk pengguna yang dikelola layanan

Anda dapat mengatur server Anda untuk mengautentikasi pengguna menggunakan metode otentikasi terkelola layanan, tempat nama pengguna dan kunci SSH disimpan dalam layanan. Kunci SSH publik pengguna diunggah ke server sebagai properti pengguna. Kunci ini digunakan oleh server sebagai bagian dari proses otentikasi berbasis kunci standar. Setiap pengguna dapat memiliki beberapa kunci SSH publik pada file dengan server individual. Untuk batasan jumlah kunci yang dapat disimpan per pengguna, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum Amazon Web

Sebagai alternatif dari metode otentikasi terkelola layanan, Anda dapat mengautentikasi pengguna menggunakan penyedia identitas kustom, atau. AWS Directory Service for Microsoft Active Directory Untuk informasi selengkapnya, lihat [Bekerja dengan penyedia identitas khusus](#) atau [Menggunakan AWS Directory Service untuk Microsoft Active Directory](#).

Server hanya dapat mengautentikasi pengguna menggunakan satu metode (layanan dikelola, layanan direktori, atau penyedia identitas kustom), dan metode itu tidak dapat diubah setelah server dibuat.

Topik

- [Membuat kunci SSH di macOS, Linux, atau Unix](#)
- [Membuat kunci SSH di Microsoft Windows](#)
- [Mengonversi kunci SSH2 ke format kunci publik SSH](#)

Membuat kunci SSH di macOS, Linux, atau Unix

Pada sistem operasi macOS, Linux, atau Unix, Anda menggunakan `ssh-keygen` perintah untuk membuat kunci publik SSH dan kunci pribadi SSH yang juga dikenal sebagai key pair.

Note

Dalam contoh berikut, kami tidak menentukan frasa sandi: dalam hal ini, alat meminta Anda untuk memasukkan frasa sandi Anda dan kemudian mengulangnya untuk memverifikasi. Membuat frasa sandi menawarkan perlindungan yang lebih baik untuk kunci pribadi Anda, dan mungkin juga meningkatkan keamanan sistem secara keseluruhan. Anda tidak dapat memulihkan frasa sandi Anda: jika Anda lupa, Anda harus membuat kunci baru. Namun, jika Anda membuat kunci host server, Anda harus menentukan frasa sandi kosong, dengan menentukan `-N ""` opsi dalam perintah (atau dengan menekan **Enter** dua kali saat diminta), karena server Transfer Family tidak dapat meminta kata sandi saat start-up.

Untuk membuat kunci SSH pada sistem operasi macOS, Linux, atau Unix

1. Pada sistem operasi macOS, Linux, atau Unix, buka terminal perintah.
2. AWS Transfer Family menerima RSA-, ECDSA-, dan kunci. ED25519-formatted Pilih perintah yang sesuai berdasarkan jenis pasangan kunci yang Anda hasilkan.

Tip: Ganti *key_name* dengan nama sebenarnya dari file key pair SSH Anda.

- Untuk menghasilkan key pair RSA 4096-bit:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Untuk menghasilkan pasangan kunci ECDSA 521-bit (ECDSA memiliki ukuran bit 256, 384, dan 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Untuk menghasilkan key pair ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

Berikut ini menunjukkan contoh ssh-keygen output.

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

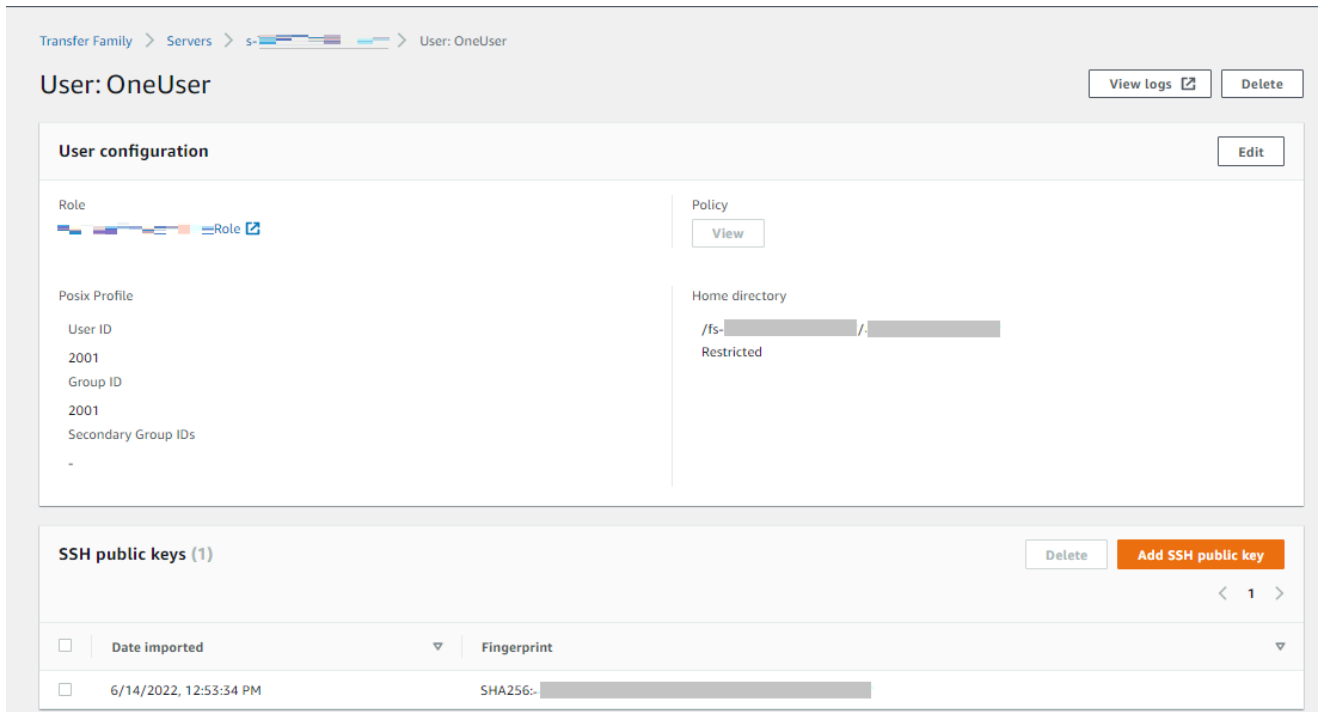
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|    . ....E        |
| .   = ...         |
|. . . = ..o        |
| . o + oo =        |
| + = .S.= *        |
| . o o ..B + o     |
|    .o+.* .        |
|    =o*+*.         |
|    ..*o*+.        |
+-----[SHA256]-----+
```

Tip: Ketika Anda menjalankan ssh-keygen perintah seperti yang ditunjukkan sebelumnya, itu membuat kunci publik dan pribadi sebagai file dalam direktori saat ini.

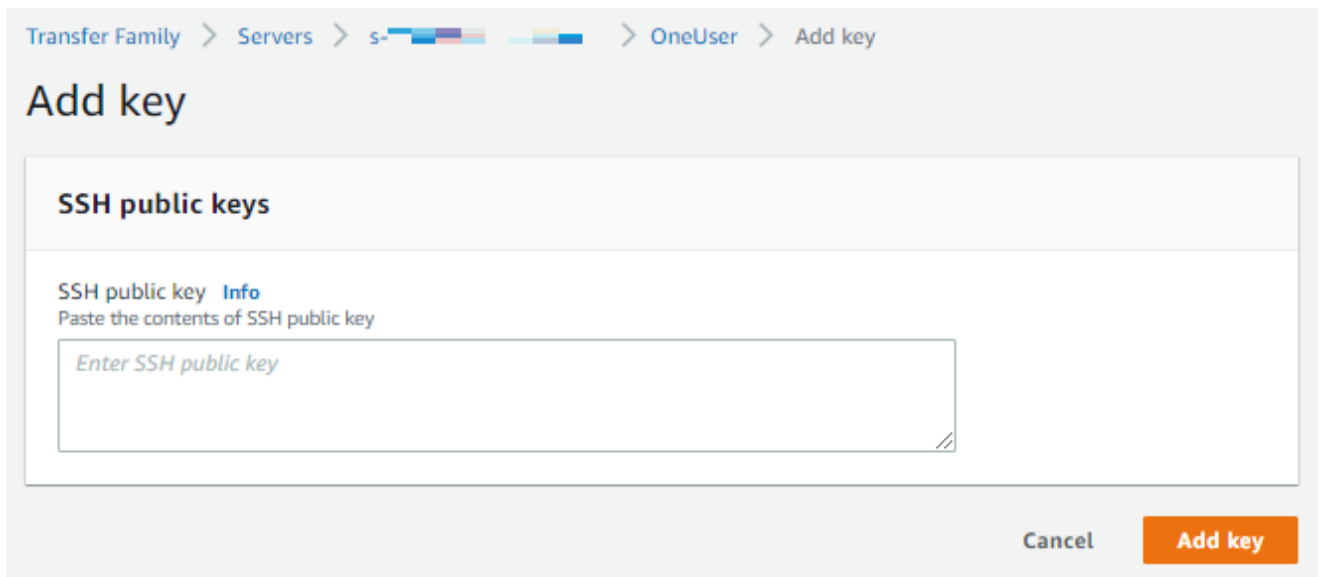
Key pair SSH Anda sekarang siap digunakan. Ikuti langkah 3 dan 4 untuk menyimpan kunci publik SSH untuk pengguna yang dikelola layanan Anda. Pengguna ini menggunakan kunci ketika mereka mentransfer file pada endpoint server Transfer Family.

3. Arahkan ke *key_name*.pub file dan buka.
4. Salin teks dan tempel di kunci publik SSH untuk pengguna yang dikelola layanan.

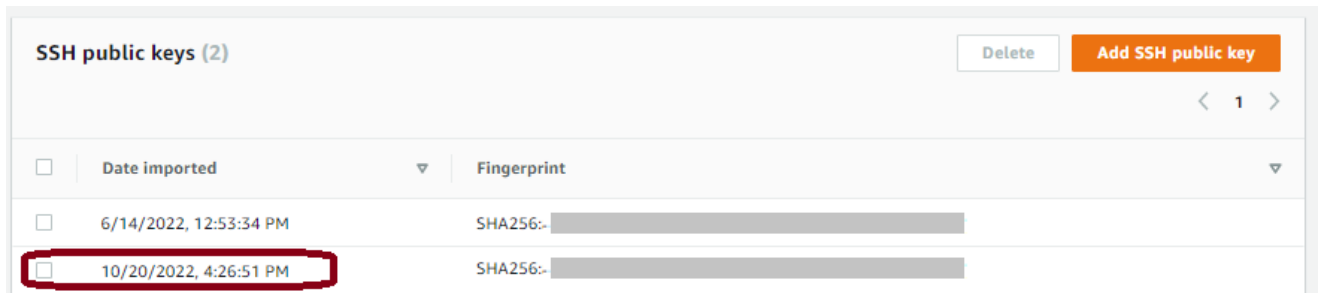
- a. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>, lalu pilih Server dari panel navigasi.
- b. Pada halaman Server, pilih ID Server untuk server yang berisi pengguna yang ingin Anda perbarui.
- c. Pilih pengguna yang Anda tambahkan kunci publiknya.
- d. Di panel kunci publik SSH, pilih Tambahkan kunci publik SSH.



- e. Tempelkan teks kunci publik yang Anda buat ke dalam kotak teks kunci publik SSH, lalu pilih Tambah kunci.



Kunci baru tercantum di panel kunci publik SSH.



☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256- [truncated]
☐	10/20/2022, 4:26:51 PM	SHA256- [truncated]

Membuat kunci SSH di Microsoft Windows

Windows menyertakan OpenSSH sebagai fitur bawaan, yang dapat Anda gunakan untuk menghasilkan kunci SSH dalam format yang sama seperti di Linux atau macOS. Atau, Anda dapat menggunakan alat pihak ketiga seperti generator kunci PuTTY (PuttyGen).

Menggunakan OpenSSH bawaan Windows

Versi terbaru Windows menyertakan OpenSSH secara default. Anda dapat menggunakan `ssh-keygen` perintah yang sama seperti yang dijelaskan di macOS/Linux bagian:

1. Buka Windows PowerShell atau Command Prompt.
2. Jalankan salah satu perintah berikut berdasarkan jenis kunci yang ingin Anda hasilkan:
 - Untuk menghasilkan key pair RSA 4096-bit:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Untuk menghasilkan pasangan kunci ECDSA 521-bit:

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Untuk menghasilkan key pair ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

3. Ikuti langkah-langkah yang sama seperti di macOS/Linux bagian untuk mengunggah kunci publik Anda AWS Transfer Family.

Menggunakan PuttyGen (alat pihak ketiga)

Beberapa klien SSH pihak ketiga untuk Windows, seperti PuTTY, menggunakan format kunci yang berbeda. PuTTY menggunakan PPK format untuk kunci pribadi. Jika Anda menggunakan Putty atau alat terkait seperti WinSCP, Anda dapat menggunakan PuttyGen untuk membuat kunci dalam format ini.

Note

Jika Anda menyajikan WinSCP dengan file kunci pribadi yang tidak .ppk dalam format, klien itu menawarkan untuk mengubah kunci .ppk menjadi format untuk Anda.

[Untuk tutorial tentang membuat kunci SSH dengan menggunakan PuttyGen, lihat situs web. SSH.com](#)

Mengonversi kunci SSH2 ke format kunci publik SSH

AWS Transfer Family hanya menerima kunci SSH-formatted publik. Jika Anda memiliki kunci publik SSH2, Anda perlu mengonversinya. Kunci publik SSH2 memiliki format berikut:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: "rsa-key-20160402"  
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI  
:  
:
```



```
----- END SSH2 PUBLIC KEY -----
```

Kunci publik SSH memiliki format berikut:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Jalankan perintah berikut untuk mengubah kunci SSH2-formatted publik menjadi kunci SSH-formatted publik. Ganti *ssh2-key* dengan nama kunci SSH2 Anda, dan *ssh-key* dengan nama kunci SSH Anda.

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

Putar tombol SSH

Untuk keamanan, kami merekomendasikan praktik terbaik untuk memutar kunci SSH Anda. Biasanya, rotasi ini ditentukan sebagai bagian dari kebijakan keamanan dan diimplementasikan dalam beberapa cara otomatis. Tergantung pada tingkat keamanan, untuk komunikasi yang sangat sensitif, key pair SSH mungkin hanya digunakan sekali. Melakukan hal ini menghilangkan risiko apa pun karena kunci yang disimpan. Namun, jauh lebih umum untuk menyimpan kredensial SSH untuk jangka waktu tertentu dan menetapkan interval yang tidak menempatkan beban yang tidak semestinya pada pengguna. Interval waktu tiga bulan adalah hal biasa.

Note

Untuk rotasi kunci SSH otomatis menggunakan infrastruktur sebagai kode, lihat [Modul Transfer Family Terraform](#).

Ada dua metode yang digunakan untuk melakukan rotasi kunci SSH:

- Di konsol, Anda dapat mengunggah kunci publik SSH baru dan menghapus kunci publik SSH yang ada.
- Dengan menggunakan API, Anda dapat memperbarui pengguna yang ada dengan menggunakan [DeleteSshPublicKey](#) API untuk menghapus kunci publik Secure Shell (SSH) pengguna dan [ImportSshPublicKey](#) API untuk menambahkan kunci publik Secure Shell (SSH) baru ke akun pengguna.

Console

Untuk melakukan rotasi kunci di konsol

1. Buka AWS Transfer Family konsol di <https://console.aws.amazon.com/transfer/>.
2. Arahkan ke halaman Server.
3. Pilih pengenalan di kolom ID Server untuk melihat halaman Detail Server.
4. Di bawah Pengguna, pilih kotak centang pengguna yang kunci publik SSH yang ingin Anda putar, lalu pilih Tindakan, lalu pilih Tambah kunci untuk melihat halaman Tambah kunci.

atau

Pilih nama pengguna untuk melihat halaman Detail pengguna, lalu pilih Tambahkan kunci publik SSH untuk melihat halaman Tambah kunci.

5. Masukkan kunci publik SSH baru dan pilih Tambah kunci.



Important

Format kunci publik SSH tergantung pada jenis kunci yang Anda hasilkan.

- Untuk kunci RSA, formatnya adalah `ssh-rsa string`.
- Untuk tombol ED25519, formatnya adalah `ssh-ed25519 string`
- Untuk kunci ECDSA, kunci dimulai dengan `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, atau `ecdsa-sha2-nistp521`, tergantung pada ukuran kunci yang Anda hasilkan. String awal kemudian diikuti oleh *string*, mirip dengan jenis kunci lainnya.

Anda dikembalikan ke halaman detail Pengguna, dan kunci publik SSH baru yang baru saja Anda masukkan muncul di bagian kunci publik SSH.

6. Pilih kotak centang kunci lama yang ingin Anda hapus dan kemudian pilih Hapus.
7. Konfirmasikan operasi penghapusan dengan memasukkan kata **delete**, lalu pilih Hapus.

API

Untuk melakukan rotasi kunci menggunakan API

1. Pada sistem operasi macOS, Linux, atau Unix, buka terminal perintah.
2. Ambil kunci SSH yang ingin Anda hapus dengan memasukkan perintah berikut. Untuk menggunakan perintah ini, ganti *serverID* dengan ID server untuk server Transfer Family Anda, dan ganti *username* dengan nama pengguna Anda.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

Perintah mengembalikan rincian tentang pengguna. Salin isi "SshPublicKeyId": bidang. Anda harus memasukkan nilai ini nanti dalam prosedur ini.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. Selanjutnya, impor kunci SSH baru untuk pengguna Anda. Di perintah , masukkan perintah berikut. Untuk menggunakan perintah ini, ganti *serverID* dengan ID server untuk server Transfer Family Anda, ganti *username* dengan nama pengguna Anda, dan ganti *public-key* dengan sidik jari kunci publik baru Anda.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-body='public-key'
```

Jika perintah berhasil, tidak ada output yang dikembalikan.

4. Terakhir, hapus kunci lama dengan menjalankan perintah berikut. Untuk menggunakan perintah ini, ganti *serverID* dengan ID server untuk server Transfer Family Anda, ganti *username* dengan nama pengguna Anda, dan ganti *keyID-from-step-2* dengan nilai ID kunci yang Anda salin di langkah 2 prosedur ini

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-id='keyID-from-step-2'
```

5. (Opsional) Untuk mengonfirmasi bahwa kunci lama tidak ada lagi, ulangi langkah 2.

Hasilkan kunci PGP

Anda dapat menggunakan dekripsi Pretty Good Privacy (PGP) dengan file yang diproses Transfer Family dengan alur kerja. Untuk menggunakan dekripsi dalam langkah alur kerja, berikan kunci PGP. Untuk informasi rinci tentang algoritma kunci PGP, termasuk rekomendasi dan kepatuhan FIPS, lihat [Algoritma key pair PGP](#)

Blog AWS penyimpanan memiliki posting yang menjelaskan cara mendekripsi file tanpa menulis kode apa pun menggunakan alur kerja Transfer Family Managed, [Enkripsi dan dekripsi file dengan PGP dan](#). AWS Transfer Family

Operator yang Anda gunakan untuk menghasilkan kunci PGP Anda bergantung pada sistem operasi Anda dan versi perangkat lunak generasi kunci yang Anda gunakan.

Jika Anda menggunakan Linux atau Unix, gunakan penginstal paket Anda untuk menginstal. gpg Tergantung pada distribusi Linux Anda, salah satu perintah berikut akan bekerja untuk Anda.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Untuk Windows atau macOS, Anda dapat mengunduh apa yang Anda butuhkan. <https://gnupg.org/download/>

Setelah Anda menginstal perangkat lunak generator kunci PGP Anda, Anda menjalankan `gpg --gen-key` perintah `gpg --full-gen-key` or untuk menghasilkan key pair.

Note

Jika Anda menggunakan GnuPG versi 2.3.0 atau yang lebih baru, Anda harus menjalankannya. `gpg --full-gen-key` Ketika diminta untuk jenis kunci yang akan dibuat, pilih RSA atau ECC. Jika Anda memilih ECC, Anda dapat memilih dari NIST, BrainPool dan Curve25519 untuk kurva elips.

gpgSubperintah yang berguna

Berikut ini adalah beberapa subperintah yang berguna untuk gpg:

- `gpg --help`— Perintah ini mencantumkan opsi yang tersedia dan mungkin menyertakan beberapa contoh.
- `gpg --list-keys`— Perintah ini mencantumkan detail untuk semua pasangan kunci yang telah Anda buat.
- `gpg --fingerprint`— Perintah ini mencantumkan detail untuk semua pasangan kunci Anda, termasuk sidik jari masing-masing tombol.
- `gpg --export -a user-name`— Perintah ini mengeksport bagian kunci publik dari kunci untuk *user-name* yang digunakan saat kunci dihasilkan.

Kelola kunci PGP

Untuk mengelola kunci PGP Anda, gunakan AWS Secrets Manager

Note

Nama rahasia Anda termasuk ID server Transfer Family Anda. Ini berarti Anda seharusnya sudah mengidentifikasi atau membuat server sebelum Anda dapat menyimpan informasi kunci PGP Anda. AWS Secrets Manager

Jika Anda ingin menggunakan satu kunci dan frasa sandi untuk semua pengguna, Anda dapat menyimpan informasi blok kunci PGP di bawah nama rahasia `aws/transfer/server-id@pgp-default`, di mana ID untuk server Transfer *server-id* Family Anda. Transfer Family menggunakan kunci default ini jika tidak ada kunci yang *user-name* cocok dengan pengguna yang menjalankan alur kerja.

Anda dapat membuat kunci untuk pengguna tertentu. Dalam hal ini, format untuk nama rahasia adalah `aws/transfer/server-id/user-name`, di mana *user-name* cocok dengan pengguna yang menjalankan alur kerja untuk server Transfer Family.

Note

Anda dapat menyimpan maksimal 3 kunci pribadi PGP, per server Transfer Family, per pengguna.

Untuk mengkonfigurasi kunci PGP untuk digunakan dengan dekripsi

1. Bergantung pada versi GPG yang Anda gunakan, jalankan salah satu perintah berikut untuk menghasilkan key pair PGP.
 - Jika Anda menggunakan **GnuPG** versi 2.3.0 atau yang lebih baru, jalankan perintah berikut:

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

Anda dapat memilih **RSA**, atau, jika Anda memilih **ECC**, Anda dapat memilih salah satu **NIST**, **BrainPool** atau **Curve25519** untuk kurva elips. Jika Anda `gpg --gen-key` menjalankannya, Anda membuat key pair yang menggunakan algoritma enkripsi ECC Curve 25519.

- Untuk versi **GnuPG** sebelum 2.3.0, Anda dapat menggunakan perintah berikut, karena RSA adalah jenis enkripsi default.

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

Important

Selama proses pembuatan kunci, Anda harus memberikan frasa sandi dan alamat email. Pastikan untuk mencatat nilai-nilai ini. Anda harus memberikan frasa sandi ketika Anda memasukkan detail kunci ke dalam prosedur ini AWS Secrets Manager nanti. Dan Anda harus memberikan alamat email yang sama untuk mengeksport kunci pribadi di langkah berikutnya.

2. Jalankan perintah berikut untuk mengeksport kunci pribadi. Untuk menggunakan perintah ini, ganti *private.pgp* dengan nama file untuk menyimpan blok kunci pribadi, dan *marymajor@example.com* dengan alamat email yang Anda gunakan saat Anda membuat key pair.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. Gunakan AWS Secrets Manager untuk menyimpan kunci PGP Anda.
 - a. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.

- b. Pada panel navigasi kiri, pilih Rahasia.
- c. Pada halaman Rahasia, pilih Simpan rahasia baru.
- d. Pada halaman Pilih jenis rahasia, untuk jenis Rahasia, pilih Jenis rahasia lainnya.
- e. Di bagian Key/value pasangan, pilih Key/valuetaab.

- Kunci — Masukkan **PGPPrivateKey**.

 Note

Anda harus memasukkan **PGPPrivateKey** string dengan tepat: jangan menambahkan spasi sebelum atau di antara karakter.

- nilai — Tempelkan teks kunci pribadi Anda ke bidang nilai. Anda dapat menemukan teks kunci pribadi Anda dalam file (misalnya, `private.pgp`) yang Anda tentukan saat Anda mengekspor kunci Anda sebelumnya dalam prosedur ini. Kuncinya dimulai dengan `-----BEGIN PGP PRIVATE KEY BLOCK-----` dan diakhiri dengan `-----END PGP PRIVATE KEY BLOCK-----`.

 Note

Pastikan bahwa blok teks hanya berisi kunci pribadi dan tidak mengandung kunci publik juga.

- f. Pilih Tambahkan baris dan di bagian Key/value pasangan, pilih Key/valuetaab.

- Kunci — Masukkan **PGPPassphrase**.

 Note

Anda harus memasukkan **PGPPassphrase** string dengan tepat: jangan menambahkan spasi sebelum atau di antara karakter.

- value — Masukkan kata sandi yang Anda gunakan saat membuat key pair PGP Anda.

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	mypassphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager [Add new key](#)

Note

Anda dapat menambahkan hingga 3 set kunci dan frasa sandi. Untuk menambahkan set kedua, tambahkan dua baris baru, dan masukkan **PGPPrivateKey2** dan **PGPPassphrase2** untuk kunci, dan tempel di kunci pribadi dan frasa sandi lainnya. Untuk menambahkan set ketiga, nilai kunci harus **PGPPrivateKey3** dan **PGPPassphrase3**.

- g. Pilih Berikutnya.
- h. Pada halaman Konfigurasi rahasia, masukkan nama dan deskripsi untuk rahasia Anda.
 - Jika Anda membuat kunci default, yaitu kunci yang dapat digunakan oleh pengguna Transfer Family, masukkan **aws/transfer/server-id/@pgp-default**. Ganti **server-id** dengan ID server yang berisi alur kerja yang memiliki langkah dekripsi.
 - Jika Anda membuat kunci untuk digunakan oleh pengguna Transfer Family tertentu, masukkan **aws/transfer/server-id/user-name**. Ganti **server-id** dengan ID server yang berisi alur kerja yang memiliki langkah dekripsi, dan ganti **user-name**

dengan nama pengguna yang menjalankan alur kerja. *user-name* Ini disimpan di penyedia identitas yang digunakan server Transfer Family.

- i. Pilih Berikutnya dan terima default pada halaman Konfigurasi rotasi. Lalu pilih Selanjutnya.
- j. Pada halaman Review, pilih Store untuk membuat dan menyimpan rahasia.

Tangkapan layar berikut menunjukkan detail untuk pengguna **marymajor** untuk server Transfer Family tertentu. Contoh ini menunjukkan tiga kunci dan frasa sandi yang sesuai.

The screenshot shows the AWS Secrets Manager console for a secret named `/aws/transfer/s-.../marymajor`. The secret is stored in the `aws/secretsmanager` encryption key. The secret value is displayed in a table with three rows, each containing a PGP private key and a corresponding passphrase.

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase3	mypassphrase3

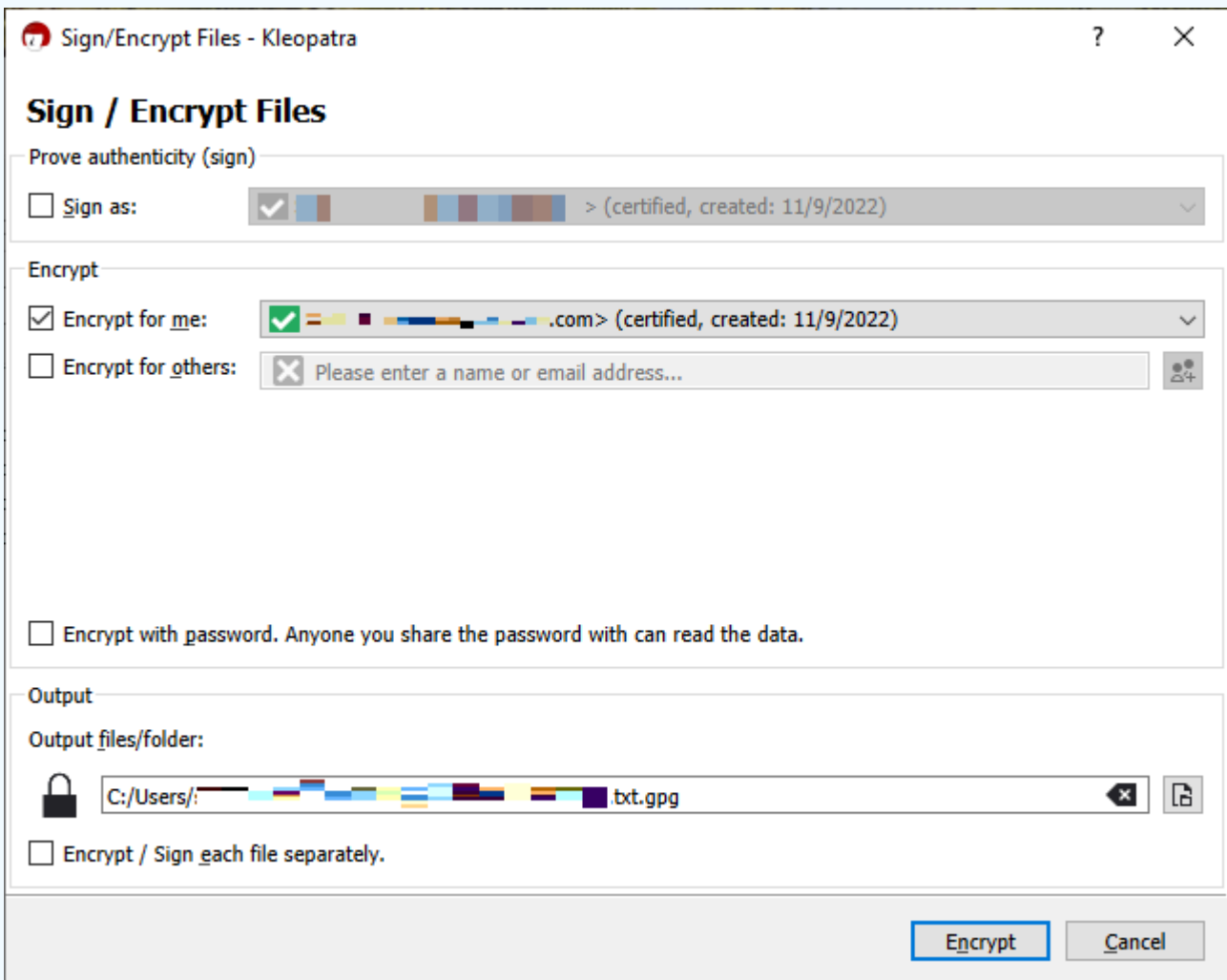
Klien PGP yang didukung

Klien berikut telah diuji dengan Transfer Family dan dapat digunakan untuk menghasilkan kunci PGP, dan untuk mengenkripsi file yang ingin Anda dekripsi dengan alur kerja.

- GPG4win + Kleopatra.

Note

Saat Anda memilih Sign/Encrypt Files, pastikan untuk menghapus pilihan untuk Sign as: saat ini kami tidak mendukung penandatanganan untuk file terenkripsi.



Jika Anda menandatangani file terenkripsi dan mencoba mengunggahnya ke server Transfer Family dengan alur kerja dekripsi, Anda menerima kesalahan berikut:

Encrypted file with signed message unsupported

- Versi GnuPG utama: 2.4, 2.3, 2.2, 2.0, dan 1.4.

Perhatikan bahwa klien PGP lain mungkin bekerja juga, tetapi hanya klien yang disebutkan di sini yang telah diuji dengan Transfer Family.

Identitas dan manajemen akses untuk AWS Transfer Family

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang

dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Transfer Family IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Transfer Family bekerja dengan IAM](#)
- [AWS Transfer Family contoh kebijakan berbasis identitas](#)
- [AWS Transfer Family contoh kebijakan berbasis tag](#)
- [Pemecahan masalah AWS Transfer Family identitas dan akses](#)
- [Kunci kondisi IAM untuk tata kelola organisasi](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Pemecahan masalah AWS Transfer Family identitas dan akses](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana AWS Transfer Family bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [AWS Transfer Family contoh kebijakan berbasis identitas](#))

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Pengguna root akun AWS

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan

memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3.

Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana AWS Transfer Family bekerja dengan IAM

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses AWS Transfer Family, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan. AWS Transfer Family Untuk mendapatkan pandangan tingkat tinggi tentang bagaimana AWS Transfer Family dan AWS layanan lain bekerja dengan IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Topik

- [AWS Transfer Family kebijakan berbasis identitas](#)
- [AWS Transfer Family kebijakan berbasis sumber daya](#)
- [Otorisasi berdasarkan AWS Transfer Family tag](#)
- [AWS Transfer Family Peran IAM](#)

AWS Transfer Family kebijakan berbasis identitas

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi di mana tindakan tersebut diperbolehkan atau ditolak. AWS Transfer Family mendukung tindakan tertentu, sumber daya, dan kunci syarat. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat [referensi elemen kebijakan IAM JSON di Panduan](#) Pengguna.AWS Identity and Access Management

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan AWS Transfer Family menggunakan awalan berikut sebelum tindakan: `transfer:`. Misalnya, untuk memberikan izin kepada seseorang untuk membuat server, dengan operasi Transfer Family `CreateServer` API, Anda menyertakan `transfer:CreateServer` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus menyertakan elemen `Action` atau `NotAction`. AWS Transfer Family menentukan serangkaian tindakan sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut.

```
"Action": [  
    "transfer:action1",  
    "transfer:action2"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut.

```
"Action": "transfer:Describe*"
```

Untuk melihat daftar AWS Transfer Family tindakan, lihat [Tindakan yang ditentukan oleh AWS Transfer Family](#) dalam Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*" 
```

Sumber daya server Transfer Family memiliki ARN berikut.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```


Misalnya, untuk menentukan server `s-01234567890abcdef` Transfer Family dalam pernyataan Anda, gunakan ARN berikut.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Untuk informasi selengkapnya tentang format ARN, lihat [Nama Sumber Daya Amazon \(ARN\)](#) di Referensi Otorisasi Layanan, atau [ARN IAM](#) di Panduan Pengguna IAM.

Untuk menentukan semua instance milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

Beberapa AWS Transfer Family tindakan dilakukan pada beberapa sumber daya, seperti yang digunakan dalam kebijakan IAM. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

Dalam beberapa kasus, Anda perlu menentukan lebih dari satu jenis sumber daya, misalnya, jika Anda membuat kebijakan yang memungkinkan akses ke server dan pengguna Transfer Family. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Untuk melihat daftar AWS Transfer Family sumber daya, lihat [Jenis sumber daya yang ditentukan oleh AWS Transfer Family](#) dalam Referensi Otorisasi Layanan.

Kunci syarat

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang

diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

AWS Transfer Family mendefinisikan kumpulan kunci kondisinya sendiri dan juga mendukung penggunaan beberapa kunci kondisi global. Untuk melihat daftar kunci AWS Transfer Family kondisi, lihat [Kunci kondisi untuk AWS Transfer Family](#) dalam Referensi Otorisasi Layanan.

Contoh

Untuk melihat contoh kebijakan AWS Transfer Family berbasis identitas, lihat. [AWS Transfer Family contoh kebijakan berbasis identitas](#) Untuk kebijakan IAM khusus titik akhir VPC, lihat. [Membatasi akses endpoint VPC untuk server Transfer Family](#)

AWS Transfer Family kebijakan berbasis sumber daya

Resource-based kebijakan adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada AWS Transfer Family sumber daya dan dalam kondisi apa. Amazon S3 mendukung kebijakan izin berbasis sumber daya untuk Amazon S3.

buckets Resource-based kebijakan memungkinkan Anda memberikan izin penggunaan ke akun lain berdasarkan per sumber daya. Anda juga dapat menggunakan kebijakan berbasis sumber daya untuk mengizinkan AWS layanan mengakses Amazon S3 Anda. *buckets*

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai [prinsipal di kebijakan berbasis sumber daya](#). Menambahkan principal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berada di AWS akun yang berbeda, Anda juga harus memberikan izin entitas utama untuk mengakses sumber daya. Berikan izin dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, [lihat Perbedaan peran IAM dari kebijakan berbasis sumber daya](#) di Panduan Pengguna.AWS Identity and Access Management

Layanan Amazon S3 hanya mendukung satu jenis kebijakan berbasis sumber daya yang disebut *bucket*kebijakan, yang dilampirkan ke file. *bucket* Kebijakan ini menentukan entitas utama mana (akun, pengguna, peran, dan pengguna gabungan) yang dapat melakukan tindakan pada objek.

Contoh

Untuk melihat contoh kebijakan AWS Transfer Family berbasis sumber daya, lihat. [AWS Transfer Family contoh kebijakan berbasis tag](#)

Otorisasi berdasarkan AWS Transfer Family tag

Anda dapat melampirkan tag ke AWS Transfer Family sumber daya atau meneruskan tag dalam permintaan AWS Transfer Family. Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `transfer:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`. Untuk informasi tentang cara menggunakan tag untuk mengontrol akses ke AWS Transfer Family sumber daya, lihat [AWS Transfer Family contoh kebijakan berbasis tag](#).

AWS Transfer Family Peran IAM

[Peran IAM](#) adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensi sementara dengan AWS Transfer Family

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensial keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau [GetFederationToken](#).

AWS Transfer Family mendukung menggunakan kredensi sementara.

AWS Transfer Family contoh kebijakan berbasis identitas

Secara default, pengguna dan IAM role tidak memiliki izin untuk membuat atau memodifikasi AWS Transfer Family sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan pada tab JSON di Panduan Pengguna](#). AWS Identity and Access Management

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan AWS Transfer Family konsol](#)
- [Izinkan para pengguna untuk melihat izin mereka sendiri](#)

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS Transfer Family sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS Anda. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan terkelola AWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan AWS Transfer Family konsol

Untuk mengakses AWS Transfer Family konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Transfer Family sumber daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) di Panduan AWS Identity and Access Management Pengguna.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
    },
  ],
}
```

```
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
```

AWS Transfer Family contoh kebijakan berbasis tag

Berikut ini adalah contoh cara mengontrol akses ke AWS Transfer Family sumber daya berdasarkan tag.

Menggunakan tag untuk mengontrol akses AWS Transfer Family sumber daya

Ketentuan dalam kebijakan IAM adalah bagian dari sintaks yang Anda gunakan untuk menentukan izin ke sumber daya. AWS Transfer Family Anda dapat mengontrol akses ke AWS Transfer Family sumber daya (seperti pengguna, server, peran, dan entitas lain) berdasarkan tag pada sumber daya tersebut. Tag adalah pasangan kunci-nilai. Untuk informasi selengkapnya tentang menandai sumber daya, lihat [Menandai AWS sumber daya](#) di. Referensi Umum AWS

Di AWS Transfer Family, sumber daya dapat memiliki tag, dan beberapa tindakan dapat menyertakan tag. Saat membuat kebijakan IAM, Anda dapat menggunakan kunci syarat tanda berikut:

- Pengguna mana yang dapat melakukan tindakan pada AWS Transfer Family sumber daya, berdasarkan tag yang dimiliki sumber daya.
- Tag apa yang dapat diteruskan dalam permintaan tindakan.
- Apakah kunci tag tertentu dapat digunakan dalam permintaan.

Dengan menggunakan kontrol akses berbasis tag, Anda dapat menerapkan kontrol yang lebih baik daripada di API level. Anda juga dapat menerapkan kontrol yang lebih dinamis daripada dengan menggunakan kontrol akses berbasis sumber daya. Anda dapat membuat kebijakan IAM yang mengizinkan atau menolak operasi berdasarkan tag yang disediakan dalam permintaan (tag permintaan). Anda juga dapat membuat kebijakan IAM berdasarkan tag pada sumber daya yang sedang dioperasikan (tag sumber daya). Secara umum, tag sumber daya adalah untuk tag yang sudah ada di sumber daya, tag permintaan digunakan saat Anda menambahkan tag atau menghapus tag dari sumber daya.

Untuk sintaks dan semantik lengkap kunci kondisi tag, lihat [Mengontrol akses ke AWS sumber daya menggunakan tag sumber daya di Panduan Pengguna](#) IAM. Untuk detail tentang menentukan kebijakan IAM dengan API Gateway, lihat [Mengontrol akses ke API dengan izin IAM](#) di Panduan Pengembang API Gateway.

Contoh 1: Tolak tindakan berdasarkan tag sumber daya

Anda dapat menolak tindakan yang akan dilakukan pada sumber daya berdasarkan tag. Contoh kebijakan berikut menyangkal `TagResource`, `UntagResource`, `StartServer`, `StopServer`, `DescribeServer`, dan `DescribeUser` operasi jika sumber daya pengguna atau server ditandai dengan kunci stage dan nilainya. `prod`

```
{
  "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"
        }
      }
    }
  ]
}
```

```

    }
  }
]
}

```

Contoh 2: Izinkan tindakan berdasarkan tag sumber daya

Anda dapat mengizinkan tindakan dilakukan pada sumber daya berdasarkan tag. Contoh kebijakan berikut

memungkinkan `TagResource`, `UntagResource`, `StartServer`, `StopServer`, `DescribeServer`, dan `DescribeUser` operasi jika sumber daya pengguna atau server ditandai dengan kunci `stage` dan nilainya `prod`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}

```

Contoh 3: Tolak pembuatan pengguna atau server berdasarkan tag permintaan

Contoh kebijakan berikut berisi dua pernyataan. Pernyataan pertama menyangkal `CreateServer` operasi pada semua sumber daya jika kunci pusat biaya untuk tag tidak memiliki nilai.

Pernyataan kedua menyangkal CreateServer operasi jika kunci pusat biaya untuk tag berisi nilai lain selain 1, 2 atau 3.

 Note

Kebijakan ini memungkinkan pembuatan atau penghapusan sumber daya yang berisi kunci yang dipanggil costcenter dan nilai1,2, atau3.

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

```
]
}
```

Pemecahan masalah AWS Transfer Family identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Transfer Family dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di AWS Transfer Family](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya AWS akun untuk mengakses AWS Transfer Family sumber daya](#)

Saya tidak berwenang untuk melakukan tindakan di AWS Transfer Family

Jika Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna mateojackson IAM mencoba menggunakan konsol untuk melihat detail tentang *widget* tetapi tidak memiliki `transfer:GetWidget` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
transfer:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *my-example-widget* menggunakan tindakan `transfer::GetWidget`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Transfer Family.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di AWS Transfer Family. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Kebijakan contoh berikut berisi izin untuk meneruskan peran AWS Transfer Family. Ganti **123456789012** dengan ID akun AWS Anda dan **MyTransferRole** dengan nama peran IAM Anda yang sebenarnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "Effect": "Allow"
    }
  ]
}
```

Saya ingin mengizinkan orang di luar saya AWS akun untuk mengakses AWS Transfer Family sumber daya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS Transfer Family mendukung fitur-fitur ini, lihat [Bagaimana AWS Transfer Family bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

Kunci kondisi IAM untuk tata kelola organisasi

AWS Transfer Family menyediakan kunci kondisi IAM yang memungkinkan Anda membatasi konfigurasi sumber daya dalam kebijakan IAM apa pun. Kunci kondisi ini dapat digunakan dalam kebijakan berbasis identitas yang dilampirkan pada pengguna atau peran, atau Kebijakan Kontrol Layanan (SCP) untuk tata kelola organisasi.

Kebijakan Kontrol Layanan adalah kebijakan IAM yang berlaku untuk seluruh AWS organisasi, menyediakan pagar pembatas pencegahan di beberapa akun. Saat digunakan di SCP, kunci kondisi ini membantu menegakkan persyaratan keamanan dan kepatuhan di seluruh organisasi.

Lihat juga

- [Tindakan, sumber daya, dan kunci kondisi untuk Transfer Family](#)
- [Kebijakan kontrol layanan \(SCP\)](#)
- Lihat [video ini](#) yang menjelaskan cara menerapkan pagar pembatas preventif menggunakan kebijakan kontrol layanan

Kunci kondisi yang tersedia

AWS Transfer Family mendukung kunci kondisi berikut untuk digunakan dalam kebijakan IAM:

`transfer:RequestServerEndpointType`

Membatasi pembuatan dan pembaruan server berdasarkan jenis endpoint (PUBLIC, VPC, VPC_ENDPOINT). Umumnya digunakan untuk mencegah titik akhir yang menghadap publik.

`transfer:RequestServerProtocols`

Membatasi pembuatan dan pembaruan server berdasarkan protokol yang didukung (SFTP, FTPS, FTP, AS2).

`transfer:RequestServerDomain`

Membatasi pembuatan server berdasarkan jenis domain (S3, EFS).

`transfer:RequestConnectorProtocol`

Membatasi pembuatan konektor berdasarkan protokol (AS2, SFTP).

Tindakan yang didukung

Kunci kondisi dapat diterapkan pada AWS Transfer Family tindakan berikut:

- `CreateServer`: Mendukung `RequestServerEndpointType`, `RequestServerProtocols`, dan tombol `RequestServerDomain` kondisi
- `UpdateServer`: Mendukung `RequestServerEndpointType` dan tombol `RequestServerProtocols` kondisi
- `CreateConnector`: Mendukung kunci `RequestConnectorProtocol` kondisi

Contoh kebijakan SCP

Contoh SCP berikut mencegah pembuatan AWS Transfer Family server publik di seluruh organisasi Anda:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
```

```
"Resource": "*",
"Condition": {
  "StringEquals": {
    "transfer:RequestServerEndpointType": "PUBLIC"
  }
}
}]
}
```

Validasi kepatuhan untuk AWS Transfer Family

Third-party auditor menilai keamanan dan kepatuhan AWS Transfer Family sebagai bagian dari beberapa program AWS kepatuhan. Hal ini mencakup SOC, PCI, HIPAA, dan lainnya. Untuk daftar lengkapnya, lihat [AWS Layanan dalam Lingkup menurut Program Kepatuhan](#).

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS layanan dalam lingkup oleh program kepatuhan](#). Untuk informasi umum, lihat [Program kepatuhan AWS](#).

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan AWS Transfer Family ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan memulai cepat keamanan dan kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- [Arsitektur untuk whitepaper keamanan dan kepatuhan HIPAA — Whitepaper](#) ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi. AWS HIPAA-compliant
- [Sumber daya kepatuhan AWS](#) – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Config](#) AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub CSPM](#)— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di AWS Transfer Family

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

AWS Transfer Family mendukung hingga 3 Availability Zones dan didukung oleh penskalaan otomatis, armada redundan untuk permintaan koneksi dan transfer Anda.

Untuk semua titik akhir Transfer Family:

- Zone-level Redundansi ketersediaan dibangun ke dalam layanan.
- Ada armada redundan untuk setiap AZ.
- Redundansi ini disediakan secara otomatis.

Note

Untuk titik akhir di Virtual Private Cloud (VPC), dimungkinkan untuk menyediakan satu subnet. Namun, kami menyarankan Anda membuat titik akhir di beberapa zona ketersediaan dalam VPC Anda, untuk mengurangi risiko gangguan layanan selama pemadaman Zona Ketersediaan.

Lihat juga

- Untuk detail tentang cara membuat server Transfer Family di VPC, lihat [Buat server di cloud pribadi virtual](#)
- Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [infrastruktur AWS global](#).
- Untuk contoh tentang cara membangun redundansi yang lebih tinggi dan meminimalkan latensi jaringan dengan menggunakan Latency-based perutean, lihat posting blog [Minimalkan latensi jaringan](#) dengan server Anda. AWS Transfer Family

Buat koneksi pribadi antara VPC dan AWS Transfer Family API

Anda dapat membuat koneksi pribadi antara VPC dan AWS Transfer Family API Anda dengan membuat titik akhir VPC antarmuka, yang didukung oleh [AWS PrivateLink](#). Anda dapat mengakses AWS Transfer Family API seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans dalam VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API AWS Transfer Family.

Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Untuk informasi selengkapnya, lihat [Akses AWS layanan melalui AWS PrivateLink AWS PrivateLink Panduan](#). Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk AWS Transfer Family API, tinjau [Pertimbangan dalam Panduan](#).AWS PrivateLink

Mengontrol akses menggunakan kebijakan titik akhir VPC

Secara default, akses penuh ke AWS Transfer Family API diizinkan melalui titik akhir. Anda dapat mengontrol akses ke titik akhir antarmuka menggunakan kebijakan titik akhir VPC. Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke API. AWS Transfer Family Kebijakan titik akhir menentukan informasi berikut:

- Kepala sekolah yang dapat melakukan tindakan.
- Tindakan yang bisa dilakukan.
- Sumber daya di mana tindakan dapat dilakukan.

Untuk informasi selengkapnya, lihat [Mengontrol Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Berikut ini adalah contoh kebijakan endpoint untuk AWS Transfer Family API. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke semua tindakan AWS Transfer Family API di semua sumber daya, kecuali yang ditandai dengan kunci Environment dan nilai Test

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
```



```
        "StringEquals": {
            "aws:ResourceTag/Environment": "Test"
        }
    }, {
        "Effect": "Allow",
        "Action": "transfer:*",
        "Principal": "*",
        "Resource": "*"
    }]
}
```

Buat titik akhir VPC antarmuka untuk AWS Transfer Family API

Anda dapat membuat titik akhir VPC untuk AWS Transfer Family API menggunakan konsol VPC Amazon atau Antarmuka Baris AWS Perintah ().AWS CLI Untuk informasi selengkapnya, lihat [Membuat titik akhir VPC](#) di Panduan Pengguna AWS PrivateLink.

Buat titik akhir VPC untuk AWS Transfer Family API menggunakan salah satu nama layanan berikut:

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Untuk membuat antarmuka VPC endpoint yang sesuai dengan Standar Pemrosesan Informasi Federal (FIPS) Publikasi 140-3 standar pemerintah AS.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke AWS Transfer Family API menggunakan nama DNS default untuk Wilayah, misalnya, `transfer.us-east-1.amazonaws.com`

Keamanan infrastruktur di AWS Transfer Family

Sebagai layanan terkelola, AWS Transfer Family dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Transfer Family melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Hindari menempatkan NLB dan NAT di depan AWS Transfer Family server

Note

Server yang dikonfigurasi dengan protokol FTP dan FTPS hanya mengizinkan konfigurasi dengan VPC: tidak ada titik akhir publik yang tersedia untuk FTP/FTPS

Banyak pelanggan mengonfigurasi Network Load Balancer (NLB) untuk merutekan lalu lintas ke server mereka. AWS Transfer Family Mereka biasanya melakukan ini baik karena mereka membuat server mereka sebelum AWS menawarkan cara untuk mengaksesnya dari dalam VPC mereka dan dari internet, atau untuk mendukung FTP di internet. Konfigurasi ini tidak hanya meningkatkan biaya bagi pelanggan, tetapi juga dapat menyebabkan masalah lain, yang kami jelaskan di bagian ini.

Gateway NAT adalah komponen wajib ketika klien terhubung dari jaringan pribadi pelanggan di belakang firewall perusahaan. Namun, Anda harus menyadari bahwa ketika banyak klien berada di belakang gateway NAT yang sama, ini dapat memengaruhi batas kinerja dan koneksi. Jika ada NLB atau NAT di jalur komunikasi dari klien ke server FTP atau FTPS, server tidak dapat secara akurat mengenali alamat IP klien, karena hanya AWS Transfer Family melihat alamat IP NLB atau NAT.

Jika Anda menggunakan konfigurasi server Transfer Family di belakang NLB, sebaiknya Anda pindah ke titik akhir VPC dan menggunakan alamat IP Elastis alih-alih menggunakan NLB. Saat menggunakan gateway NAT, perhatikan batasan koneksi yang dijelaskan di bawah ini.

Jika Anda menggunakan protokol FTPS, konfigurasi ini tidak hanya mengurangi kemampuan Anda untuk mengaudit siapa yang mengakses server Anda, tetapi juga dapat memengaruhi kinerja. AWS Transfer Family menggunakan alamat IP sumber untuk menghancurkan koneksi Anda di seluruh bidang data kami. Untuk FTPS, ini berarti bahwa alih-alih memiliki 10.000 koneksi simultan, server Transfer Family dengan gateway NLB atau NAT pada rute komunikasi dibatasi hanya 300 koneksi simultan.

Meskipun kami menyarankan untuk menghindari Network Load Balancer di depan AWS Transfer Family server, jika implementasi FTP atau FTPS Anda memerlukan NLB atau NAT dalam rute komunikasi dari klien, ikuti rekomendasi ini:

- Untuk NLB, gunakan port 21 untuk pemeriksaan kesehatan, bukan port 8192-8200.
- Untuk AWS Transfer Family server, aktifkan dimulainya kembali sesi TLS dengan pengaturan. `TlsSessionResumptionMode = ENFORCED`

Note

Ini adalah mode yang disarankan, karena memberikan keamanan yang ditingkatkan:

- Membutuhkan klien untuk menggunakan dimulainya kembali sesi TLS untuk koneksi berikutnya.
 - Memberikan jaminan keamanan yang lebih kuat dengan memastikan parameter enkripsi yang konsisten.
 - Membantu mencegah potensi serangan downgrade.
 - Menjaga kepatuhan terhadap standar keamanan sambil mengoptimalkan kinerja.
- Jika memungkinkan, bermigrasi dari menggunakan NLB untuk memanfaatkan batas AWS Transfer Family kinerja dan koneksi sepenuhnya.

Untuk panduan tambahan tentang alternatif NLB, hubungi tim Manajemen AWS Transfer Family Produk melalui Support AWS . Untuk informasi lebih lanjut tentang meningkatkan postur keamanan Anda, lihat posting blog [Enam tips untuk meningkatkan keamanan AWS Transfer Family server Anda](#).

Keamanan infrastruktur konektivitas VPC

Konektor SFTP dengan tipe jalan keluar VPC memberikan keamanan infrastruktur yang ditingkatkan melalui isolasi jaringan dan konektivitas pribadi:

Manfaat isolasi jaringan

- Lalu lintas jaringan pribadi: Semua lalu lintas konektor ke server SFTP pribadi tetap berada dalam VPC Anda, tidak pernah melintasi internet publik.
- Jalan keluar terkontrol: Untuk titik akhir publik yang diakses melalui VPC, rute lalu lintas melalui gateway NAT Anda, memberi Anda kontrol atas alamat IP jalan keluar dan kebijakan jaringan.

- Kontrol keamanan VPC: Manfaatkan grup keamanan VPC yang ada, ACL jaringan, dan tabel rute untuk mengontrol akses jaringan konektor.
- Konektivitas hibrid: Akses server SFTP lokal melalui koneksi VPN atau Direct Connect yang sudah ada tanpa eksposur internet tambahan.

Pertimbangan keamanan Resource Gateway

Resource Gateways menyediakan titik masuk yang aman untuk Cross-VPC Akses Sumber Daya:

- Multi-AZ deployment: Resource Gateways memerlukan subnet di setidaknya dua Availability Zone untuk ketersediaan tinggi dan toleransi kesalahan.
- Kontrol grup keamanan: Konfigurasi grup keamanan untuk membatasi akses ke port SFTP (biasanya port 22) dari sumber resmi saja.
- Penempatan subnet pribadi: Menyebarkan Resource Gateways di subnet pribadi saat menghubungkan ke server SFTP pribadi untuk mempertahankan isolasi jaringan.
- Batas koneksi: Setiap Resource Gateway mendukung hingga 350 koneksi bersamaan dengan batas waktu idle 350 detik untuk koneksi TCP.

Tambahkan firewall aplikasi web

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Anda dapat menggunakannya untuk mengonfigurasi seperangkat aturan yang dikenal sebagai daftar kontrol akses web (web ACL) yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Untuk informasi selengkapnya, lihat [Menggunakan AWS WAF untuk melindungi API Anda](#).

Untuk menambahkan AWS WAF

1. Buka konsol API Gateway di <https://console.aws.amazon.com/apigateway/>.
2. Di panel navigasi API, lalu pilih templat penyedia identitas kustom Anda.
3. Memilih Tahapan.
4. Di panel Tahapan, pilih nama panggung.
5. Di panel Editor Panggung, pilih Pengaturan tab.
6. Lakukan salah satu tindakan berikut:

- Di bawah Web Application Firewall (WAF), untuk Web ACL, pilih ACL web yang ingin Anda kaitkan dengan tahap ini.
- Jika ACL web yang Anda butuhkan tidak ada, Anda harus membuatnya dengan melakukan hal berikut:
 1. Pilih Buat Web ACL.
 2. Di beranda layanan AWS WAF, pilih Buat web ACL.
 3. Dalam detail Web ACL, untuk Nama, ketikkan nama ACL web.
 4. Di Aturan, pilih Tambahkan aturan, lalu pilih Tambahkan aturan dan grup aturan saya sendiri.
 5. Untuk tipe Rule, pilih IP set untuk mengidentifikasi daftar alamat IP tertentu.
 6. Untuk Aturan, masukkan nama aturan.
 7. Untuk set IP, pilih set IP yang ada. Untuk membuat kumpulan IP, lihat [Membuat set IP](#).
 8. Untuk alamat IP yang akan digunakan sebagai alamat asal, pilih alamat IP di header.
 9. Untuk nama bidang Header, masukkan SourceIP.
 10. Untuk Posisi di dalam header, pilih Alamat IP Pertama.
 11. Untuk Fallback untuk alamat IP yang hilang, pilih Match or No Match tergantung pada bagaimana Anda ingin menangani alamat IP yang tidak valid (atau hilang) di header.
 12. Untuk Tindakan, pilih tindakan set IP.
 13. Untuk tindakan ACL web default untuk permintaan yang tidak cocok dengan aturan apa pun, pilih Izinkan atau Blokir, lalu klik Berikutnya.
 14. Untuk langkah 4 dan 5, pilih Berikutnya.
 15. Di Tinjau dan buat, tinjau pilihan Anda, lalu pilih Buat ACL web.
- 7. Pilih Simpan Perubahan.
- 8. Pilih Sumber daya.
- 9. Untuk Tindakan, pilih Deploy API.

Untuk informasi tentang cara aman Transfer Family dengan firewall aplikasi AWS web, lihat [Mengamankan Transfer Family dengan firewall AWS aplikasi dan Amazon API Gateway](#) di blog AWS penyimpanan.

Cross-service pencegahan wakil bingung

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Cross-service peniruan identitas dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda. Untuk penjelasan rinci tentang masalah ini, lihat [masalah wakil yang membingungkan](#) di Panduan Pengguna IAM.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global dalam kebijakan sumber daya untuk membatasi izin yang dimiliki AWS Transfer Family untuk sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan Nama Sumber Daya Amazon (ARN) yang tepat dari sumber daya yang ingin Anda izinkan. Jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan karakter wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:transfer::region::account-id:server/*`.

AWS Transfer Family menggunakan jenis peran berikut:

- Peran pengguna — Memungkinkan pengguna yang dikelola layanan mengakses sumber daya Transfer Family yang diperlukan. AWS Transfer Family mengambil peran ini dalam konteks ARN pengguna Transfer Family.
- Peran akses - Menyediakan akses hanya ke file Amazon S3 yang sedang ditransfer. Untuk transfer AS2 masuk, peran akses menggunakan Amazon Resource Name (ARN) untuk perjanjian. Untuk transfer AS2 keluar, peran akses menggunakan ARN untuk konektor.
- Peran pemanggilan — Untuk digunakan dengan Amazon API Gateway sebagai penyedia identitas kustom server. Transfer Family mengasumsikan peran ini dalam konteks ARN server Transfer Family.
- Peran logging - Digunakan untuk log entri ke Amazon CloudWatch. Transfer Family menggunakan peran ini untuk mencatat detail keberhasilan dan kegagalan bersama dengan informasi tentang

transfer file. Transfer Family mengasumsikan peran ini dalam konteks ARN server Transfer Family. Untuk transfer AS2 keluar, peran logging menggunakan konektor ARN.

- Peran eksekusi — Memungkinkan pengguna Transfer Family memanggil dan meluncurkan alur kerja. Transfer Family mengasumsikan peran ini dalam konteks alur kerja Transfer Family ARN.

Untuk informasi selengkapnya, lihat [Kebijakan dan izin di IAM](#) dalam Panduan Pengguna IAM.

Note

Dalam contoh berikut, ganti masing-masing *user input placeholder* dengan informasi Anda sendiri.

Note

Dalam contoh kami, kami menggunakan keduanya `ArnLike` dan `ArnEquals`. Mereka identik secara fungsional, dan oleh karena itu Anda dapat menggunakan keduanya ketika Anda membuat kebijakan Anda. Dokumentasi Transfer Family digunakan `ArnLike` ketika kondisi berisi karakter wildcard, dan `ArnEquals` untuk menunjukkan kondisi kecocokan yang tepat.

AWS Transfer Family peran pengguna lintas layanan pencegahan wakil yang membingungkan

Contoh kebijakan berikut memungkinkan setiap pengguna dari server mana pun di akun untuk mengambil peran.

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

```

        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/
*\"
        }
    }
}

```

Contoh kebijakan berikut memungkinkan setiap pengguna dari server tertentu untuk mengambil peran.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/
*\"
        }
      }
    }
  ]
}

```

Contoh kebijakan berikut memungkinkan pengguna tertentu dari server tertentu untuk mengambil peran.


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/user-name"
        }
      }
    }
  ]
}
```

AWS Alur kerja Transfer Family peran lintas layanan membingungkan pencegahan wakil

Contoh kebijakan berikut memungkinkan alur kerja apa pun di akun untuk mengambil peran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
```

```

        "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/*"
    }
}
]
}

```

Contoh kebijakan berikut memungkinkan alur kerja tertentu untuk mengambil peran.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}

```

AWS Peran konektor Transfer Family lintas layanan pencegahan wakil yang membingungkan

Contoh kebijakan berikut memungkinkan konektor apa pun di akun untuk mengambil peran.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
      }
    }
  }
]
}

```

Contoh kebijakan berikut memungkinkan konektor tertentu untuk mengambil peran.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/connector-id"
        }
      }
    }
  ]
}

```

AWS Transfer Family logging dan peran doa lintas layanan membingungkan deputi pencegahan

Note

Contoh berikut dapat digunakan dalam peran logging dan pemanggilan. Dalam contoh ini, Anda dapat menghapus detail ARN untuk alur kerja jika server Anda tidak memiliki alur kerja yang melekat padanya.

Contoh logging/invoke kebijakan berikut memungkinkan setiap server (dan alur kerja) dalam akun untuk mengambil peran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

Contoh logging/invoke kebijakan berikut memungkinkan server tertentu (dan alur kerja) untuk mengambil peran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/server-id",
            "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}
```

AWS kebijakan terkelola untuk AWS Transfer Family

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk [membuat kebijakan terkelola pelanggan AWS Identity and Access Management \(IAM\)](#) yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi lebih lanjut tentang kebijakan yang dikelola AWS, lihat [kebijakan yang dikelola AWS](#) di Panduan Pengguna IAM. Untuk daftar detail semua kebijakan AWS terkelola, lihat [panduan referensi kebijakan AWS terkelola](#).

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat [kebijakan yang dikelola AWS untuk fungsi tugas](#) di Panduan Pengguna IAM.

AWS kebijakan terkelola: `AWSTransferConsoleFullAccess`

`AWSTransferConsoleFullAccess` Kebijakan ini menyediakan akses penuh ke Transfer Family melalui Konsol AWS Manajemen. Untuk informasi selengkapnya, lihat [Service-linked peran untuk AWS Transfer Family](#).

AWS kebijakan terkelola: `AWSTransferFullAccess`

`AWSTransferFullAccess` Kebijakan ini menyediakan akses penuh ke layanan Transfer Family. Untuk informasi selengkapnya, lihat [Service-linked peran untuk AWS Transfer Family](#).

AWS kebijakan terkelola: `AWSTransferLoggingAccess`

`AWSTransferLoggingAccess` Kebijakan ini memberikan akses penuh kepada AWS Transfer Family untuk membuat aliran log dan grup serta memasukkan peristiwa log ke akun Anda. Untuk informasi selengkapnya, lihat [Service-linked peran untuk AWS Transfer Family](#).

AWS kebijakan terkelola: `AWSTransferReadOnlyAccess`

`AWSTransferReadOnlyAccess` Kebijakan ini menyediakan akses hanya-baca ke layanan Transfer Family. Untuk informasi selengkapnya, lihat [Service-linked peran untuk AWS Transfer Family](#).

AWS Transfer Family update ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk AWS Transfer Family sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman [Riwayat dokumen untuk AWS Transfer Family](#).

Perubahan	Deskripsi	Date
Pembaruan dokumentasi	Menambahkan bagian untuk setiap kebijakan yang dikelola Transfer Family.	27 Januari 2022
AWSTransferReadOnlyAccess – Pembaruan ke kebijakan yang ada	AWS Transfer Family menambahkan izin baru agar kebijakan dapat dibaca AWS Managed Microsoft AD.	30 September 2021
AWS Transfer Family mulai melacak perubahan	AWS Transfer Family mulai melacak perubahan untuk kebijakan yang AWS dikelola.	15 Juni 2021

Modul Transfer Family Terraform

[HashiCorpTerraform](#) adalah mesin Infrastructure as Code (IAC) open-source yang dikembangkan menggunakan HashiCorp Configuration Language (HCL). Terraform menyediakan alur kerja antarmuka baris perintah (CLI) yang konsisten yang, bersama dengan Transfer AWS Family untuk infrastruktur back-end, dapat mengelola ratusan layanan cloud dan mengkodefikasi API cloud menjadi file konfigurasi deklaratif.

Anda dapat menggunakan Terraform untuk menyebarkan server SFTP AWS Transfer Family dan konektor SFTP dengan aman, bersama dengan dependensi dan penyesuaian terkait. Untuk repositori yang berisi kode Terraform guna membuat sumber daya yang diperlukan untuk menjalankan AWS Transfer Family, lihat kode sumber modul Terraform [Transfer Family](#). GitHub

Note

Modul AWS Transfer Family untuk Terraform adalah upaya yang didukung komunitas. Mereka bukan bagian dari AWS layanan. Best-effort dukungan disediakan oleh komunitas AWS Storage.

Server SFTP

Otomatisasi ini memberi Anda modul Terraform yang dapat disesuaikan dan contoh ujung ke ujung untuk membuat titik akhir SFTP (atau VPC tipe PUBLIC titik akhir), berintegrasi dengan Amazon CloudWatch untuk pencatatan dan pemantauan, mengelola identitas pengguna untuk akses titik akhir, dan mengonfigurasi peran IAM untuk akses ke bucket Amazon S3 tempat file disimpan. Modul ini mendukung beberapa kunci publik SSH per pengguna (hingga 50 kunci) untuk meningkatkan keamanan dan kemampuan rotasi kunci.

Konektor SFTP

AWS Modul Transfer Family Terraform sekarang mendukung penerapan konektor SFTP untuk mentransfer file antara Amazon S3 dan server SFTP jarak jauh. Konektor SFTP menyediakan kemampuan yang dikelola sepenuhnya dan kode rendah untuk menyalin file antara Amazon S3 dan server SFTP jarak jauh.

Anda sekarang dapat menggunakan Terraform untuk menyediakan konektor SFTP, dependensi terkait, dan penyesuaian secara terprogram dalam satu penerapan. Modul ini juga menyediakan contoh ujung ke ujung untuk mengotomatiskan alur kerja transfer file berdasarkan jadwal atau pemicu peristiwa. Menggunakan Terraform untuk penerapan menghilangkan kebutuhan akan konfigurasi manual yang memakan waktu dan rawan kesalahan, dan memberi Anda opsi penerapan yang cepat, berulang, dan aman yang dapat diskalakan.

AS2

Untuk menunjukkan dukungan untuk template AS2 Terraform, tambahkan reaksi jempol (#) ke permintaan fitur template [Transfer Family Terraform](#). Anda juga dapat menambahkan komentar yang menjelaskan kasus penggunaan Anda.

Pertukaran Data B2B

AWS B2B Pertukaran Data mengotomatiskan transformasi, validasi, dan pembuatan dokumen Electronic Data Interchange (EDI) ke dan dari format data JSON dan XHTML. [Untuk menunjukkan dukungan untuk template Terraform untuk Pertukaran Data B2B, tambahkan reaksi jempol \(#\) ke permintaan fitur](#). Anda juga dapat menambahkan komentar yang menjelaskan kasus penggunaan Anda.

Pemecahan masalah AWS Transfer Family

Bab ini menyediakan informasi pemecahan masalah untuk masalah umum yang mungkin Anda temui saat menggunakan AWS Transfer Family. Setiap bagian berfokus pada area fungsionalitas tertentu untuk membantu Anda dengan cepat menemukan solusi untuk masalah Anda.

- Untuk masalah dengan IAM di Transfer Family, lihat [Pemecahan masalah AWS Transfer Family identitas dan akses](#).
- Untuk masalah dengan aplikasi web Transfer Family Anda, lihat [Memecahkan masalah aplikasi web Anda](#).

Topik

- [Memecahkan masalah otentikasi](#)
- [Memecahkan masalah konektor SFTP](#)
- [Memecahkan masalah konektivitas dan transfer SFTP](#)
- [Memecahkan masalah penyedia identitas kustom](#)
- [Memecahkan masalah alur kerja](#)
- [Memecahkan masalah EFS](#)
- [Memecahkan masalah penyimpanan dan enkripsi](#)
- [Memecahkan masalah pemantauan dan peringatan](#)
- [Memecahkan masalah transfer lintas wilayah](#)
- [Memecahkan masalah penerapan Terraform](#)
- [Memecahkan masalah integrasi Firewall Aplikasi Web](#)
- [Memecahkan masalah pengguna yang dikelola layanan](#)
- [Memecahkan masalah AS2](#)

Memecahkan masalah otentikasi

Bagian ini menjelaskan kemungkinan solusi untuk masalah otentikasi berikut.

Topik

- [Kegagalan otentikasi— SSH/SFTP](#)
- [Masalah alam tidak cocok AD terkelola](#)

- [Batas grup Active Directory terlampaui](#)
- [Masalah otentikasi lain-lain](#)
- [Memecahkan masalah Amazon API Gateway](#)
- [Memecahkan masalah pengujian penyedia identitas Anda](#)
- [Duplikat bucket Amazon S3 di aplikasi web](#)

Kegagalan otentikasi— SSH/SFTP

Deskripsi

Ketika Anda mencoba untuk terhubung ke server Anda menggunakan Secure Shell (SSH) File Transfer Protocol (SFTP), Anda menerima pesan yang mirip dengan berikut ini:

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

Jika Anda menggunakan API Gateway dan menerima kesalahan ini, lihat [Terlalu banyak kegagalan otentikasi](#).

Menyebabkan

Anda belum menambahkan key pair RSA untuk pengguna Anda, jadi Anda harus mengautentikasi menggunakan kata sandi sebagai gantinya.

Solusi

Saat Anda menjalankan sftp perintah, tentukan -o PubkeyAuthentication=no opsi. Opsi ini memaksa sistem untuk meminta kata sandi Anda. Contoh:

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

Masalah alam tidak cocok AD terkelola

Deskripsi

Ranah pengguna dan ranah grup mereka harus cocok. Mereka berdua harus berada di ranah default, atau keduanya harus berada di ranah tepercaya.

Menyebabkan

Jika pengguna dan grup mereka tidak cocok, pengguna tidak dapat diautentikasi oleh Transfer Family. Jika Anda menguji penyedia identitas untuk pengguna, Anda menerima kesalahan Tidak ada akses terkait yang ditemukan untuk grup pengguna.

Solusi

Referensikan grup di ranah pengguna yang cocok dengan ranah grup (baik default atau tepercaya).

Batas grup Active Directory terlampaui

Deskripsi

Saat mencoba menambahkan lebih banyak grup Direktori Aktif ke AWS Transfer Family server Anda, Anda menerima kesalahan yang menunjukkan bahwa Anda telah mencapai jumlah grup maksimum yang diizinkan.

Menyebabkan

AWS Transfer Family memiliki batas default 100 grup Active Directory per server.

Solusi

Ini adalah dua solusi yang mungkin:

- Konsolidasikan grup Active Directory Anda untuk mengurangi jumlah total yang dibutuhkan.
- Jika kasus penggunaan Anda memerlukan lebih dari 100 grup, pertimbangkan untuk menggunakan solusi penyedia identitas kustom seperti yang dijelaskan dalam [Simplify Active Directory autentikasi dengan penyedia identitas kustom untuk](#). AWS Transfer Family

Masalah otentikasi lain-lain

Deskripsi

Anda menerima kesalahan otentikasi dan tidak ada pemecahan masalah lainnya yang berfungsi

Menyebabkan

Anda mungkin telah menentukan target untuk direktori logis yang berisi garis miring (/) di depan atau belakang.

Solusi

Perbarui target direktori logis Anda, untuk memastikannya dimulai dengan garis miring, dan tidak berisi garis miring. Misalnya, dapat /amzn-s3-demo-bucket/images diterima, tetapi amzn-s3-demo-bucket/images dan /amzn-s3-demo-bucket/images/ tidak.

Memecahkan masalah Amazon API Gateway

Bagian ini menjelaskan kemungkinan solusi untuk masalah API Gateway berikut.

Topik

- [Terlalu banyak kegagalan otentikasi](#)
- [Koneksi ditutup](#)

Terlalu banyak kegagalan otentikasi

Deskripsi

Ketika Anda mencoba untuk terhubung ke server Anda menggunakan Secure Shell (SSH) File Transfer Protocol (SFTP), Anda mendapatkan kesalahan berikut:

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

Menyebabkan

Anda mungkin telah memasukkan kata sandi yang salah untuk pengguna Anda. Coba lagi untuk memasukkan kata sandi yang benar.

Jika kata sandi sudah benar, masalah mungkin disebabkan oleh peran Amazon Resource Name (ARN) yang tidak valid. Untuk mengonfirmasi bahwa ini masalahnya, uji penyedia identitas untuk server Anda. Jika Anda melihat respons yang mirip dengan berikut ini, ARN peran hanya merupakan placeholder, seperti yang ditunjukkan oleh nilai ID peran dari semua nol:

```
{
```

```
"Response": "{\n  \"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",\n  \"HomeDirectory\": \"\\\"/\\\"\",\n  \"StatusCode\": 200,\n  \"Message\": \"\",\n  \"Url\": \"https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/servers/transfer-server-ID/users/myuser/config\"\n}
```

Solusi

Ganti peran placeholder ARN dengan peran aktual yang memiliki izin untuk mengakses server.

Untuk memperbarui peran

1. Buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Di panel navigasi sebelah kiri, pilih Tumpukan.
3. Dalam daftar Stacks, pilih tumpukan Anda, lalu pilih tab Parameter.
4. Pilih Perbarui. Pada halaman Update stack, pilih Use current template, lalu pilih Next.
5. Ganti UserRoleArn dengan ARN peran yang memiliki izin yang cukup untuk mengakses server Transfer Family Anda.

Note

Untuk memberikan izin yang diperlukan, Anda dapat menambahkan AmazonAPIGatewayAdministrator dan kebijakan AmazonS3FullAccess terkelola ke peran Anda.

6. Pilih Berikutnya, lalu pilih Berikutnya lagi. Pada *stack* halaman Tinjauan, pilih Saya mengakui yang AWS CloudFormation mungkin membuat sumber daya IAM, lalu pilih Perbarui tumpukan.

Koneksi ditutup

Deskripsi

Ketika Anda mencoba untuk terhubung ke server Anda menggunakan Secure Shell (SSH) File Transfer Protocol (SFTP), Anda mendapatkan kesalahan berikut:

```
Connection closed
```

Menyebabkan

Salah satu kemungkinan penyebab masalah ini adalah bahwa peran CloudWatch pencatatan Amazon Anda tidak memiliki hubungan kepercayaan dengan Transfer Family.

Solusi

Pastikan bahwa peran logging untuk server memiliki hubungan kepercayaan dengan Transfer Family. Untuk informasi selengkapnya, lihat [Untuk membangun hubungan kepercayaan](#).

Memecahkan masalah pengujian penyedia identitas Anda

Deskripsi

Jika Anda menguji penyedia identitas menggunakan konsol atau operasi `TestIdentityProvider` API, Response bidang tersebut kosong. Contoh:

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

Menyebabkan

Penyebab yang paling mungkin adalah otentikasi gagal karena nama pengguna atau kata sandi yang salah.

Solusi

Pastikan Anda menggunakan kredensi yang benar untuk pengguna Anda, dan buat pembaruan pada nama pengguna atau kata sandi, jika perlu.

Duplikat bucket Amazon S3 di aplikasi web

Deskripsi

Bucket Amazon S3 yang sama muncul beberapa kali di antarmuka aplikasi web Transfer Family.

Menyebabkan

Ini terjadi ketika pengguna termasuk dalam beberapa grup Direktori Aktif yang memiliki hibah ke bucket Amazon S3 yang sama. Aplikasi web mencantumkan semua hibah tingkat atas yang terkait dengan UID atau GID pengguna, termasuk hibah duplikat ke lokasi bucket yang sama.

Solusi

Untuk mencegah daftar duplikat, konsolidasikan hibah sehingga setiap pengguna hanya memiliki satu hibah per lokasi Amazon S3. Tinjau konfigurasi Amazon S3 Access Grants dan hapus hibah redundan untuk bucket yang sama di berbagai grup Active Directory.

Memecahkan masalah konektor SFTP

Bagian ini menjelaskan kemungkinan solusi untuk masalah dengan konektor SFTP.

Topik

- [Memecahkan masalah menambahkan kunci host tepercaya untuk konektor SFTP Anda](#)
- [Negosiasi kunci gagal](#)
- [Pelambatan konektor SFTP](#)
- [Mengoptimalkan kinerja konektor SFTP](#)
- [Memecahkan masalah konektivitas VPC](#)
- [Masalah konektor SFTP lain-lain](#)

Memecahkan masalah menambahkan kunci host tepercaya untuk konektor SFTP Anda

Deskripsi

Saat Anda membuat atau mengedit konektor SFTP, dan Anda menambahkan kunci host tepercaya, Anda menerima kesalahan berikut: `Failed to edit connector details (Invalid host key format.)`

Menyebabkan

Jika Anda menempelkan kunci publik yang benar, masalahnya mungkin Anda memasukkan comment bagian kunci tersebut. AWS Transfer Family saat ini tidak menerima bagian komentar dari kunci.

Solusi

Hapus bagian komentar dari kunci, saat Anda menempelkannya ke bidang teks. Misalnya, anggap kunci Anda terlihat mirip dengan yang berikut ini:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Hapus teks yang mengikuti == karakter dan hanya tempel di bagian tombol hingga dan termasuk==.

```
ssh-rsa AAAA...==
```

Negosiasi kunci gagal

Deskripsi

Anda menerima kesalahan di mana negosiasi pertukaran kunci gagal. Contoh:

```
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]
```

Menyebabkan

Kesalahan ini karena tidak ada tumpang tindih antara algoritma kunci host yang didukung oleh server dan yang didukung oleh konektor.

Solusi

Pastikan server jarak jauh mendukung setidaknya satu dari algoritma kunci host Klien yang tercantum dalam pesan kesalahan. Untuk daftar algoritma yang didukung, lihat [Kebijakan keamanan untuk AWS Transfer Family Konektor SFTP](#).

Pelambatan konektor SFTP

Deskripsi

Saat menggunakan konektor SFTP untuk transfer file, Anda mengalami kesalahan seperti:

```
{"type":"ExecutionThrottled","details":{},"connectorId":"c-1234567890abcdef0"}
```

Atau Anda melihat bahwa transfer file sedang tertunda atau gagal sebentar-sebentar selama operasi volume tinggi.

Menyebabkan

Konektor SFTP memiliki kuota layanan yang membatasi jumlah transfer file bersamaan dan operasi API. Ketika batas ini terlampaui, pembatasan terjadi untuk melindungi layanan dan memastikan penggunaan yang adil di semua pelanggan.

Solusi

Untuk mengatasi masalah konektor SFTP, coba solusi berikut:

1. Terapkan backoff eksponensial dan coba lagi logika dalam aplikasi Anda. Misalnya, buat fungsi yang secara otomatis mencoba ulang operasi yang gagal dengan waktu tunggu yang meningkat di antara upaya.
2. Menerapkan pembatasan tarif dalam aplikasi Anda:
 - Batasi jumlah transfer bersamaan.
 - Tambahkan penundaan antara batch transfer.
3. Pantau penggunaan Anda terhadap kuota layanan:
 - Gunakan CloudWatch metrik untuk melacak penggunaan API.
 - Siapkan alarm untuk memberi tahu Anda saat mendekati batas kuota.
4. Untuk opsi untuk menskalakan konektor SFTP Anda, lihat [Menskalakan konektor SFTP Anda](#)
5. Jika pembatasan berlanjut dan berdampak pada operasi bisnis Anda, mintalah peningkatan kuota melalui konsol Service Quotas.

Mengoptimalkan kinerja konektor SFTP

Deskripsi

Transfer konektor SFTP Anda lebih lambat dari yang diharapkan atau Anda mengalami kinerja yang tidak konsisten.

Menyebabkan

Kinerja konektor SFTP dapat dipengaruhi oleh berbagai faktor termasuk kondisi jaringan, ukuran file, konfigurasi server jarak jauh, dan batas transfer bersamaan.

Solusi

Untuk mengoptimalkan kinerja konektor SFTP:

- Konfigurasi server SFTP jarak jauh Anda untuk kinerja optimal:
 - Tingkatkan sesi maksimum dan transfer per sesi
 - Optimalkan ukuran jendela TCP untuk koneksi latensi tinggi
 - Gunakan kompresi jika didukung oleh kedua ujungnya
- Pertimbangkan pengoptimalan jaringan, dengan menempatkan konektor Transfer Family Anda di wilayah yang dekat dengan server SFTP jarak jauh Anda.
- Menerapkan strategi pemantauan untuk mengidentifikasi kemacetan kinerja:
 - Pantau throughput dan latensi jaringan
 - Menganalisis log untuk pola dalam transfer lambat

Memecahkan masalah konektivitas VPC

Bagian ini menjelaskan solusi untuk masalah umum dengan konektor VPC_ LATTICE-enabled SFTP.

Konektor terjebak dalam status PENDING

Deskripsi

Konektor VPC_ LATTICE-enabled SFTP Anda tetap dalam PENDING status untuk waktu yang lama (lebih dari 10 menit).

Menyebabkan

Hal ini dapat terjadi karena penundaan resolusi DNS, masalah konfigurasi Resource Gateway, atau masalah asosiasi jaringan layanan VPC Lattice.

Solusi

[Hubungi AWS Dukungan di Contact AWS](#) untuk membantu menganalisis akar penyebab masalah. Anda juga dapat mencoba solusi berikut.

1. Verifikasi bahwa Resource Gateway Anda dalam ACTIVE status:

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifier rgw-1234567890abcdef0
```

2. Periksa apakah Konfigurasi Sumber Daya Anda dikonfigurasi dan aktif dengan benar:

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifier rcfg-1234567890abcdef0
```

3. Pastikan Resource Gateway Anda memiliki subnet di setidaknya dua Availability Zone yang mendukung VPC Lattice.
4. Jika masalah berlanjut, hapus dan buat ulang konektor dengan konfigurasi yang sama.

Konektor dalam status ERRORED

Deskripsi

Konektor VPC_ LATTICE-enabled SFTP Anda menunjukkan ERRORED status dengan detail kesalahan.

Menyebabkan

Penyebab umum termasuk ARN Konfigurasi Sumber Daya yang tidak valid, alamat IP yang tidak mencukupi dalam subnet VPC, atau upaya berbagi sumber daya lintas wilayah.

Solusi

1. Periksa detail kesalahan menggunakandescrcribe-connector:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Verifikasi ARN Konfigurasi Sumber Daya sudah benar dan berada di wilayah yang sama dengan konektor Anda.
3. Pastikan subnet VPC Anda memiliki alamat IP yang cukup tersedia untuk Resource Gateway.
4. Periksa apakah target Konfigurasi Sumber Daya Anda (alamat IP atau nama DNS) dapat dijangkau dari VPC Anda.

Alamat IP publik tidak didukung kesalahan

Deskripsi

Anda menerima kesalahan saat mencoba membuat Konfigurasi Sumber Daya dengan alamat IP publik: `ValidationException: IP address x.x.x.x is not in allowed ranges.`

Menyebabkan

Konfigurasi Sumber Daya untuk titik akhir publik harus menggunakan nama DNS, bukan alamat IP.

Solusi

Gunakan nama DNS publik server SFTP Anda alih-alih alamat IP-nya saat membuat Konfigurasi Sumber Daya:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \  
  --port-ranges 22
```

Kesalahan Availability Zone tidak didukung

Deskripsi

Anda menerima kesalahan saat membuat Resource Gateway: Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.

Menyebabkan

Tidak semua Availability Zone mendukung VPC Lattice Cross-VPC Resource Access. Pesan galat mencantumkan AZ yang didukung untuk wilayah Anda.

Solusi

1. Buat subnet di Availability Zone yang didukung yang tercantum dalam pesan galat.
2. Perbarui Resource Gateway Anda untuk menggunakan subnet dari AZ yang didukung saja.
3. Pastikan Anda memiliki setidaknya dua subnet di AZ yang didukung berbeda.

Batas waktu koneksi dengan konektor VPC_LATTICE

Deskripsi

Transfer file melalui konektor VPC habis waktu atau gagal sebentar-sebentar.

Menyebabkan

VPC Lattice memiliki batas koneksi (350 koneksi per sumber daya) dan batas waktu idle (350 detik untuk TCP).

Solusi

1. Pantau koneksi bersamaan agar tetap berada dalam batas koneksi 350 per sumber daya.
2. Terapkan penyatuan koneksi dan gunakan kembali dalam aplikasi Anda.
3. Konfigurasi nilai batas waktu yang sesuai dalam aplikasi klien SFTP Anda (kurang dari 350 detik).
4. Pertimbangkan untuk membuat beberapa Konfigurasi Sumber Daya untuk target yang sama untuk mendistribusikan beban.

Masalah konektor SFTP lain-lain

Deskripsi

Anda menerima kesalahan setelah menjalankan `StartFileTransfer`, tetapi tidak tahu penyebab masalahnya, dan hanya ID konektor yang dikembalikan setelah panggilan API.

Menyebabkan

Kesalahan ini dapat memiliki beberapa penyebab. Untuk memecahkan masalah, kami sarankan Anda menguji konektor Anda dan mencari log Anda CloudWatch .

Solusi

- Uji konektor Anda: Lihat [Uji konektor SFTP](#). Jika tes gagal, sistem memberikan pesan kesalahan berdasarkan alasan pengujian gagal. Bagian itu menjelaskan cara menguji konektor Anda baik dari konsol atau dengan menggunakan perintah [TestConnectionAPI](#).
- Lihat CloudWatch log untuk konektor Anda: Lihat [Contoh entri log untuk konektor SFTP](#). Topik ini memberikan contoh untuk entri log konektor SFTP, dan konvensi penamaan untuk membantu Anda menemukan log yang sesuai.

Memecahkan masalah konektivitas dan transfer SFTP

Bagian ini menjelaskan kemungkinan solusi untuk konektivitas SFTP dan masalah transfer file.

Topik

- [Memecahkan masalah konektivitas SFTP](#)
- [Memecahkan masalah klien SFTP](#)

- [Memecahkan masalah pengunggahan file](#)
- [Memecahkan masalah konektor SFTP tipe jalan keluar VPC](#)

Memecahkan masalah konektivitas SFTP

Deskripsi

Klien SFTP Anda tidak dapat memulai koneksi. Masalah ini dapat terjadi terus menerus atau sebentar-sebentar. Misalnya, Anda mungkin melihat urutan kejadian berikut di log debug klien SFTP Anda:

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Menyebabkan

Ada kasus tepi di mana Zero-byte TCP ACK (ACK tanpa data), juga dikenal sebagai jabat tangan tiga arah, dijatuhkan atau ditunda.

Solusi

Sebagai solusinya, Transfer Family menawarkan solusi yang menggunakan konfigurasi berbeda untuk mengatasi masalah ini, tetapi dapat menyebabkan masalah kompatibilitas dengan klien lama. Untuk alasan itu, solusi ini hanya tersedia di port 2223.

Dalam prosedur untuk membuat server Transfer Family di VPC ([Buat server di cloud pribadi virtual](#)), ketika Anda menentukan grup keamanan, konfigurasikan lalu lintas SSH untuk menggunakan port 2223.

Memecahkan masalah klien SFTP

Pesan sisi klien SFTP dijelaskan dalam [Pesan SFTP](#). Cara terbaik untuk memecahkan masalah klien SFTP adalah dengan memeriksa log klien SFTP dan, jika perlu, hubungi administrator jaringan Anda.

Memecahkan masalah pengunggahan file

Bagian ini menjelaskan kemungkinan solusi untuk masalah unggahan file berikut.

Topik

- [Memecahkan masalah kesalahan unggahan file Amazon S3](#)
- [Memecahkan masalah nama file yang tidak dapat dibaca](#)

Memecahkan masalah kesalahan unggahan file Amazon S3

Deskripsi

Saat Anda mencoba mengunggah file ke penyimpanan Amazon S3 menggunakan Transfer Family, Anda menerima pesan galat berikut AWS : Transfer tidak mendukung penulisan akses acak ke objek S3.

Menyebabkan

Saat Anda menggunakan Amazon S3 untuk penyimpanan server Anda, Transfer Family tidak mendukung beberapa koneksi untuk satu transfer.

Solusi

Jika server Transfer Family Anda menggunakan Amazon S3 untuk penyimpanannya, nonaktifkan opsi apa pun untuk perangkat lunak klien Anda yang menyebutkan menggunakan beberapa koneksi untuk satu transfer.

Memecahkan masalah nama file yang tidak dapat dibaca

Deskripsi

Anda melihat nama file rusak di beberapa file yang Anda unggah. Pengguna terkadang mengalami masalah dengan transfer FTP dan SFTP yang mengacaukan karakter tertentu dalam nama file, seperti umlauts, huruf beraksen, atau skrip tertentu, seperti bahasa Mandarin atau Arab.

Menyebabkan

Meskipun protokol FTP dan SFTP dapat memungkinkan pengkodean karakter nama file dinegosiasikan oleh klien, Amazon S3 dan Amazon EFS tidak. Sebaliknya, mereka membutuhkan pengkodean UTF-8 karakter. Akibatnya, karakter tertentu tidak ditampilkan dengan benar.

Solusi

Untuk mengatasi masalah ini, tinjau aplikasi klien Anda untuk pengkodean karakter nama file dan pastikan sudah diatur ke UTF-8.

Memecahkan masalah konektor SFTP tipe jalan keluar VPC

Jika Anda mengalami masalah dengan konektor SFTP tipe jalan keluar VPC, periksa hal berikut:

Status konektor TERTUNDA

Deskripsi

Konektor tipe jalan keluar VPC Anda tetap dalam status PENDING selama beberapa menit setelah pembuatan, dan TestConnection mengembalikan “Konektor tidak tersedia”.

Menyebabkan

Resolusi DNS untuk konektor VPC dapat memakan waktu beberapa menit untuk diselesaikan setelah pembuatan.

Solusi

Tunggu status konektor menjadi AKTIF sebelum mencoba transfer file. Ini adalah perilaku normal untuk konektor tipe jalan keluar VPC.

Batas waktu koneksi

Deskripsi

Konektor tipe jalan keluar VPC Anda habis saat mencoba terhubung ke server SFTP.

Menyebabkan

Grup keamanan mungkin tidak mengizinkan lalu lintas pada port 22 antara subnet Resource Gateway Anda dan server SFTP target.

Solusi

Verifikasi bahwa grup keamanan mengizinkan lalu lintas pada port 22 antara subnet Resource Gateway Anda dan server SFTP target.

Kesalahan Konfigurasi Sumber Daya

Deskripsi

Konektor tipe jalan keluar VPC Anda gagal terhubung karena masalah Konfigurasi Sumber Daya.

Menyebabkan

Konfigurasi Sumber Daya dapat menunjuk ke alamat IP atau nama DNS yang salah, atau Resource Gateway mungkin tidak berada di VPC yang sama dengan server SFTP Anda (untuk titik akhir pribadi).

Solusi

Pastikan Konfigurasi Sumber Daya menunjuk ke alamat IP atau nama DNS yang benar, dan Resource Gateway berada di VPC yang sama dengan server SFTP Anda (untuk titik akhir pribadi). Untuk informasi selengkapnya, lihat [Konfigurasi sumber daya](#) di Panduan Pengguna Amazon VPC Lattice.

Masalah titik akhir publik

Deskripsi

Konektor tipe jalan keluar VPC Anda tidak dapat terhubung ke titik akhir SFTP publik.

Menyebabkan

Untuk titik akhir publik, Anda harus menggunakan nama DNS (bukan alamat IP) dalam Konfigurasi Sumber Daya Anda, dan VPC Anda harus memiliki NAT Gateway untuk akses internet keluar.

Solusi

Pastikan Anda menggunakan nama DNS, bukan alamat IP, dalam Konfigurasi Sumber Daya Anda. Verifikasi bahwa VPC Anda memiliki NAT Gateway untuk akses internet keluar.

Masalah Availability Zone

Deskripsi

Anda tidak dapat membuat Resource Gateway karena keterbatasan Availability Zone.

Menyebabkan

Resource Gateways memerlukan subnet di setidaknya 2 Availability Zone, dan tidak semua AZ mendukung VPC Lattice.

Solusi

Periksa Availability Zone yang didukung untuk VPC Lattice di wilayah Anda dan pastikan Anda memiliki subnet di setidaknya 2 AZ yang didukung.

Memecahkan masalah penyedia identitas kustom

Bagian ini menjelaskan kemungkinan solusi untuk masalah yang terkait dengan penyedia identitas kustom dengan Transfer Family.

Topik

- [Memecahkan masalah kesalahan integrasi API Gateway](#)
- [Memecahkan masalah batas waktu fungsi Lambda](#)
- [Memecahkan masalah batas waktu Lambda yang konsisten](#)
- [Memecahkan masalah pengecualian KeyError](#)

Memecahkan masalah kesalahan integrasi API Gateway

Deskripsi

Pengguna tidak dapat melakukan autentikasi dengan server Transfer Family Anda, dan saat menguji penyedia identitas Anda, Anda akan melihat kesalahan seperti:

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Menyebabkan

Kesalahan integrasi API Gateway dapat terjadi karena:

- Konfigurasi API Gateway salah
- Kesalahan fungsi Lambda tidak ditangani dengan benar
- Masalah izin antara API Gateway dan Lambda
- Tanggapan cacat dari fungsi Lambda

Solusi

Untuk memecahkan masalah kesalahan integrasi API Gateway:

1. Periksa log fungsi Lambda Anda untuk informasi kesalahan terperinci:
 - Di CloudWatch konsol, navigasikan ke Grup log `>/aws/lambda/your-function-name`
 - Cari pesan kesalahan atau jejak tumpukan yang menunjukkan akar penyebabnya
2. Verifikasi bahwa fungsi Lambda Anda mengembalikan respons yang diformat dengan benar:

```
{  
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",  
  "HomeDirectory": "/mybucket/home/username"  
}
```

3. Aktifkan CloudWatch pencatatan terperinci untuk API Gateway:
 - Di konsol API Gateway, pilih API Anda dan pilih Tahapan
 - Pilih panggung Anda dan di bawahnya Logs/Tracing, aktifkan CloudWatch Log
 - Atur level log ke ERROR atau INFO
4. Uji titik akhir API Gateway Anda secara langsung:

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-server-id/users/username/config \  
  -H "Content-Type: application/json" \  
  -d '{"Password": "password"}'
```

5. Verifikasi izin antara API Gateway dan Lambda:
 - Pastikan API Gateway memiliki izin untuk menjalankan fungsi Lambda Anda
 - Periksa apakah peran eksekusi untuk fungsi Lambda Anda memiliki izin yang diperlukan

Memecahkan masalah batas waktu fungsi Lambda

Deskripsi

Saat pengguna mencoba mengautentikasi dengan server Transfer Family Anda menggunakan penyedia identitas khusus, mereka mengalami penundaan yang lama diikuti oleh kegagalan otentikasi. Di log Lambda Anda, Anda melihat kesalahan batas waktu.

Menyebabkan

Fungsi Lambda yang digunakan untuk penyedia identitas kustom memiliki batas waktu default 3 detik. Jika logika otentikasi Anda membutuhkan waktu lebih lama dari batas waktu ini (misalnya, saat

menanyakan database eksternal atau melakukan panggilan API ke penyedia identitas pihak ketiga), fungsi akan habis waktu dan otentikasi akan gagal.

Solusi

Untuk mengatasi masalah batas waktu Lambda:

1. Tingkatkan batas waktu fungsi Lambda:

- Di konsol Lambda, navigasikan ke fungsi Anda dan pilih tab Konfigurasi
- Di bawah Konfigurasi umum, klik Edit
- Tingkatkan nilai batas waktu (disarankan hingga 15 detik untuk fungsi otentikasi)

2. Optimalkan kode fungsi Lambda Anda:

- Gunakan penyatuan koneksi untuk kueri basis data
- Menerapkan caching untuk data yang sering diakses
- Minimalkan panggilan API eksternal selama otentikasi

3. Pertimbangkan untuk menggunakan Lambda Provisioned Concurrency untuk menghilangkan cold start:

```
aws lambda put-provisioned-concurrency-config \
  --function-name my-authentication-function \
  --qualifier prod \
  --provisioned-concurrent-executions 5
```

4. Pantau kinerja Lambda menggunakan CloudWatch metrik dan atur alarm untuk ambang batas durasi

Memecahkan masalah batas waktu Lambda yang konsisten

Deskripsi

Pengguna mengalami batas waktu yang konsisten saat menggunakan fungsi Lambda untuk otentikasi.

Menyebabkan

Lambda tidak dapat menjangkau AWS layanan terkait yang digunakan untuk mengautentikasi (seperti DynamoDB, Secrets Manager, atau penyedia identitas lainnya).

Solusi

Verifikasi bahwa subnet dapat menjangkau AWS layanan. Atau, jika terhubung ke penyedia identitas internet (seperti Okta), verifikasi bahwa subnet fungsi Lambda dapat menjangkau internet melalui Gateway NAT

Memecahkan masalah pengecualian **KeyError**

Deskripsi

Dalam entri log Transfer Family Anda, Anda melihat pengecualian `KeyError` ".

Menyebabkan

Penyebab yang paling mungkin adalah bahwa pengguna atau `identity_provider` catatan salah bentuk atau kehilangan bidang wajib.

Solusi

Tinjau `ERRORS` log, yang terletak di grup `/aws/transfer/your-server-id` log untuk petunjuk.

Memecahkan masalah alur kerja

Bagian ini menjelaskan kemungkinan solusi untuk masalah dengan alur kerja terkelola.

Topik

- [Memecahkan masalah alur kerja terkelola](#)
- [Memecahkan masalah dekripsi alur kerja](#)

Memecahkan masalah alur kerja terkelola

Bagian ini menjelaskan kemungkinan solusi untuk masalah alur kerja berikut.

Topik

- [Memecahkan masalah kesalahan terkait alur kerja menggunakan Amazon CloudWatch](#)
- [Memecahkan masalah kesalahan penyalinan alur kerja](#)

Memecahkan masalah kesalahan terkait alur kerja menggunakan Amazon CloudWatch

Deskripsi

Jika Anda mengalami masalah dengan alur kerja Anda, Anda dapat menggunakan Amazon CloudWatch untuk menyelidiki penyebabnya.

Menyebabkan

Mungkin ada beberapa penyebab. Gunakan Amazon CloudWatch Logs untuk menyelidiki.

Solusi

Transfer Family memancarkan status eksekusi alur kerja ke dalam CloudWatch Log. Jenis kesalahan alur kerja berikut dapat muncul di CloudWatch Log:

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

Anda dapat memfilter log eksekusi alur kerja Anda menggunakan sintaks filter dan pola yang berbeda. Misalnya, Anda dapat membuat filter log di CloudWatch log Anda untuk menangkap log eksekusi alur kerja yang berisi ExecutionErrored pesan. Untuk detailnya, lihat [Real-time pemrosesan data log dengan langganan](#) dan [Filter dan sintaks pola](#) di Panduan Pengguna Amazon CloudWatch Logs.

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"}
```

Di sini, StepErrored menunjukkan bahwa langkah dalam alur kerja telah menghasilkan kesalahan. Dalam satu alur kerja, Anda dapat memiliki beberapa langkah yang dikonfigurasi. Kesalahan ini memberi tahu Anda di langkah mana kesalahan terjadi dan memberikan pesan kesalahan. Dalam contoh khusus ini, langkah dikonfigurasi untuk menandai file; Namun, menandai file dalam sistem file Amazon EFS tidak didukung, sehingga langkah tersebut menghasilkan kesalahan.

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"}}
```

Ketika alur kerja tidak dapat mengeksekusi langkah apa pun, itu menghasilkan `ExecutionErrored` pesan. Misalnya, jika Anda telah mengonfigurasi satu langkah dalam alur kerja tertentu, dan jika langkah tersebut tidak dapat dijalankan, alur kerja keseluruhan gagal.

EksekusiTerhambat

Eksekusi dibatasi jika alur kerja dipicu pada tingkat yang lebih cepat daripada yang dapat didukung sistem. Pesan log ini menunjukkan bahwa Anda harus memperlambat laju eksekusi untuk alur kerja.

[Jika Anda tidak dapat menurunkan tingkat eksekusi alur kerja Anda, hubungi AWS Dukungan di Kontak. AWS](#)

Kegagalan layanan saat memulai alur kerja

Setiap kali Anda menghapus alur kerja dari server dan menggantinya dengan yang baru, atau memperbarui konfigurasi server (yang memengaruhi peran eksekusi alur kerja), Anda harus menunggu sekitar 10 menit sebelum menjalankan alur kerja baru. Server Transfer Family menyimpan cache detail alur kerja, dan dibutuhkan waktu 10 menit bagi server untuk menyegarkan cache-nya.

Selain itu, Anda harus keluar dari sesi SFTP aktif apa pun, dan kemudian masuk kembali setelah masa tunggu 10 menit untuk melihat perubahannya.

Memecahkan masalah kesalahan penyalinan alur kerja

Deskripsi

Jika Anda menjalankan alur kerja yang berisi langkah untuk menyalin file yang diunggah, Anda dapat mengalami kesalahan berikut:

```
{
  "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"
}
}
```

Menyebabkan

File sumber ada di bucket Amazon S3 yang berbeda Wilayah AWS dari bucket tujuan.

Solusi

Jika Anda menjalankan alur kerja yang menyertakan langkah penyalinan, pastikan bucket sumber dan tujuan berada di tempat yang sama. Wilayah AWS

Memecahkan masalah dekripsi alur kerja

Bagian ini menjelaskan kemungkinan solusi untuk masalah berikut dengan alur kerja terenkripsi.

Topik

- [Memecahkan masalah enkripsi penerima anonim](#)
- [Memecahkan masalah kesalahan untuk file enkripsi yang ditandatangani](#)
- [Memecahkan masalah kesalahan untuk algoritma FIPS](#)

Memecahkan masalah enkripsi penerima anonim

Deskripsi

Alur kerja dekripsi Anda gagal saat memproses file terenkripsi tertentu, tetapi berfungsi dengan yang lain.

Menyebabkan

File mungkin telah dienkrpsi tanpa menentukan penerima (enkripsi anonim), sehingga sulit bagi alur kerja untuk menentukan kunci mana yang akan digunakan untuk dekripsi.

Solusi

Selalu enkripsi file dengan penerima non-anonim menggunakan parameter. -r Contoh:

```
gpg -e -r user@example.com --openpgp file.txt
```

Untuk memeriksa apakah file dienkripsi dengan penerima tertentu atau secara anonim, gunakan perintah: `--list-packets`

```
gpg --list-packets file.txt.gpg
```

Perintah ini menampilkan struktur paket GPG-encrypted file tanpa mendekripsi isinya. Cari output yang mencakup informasi penerima, seperti:

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Jika Anda melihat informasi keyid, file tersebut dienkripsi untuk penerima tertentu. Jika informasi ini hilang, file mungkin telah dienkripsi secara anonim, yang dapat menyebabkan kegagalan dekripsi dalam alur kerja Transfer Family.

Anda juga dapat menggunakan perintah ini untuk memverifikasi:

- Algoritma enkripsi mana yang digunakan
- Metode kompresi (jika ada)
- Stempel waktu pembuatan

Untuk melihat daftar algoritma cipher yang didukung untuk instalasi GPG Anda, gunakan:

```
gpg --version
```

Informasi ini dapat membantu Anda memastikan bahwa Anda menggunakan algoritme enkripsi yang kompatibel dengan alur kerja Transfer Family, terutama ketika kepatuhan FIPS diperlukan.

Memecahkan masalah kesalahan untuk file enkripsi yang ditandatangani

Deskripsi

Alur kerja dekripsi Anda gagal dan Anda menerima kesalahan berikut:

```
"Encrypted file with signed message unsupported"
```

Menyebabkan

Transfer Family saat ini tidak mendukung penandatanganan untuk file terenkripsi.

Solusi

Di klien PGP Anda, jika ada opsi untuk menandatangani file terenkripsi, pastikan untuk menghapus pilihan, karena Transfer Family saat ini tidak mendukung penandatanganan untuk file terenkripsi.

Memecahkan masalah kesalahan untuk algoritma FIPS

Deskripsi

Alur kerja dekripsi Anda gagal, dan pesan log menyerupai berikut ini:

```
{
  "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"
  }
}
```

Menyebabkan

Server Transfer Family Anda mengaktifkan mode FIPS dan langkah alur kerja Dekripsi terkait. Saat mengenkripsi file sebelum mengunggah ke server Transfer Family Anda, klien enkripsi mungkin menghasilkan file terenkripsi yang menggunakan algoritme enkripsi simetris yang disetujui non-FIPS. Dalam skenario seperti itu, alur kerja tidak dapat mendekripsi file. Dalam contoh berikut, GnuPG versi 2.4.0 menggunakan OCB (mode sandi blok non-FIPS) untuk mengenkripsi file: ini menyebabkan alur kerja gagal.

Solusi

Anda harus mengedit kunci GPG yang Anda gunakan untuk mengenkripsi file Anda, dan kemudian mengenkripsi ulang mereka. Prosedur berikut menjelaskan langkah-langkah yang harus Anda ambil.

Untuk mengedit kunci PGP

1. Identifikasi kunci yang harus Anda edit dengan menjalankan `gpg --list-keys`

Ini mengembalikan daftar kunci. Setiap kunci memiliki detail yang mirip dengan yang berikut ini:

```
pub   ed25519 2022-07-07 [SC]
       wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
uid           [ultimate] Mary Major <marymajor@example.com>
sub   cv25519 2022-07-07 [E]
```

2. Identifikasi kunci yang ingin Anda edit. Pada contoh yang ditunjukkan pada langkah sebelumnya, ID adalah `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
3. Jalankan `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Sistem merespons dengan detail tentang program GnuPG dan kunci yang ditentukan.

4. Pada `gpg>` prompt, masukkan `showpref`. Rincian berikut dikembalikan:

```
[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
```

Perhatikan bahwa algoritma pilihan yang disimpan pada kunci terdaftar.

5. Kami ingin mengedit kunci untuk mempertahankan semua algoritma kecuali untuk OCB. Jalankan `setpref` perintah, tentukan semua algoritma untuk mempertahankan:

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
  BZIP2, ZIP, Uncompressed
```

Ini mengembalikan rincian berikut:

```
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. Masukkan y untuk memperbarui, lalu masukkan kata sandi Anda saat diminta untuk mengonfirmasi perubahan.
7. Simpan perubahan.

```
gpg> save
```

Sebelum menjalankan kembali alur kerja dekripsi Anda, Anda harus mengenkripsi ulang file Anda, menggunakan kunci yang diedit.

Memecahkan masalah EFS

Bagian ini menjelaskan kemungkinan solusi untuk masalah penyimpanan Amazon EFS.

Topik

- [Memecahkan masalah Amazon EFS](#)

Memecahkan masalah Amazon EFS

Bagian ini menjelaskan kemungkinan solusi untuk masalah Amazon EFS berikut.

Topik

- [Memecahkan masalah pengguna yang dikelola layanan Amazon EFS](#)
- [Memecahkan masalah profil POSIX yang hilang](#)
- [Memecahkan masalah direktori logis dengan Amazon EFS](#)

Memecahkan masalah pengguna yang dikelola layanan Amazon EFS

Deskripsi

Anda menjalankan `sftp` perintah dan prompt tidak muncul, dan sebagai gantinya Anda melihat pesan berikut:

```
Couldn't canonicalize: Permission denied
Need cwd
```

Menyebabkan

Peran pengguna AWS Identity and Access Management (IAM) Anda tidak memiliki izin untuk mengakses Amazon Elastic File System (Amazon EFS).

Solusi

Tingkatkan izin kebijakan untuk peran pengguna Anda. Anda dapat menambahkan kebijakan AWS terkelola, seperti `AmazonElasticFileSystemClientFullAccess`.

Memecahkan masalah profil POSIX yang hilang

Deskripsi

Jika Anda menggunakan penyimpanan Amazon EFS untuk server Anda dan Anda menggunakan penyedia identitas khusus, Anda harus menyediakan AWS Lambda fungsi Anda dengan profil POSIX.

Menyebabkan

Salah satu kemungkinan penyebabnya adalah template yang kami sediakan untuk membuat metode Amazon API Gateway yang AWS Lambda didukung saat ini tidak berisi informasi POSIX.

Jika Anda memang memberikan informasi POSIX, format yang Anda gunakan untuk memberikan informasi POSIX mungkin tidak diuraikan dengan benar oleh Transfer Family.

Solusi

Pastikan bahwa Anda menyediakan elemen JSON untuk Transfer Family untuk `PosixProfile` parameter.

Misalnya, jika Anda menggunakan Python, Anda dapat menambahkan baris berikut di mana Anda mengurai parameter: `PosixProfile`

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

Atau, di JavaScript, Anda bisa menambahkan baris berikut, di mana *uid-value* dan *gid-value* bilangan bulat, 0 atau lebih besar, yang mewakili User ID (UID) dan Group ID (GID) masing-masing:

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

Contoh kode ini mengirim PosixProfile parameter ke Transfer Family sebagai objek JSON, bukan sebagai string.

Juga, di dalam AWS Secrets Manager, Anda harus menyimpan PosixProfile parameter sebagai berikut. Ganti *your-uid* dan *your-gid* dengan nilai aktual Anda untuk GID dan UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Memecahkan masalah direktori logis dengan Amazon EFS

Deskripsi

Jika direktori home pengguna tidak ada, dan mereka menjalankan `ls` perintah, sistem merespons sebagai berikut:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Menyebabkan

Jika server Transfer Family Anda menggunakan Amazon EFS, direktori home untuk pengguna harus dibuat dengan akses baca dan tulis sebelum pengguna dapat bekerja di direktori home logisnya. Pengguna tidak dapat membuat direktori ini sendiri, karena mereka akan kekurangan izin untuk `mkdir` direktori home logis mereka.

Solusi

Seorang pengguna dengan akses administratif ke direktori induk perlu membuat direktori home logis pengguna.

Memecahkan masalah penyimpanan dan enkripsi

Bagian ini menjelaskan kemungkinan solusi untuk masalah penyimpanan dan enkripsi.

Topik

- [Memecahkan masalah kebijakan untuk bucket Amazon S3 terenkripsi](#)

- [Memecahkan masalah pengecualian ResourceNotFound](#)

Memecahkan masalah kebijakan untuk bucket Amazon S3 terenkripsi

Deskripsi

Anda memiliki bucket Amazon S3 terenkripsi yang Anda gunakan sebagai penyimpanan untuk server Transfer Family Anda. Jika Anda mencoba mengunggah file ke server, Anda menerima kesalahan `Couldn't close file: Permission denied`.

Dan jika Anda melihat log server, Anda melihat kesalahan berikut:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13  
ERROR Message="Access denied"
```

Menyebabkan

Kebijakan untuk pengguna IAM Anda tidak memiliki izin untuk mengakses bucket terenkripsi.

Solusi

Anda harus menentukan izin tambahan dalam kebijakan Anda untuk memberikan izin required AWS Key Management Service (AWS KMS). Lihat perinciannya di [Perlindungan data dan enkripsi](#).

Memecahkan masalah pengecualian **ResourceNotFound**

Deskripsi

Anda menerima kesalahan di mana sumber daya tidak dapat ditemukan. Misalnya, jika Anda menjalankan `UpdateServer`, Anda mungkin mendapatkan kesalahan berikut:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:  
Unknown server
```

Menyebabkan

Ada beberapa alasan untuk menerima `ResourceNotFoundException` pesan. Dalam kebanyakan kasus, sumber daya yang Anda tentukan dalam perintah API Anda tidak ada. Jika Anda memang menentukan sumber daya yang ada, maka penyebab yang paling mungkin adalah bahwa wilayah default Anda berbeda dari wilayah untuk sumber daya Anda. Misalnya, jika wilayah default Anda

adalah us-east-1, dan server Transfer Family Anda berada di us-east-2, Anda akan menerima pengecualian sumber daya Tidak Dikenal.

Untuk detail tentang menyetel wilayah default, lihat [Konfigurasi cepat dengan aws configure](#).

Solusi

Tambahkan parameter region ke perintah API Anda untuk secara eksplisit menentukan tempat menemukan sumber daya tertentu.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Memecahkan masalah pemantauan dan peringatan

Bagian ini memberikan informasi tentang pemantauan pemecahan masalah dan peringatan masalah dengan AWS Transfer Family, termasuk CloudWatch metrik yang hilang atau tidak lengkap dan peristiwa yang hilang. EventBridge

Topik

- [Memecahkan masalah metrik yang hilang atau tidak lengkap CloudWatch](#)
- [Memecahkan masalah peristiwa yang hilang EventBridge](#)

Memecahkan masalah metrik yang hilang atau tidak lengkap CloudWatch

Deskripsi

CloudWatch metrik untuk server Transfer Family Anda hilang, tidak lengkap, atau tidak diperbarui seperti yang diharapkan.

Menyebabkan

Metrik yang hilang atau tidak lengkap dapat disebabkan oleh beberapa faktor:

- Masalah konfigurasi logging
- Tingkat aktivitas rendah yang tidak menghasilkan metrik dalam jangka waktu yang diharapkan
- Melihat metrik dengan dimensi atau rentang waktu yang salah

Solusi

Untuk mengatasi masalah dengan CloudWatch metrik yang hilang atau tidak lengkap:

1. Pastikan logging dikonfigurasi dengan benar untuk Transfer Familyserver Anda:
 - Di konsol Transfer Family, periksa apakah logging diaktifkan di bawah Rincian server > Detail tambahan > Peran Logging.
 - Sangat bahwa peran logging memiliki izin dan hubungan kepercayaan yang diperlukan.
2. Saat melihat metrik di CloudWatch konsol:
 - Gunakan dimensi yang benar, misalnya ServerIduntuk metrik tingkat server
 - Sesuaikan rentang waktu untuk memastikannya mencakup periode aktivitas
 - Periksa apakah Anda berada di tempat yang benar Wilayah AWS
3. Hasilkan aktivitas pengujian di server Transfer Family Anda untuk memastikan metrik sedang diproduksi.

Memecahkan masalah peristiwa yang hilang EventBridge

Deskripsi

Anda telah mengonfigurasi EventBridge aturan Amazon untuk menangkap peristiwa Transfer Family, tetapi acara tidak dikirim ke tujuan target atau memicu tindakan yang diharapkan.

Menyebabkan

EventBridge Peristiwa yang hilang dapat disebabkan oleh:

- Pola acara yang tidak dikonfigurasi dengan benar
- Masalah izin dengan target acara
- Batas layanan atau pembatasan
- Peristiwa tidak dihasilkan karena konfigurasi server

Solusi

Untuk memecahkan masalah peristiwa yang hilang EventBridge :

1. Verifikasi pola acara Anda diformat dengan benar agar sesuai dengan acara Transfer Family:

```
{
```

```
"source": ["aws.transfer"],
"detail-type": ["Transfer State Change"],
"detail": {
  "serverId": ["s-1234567890abcdef0"]
}
}
```

2. Periksa apakah target acara Anda memiliki izin yang diperlukan:

- Untuk target Lambda, pastikan kebijakan sumber daya fungsi Lambda memungkinkan untuk memanggilnya EventBridge
- Untuk target SQS, verifikasi kebijakan antrian memungkinkan EventBridge untuk mengirim pesan
- Untuk target SNS, konfirmasikan izin kebijakan topik EventBridge untuk mempublikasikannya

3. Uji aturan Anda dengan menghasilkan contoh peristiwa:

- Gunakan EventBridge konsol untuk membuat acara pengujian yang cocok dengan pola Anda
- Lakukan tindakan di server Transfer Family Anda yang seharusnya menghasilkan acara

4. Aktifkan metrik EventBridge aturan untuk memantau pemanggilan dan kegagalan aturan:

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. Periksa CloudWatch Log untuk setiap pesan kesalahan yang terkait dengan kegagalan pengiriman acara

Memecahkan masalah transfer lintas wilayah

Bagian ini menjelaskan solusi yang mungkin untuk masalah yang terkait dengan mentransfer file. Wilayah AWS

Topik

- [Memecahkan masalah izin transfer lintas wilayah](#)
- [Memecahkan masalah performa transfer lintas wilayah](#)

Memecahkan masalah izin transfer lintas wilayah

Deskripsi

Saat mencoba mentransfer file antara bucket Amazon S3 di berbagai wilayah menggunakan alur kerja Transfer Family, Anda mengalami error seperti:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

Menyebabkan

Cross-region transfer memerlukan izin IAM khusus untuk bucket sumber dan tujuan. Peran IAM yang digunakan oleh server atau alur kerja Transfer Family Anda mungkin tidak memiliki izin yang cukup untuk mengakses bucket di wilayah lain.

Solusi

Untuk mengatasi masalah izin transfer lintas wilayah:

1. Pastikan peran IAM Anda memiliki izin untuk bucket sumber dan tujuan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::target-bucket-name/*"
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
  }
]
}

```

2. Jika menggunakan enkripsi KMS, tambahkan izin untuk kunci KMS sumber dan tujuan:

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}

```

3. Verifikasi bahwa kebijakan bucket di kedua wilayah mengizinkan akses dari peran IAM server Transfer Family
4. Untuk transfer lintas akun, pastikan izin lintas akun yang tepat dikonfigurasi

Memecahkan masalah performa transfer lintas wilayah

Deskripsi

Cross-region Transfer secara signifikan lebih lambat dari yang diharapkan atau time out selama transfer file besar.

Menyebabkan

Cross-region Transfer secara inheren melibatkan latensi yang lebih besar dan dapat dipengaruhi oleh kondisi jaringan, ukuran file, dan batas layanan. File besar atau volume file kecil yang tinggi dapat mengalami penurunan kinerja.

Solusi

Untuk meningkatkan kinerja transfer lintas wilayah:

- Untuk file besar, pertimbangkan untuk menggunakan Amazon S3 Transfer Acceleration:

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Untuk beberapa file kecil, kumpulkan mereka bersama-sama sebelum transfer:
 - Gunakan kompresi untuk menggabungkan beberapa file
 - Gunakan operasi batch Amazon S3 untuk transfer skala besar
- Pertimbangkan untuk menggunakan konektor SFTP Transfer Family dengan pengaturan batas waktu yang sesuai untuk transfer besar
- Untuk transfer berulang, pertimbangkan untuk mereplikasi data menggunakan Amazon Cross-Region S3 Replication (CRR) alih-alih transfer ad-hoc
- Pantau performa transfer menggunakan CloudWatch metrik Amazon untuk mengidentifikasi kemacetan

Memecahkan masalah penerapan Terraform

Bagian ini menjelaskan kemungkinan solusi untuk masalah yang terkait dengan penerapan sumber daya Transfer Family menggunakan Terraform. Untuk informasi umum tentang modul Terraform untuk Transfer Family, lihat. [Modul Transfer Family Terraform](#)

Topik

- [Memecahkan masalah kegagalan pembuatan sumber daya Terraform](#)
- [Memecahkan masalah manajemen status Terraform](#)

Memecahkan masalah kegagalan pembuatan sumber daya Terraform

Deskripsi

Saat mencoba membuat sumber daya Transfer Family menggunakan Terraform, Anda mengalami kesalahan seperti:

```
Error: error creating Transfer Server: InvalidRequestException: The request is not  
valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user  
because the server endpoint type is incompatible with the home directory type.
```

Menyebabkan

Kesalahan ini biasanya terjadi karena parameter konfigurasi yang tidak kompatibel atau dependensi yang hilang dalam konfigurasi Terraform Anda. Penyebab umum meliputi:

- Jenis titik akhir dan konfigurasi penyimpanan yang tidak kompatibel
- Tidak ada peran atau kebijakan IAM yang diperlukan
- Spesifikasi kebijakan keamanan yang salah
- Masalah konfigurasi titik akhir VPC

Solusi

Untuk mengatasi masalah penerapan Terraform:

- Pastikan konfigurasi Terraform Anda menggunakan kombinasi parameter yang kompatibel:
 - Untuk titik akhir publik, pastikan Anda menggunakan Amazon S3 untuk penyimpanan.
 - Untuk titik akhir VPC, verifikasi konfigurasi VPC dan grup keamanan yang tepat.
- Gunakan dependensi eksplisit dengan `depends_on` atribut untuk memastikan sumber daya dibuat dalam urutan yang benar.
- Verifikasi bahwa semua peran IAM memiliki hubungan kepercayaan dan izin yang diperlukan.
- Gunakan versi terbaru AWS penyedia untuk Terraform untuk memastikan kompatibilitas dengan semua fitur Transfer Family.
- Untuk penerapan yang kompleks dan kasus penggunaan sederhana, pertimbangkan untuk menggunakan modul Transfer Family Terraform resmi yang tersedia di GitHub <https://github.com/aws-ia/terraform-aws-transfer-family> Modul-modul ini memberikan contoh ekstensif yang mencakup kasus penggunaan pelanggan yang sederhana dan kompleks, mengikuti praktik AWS terbaik, dan dapat menyederhanakan penerapan bagi pelanggan yang membutuhkan bantuan dengan konfigurasi infrastruktur sebagai kode (IAC).

Memecahkan masalah manajemen status Terraform

Deskripsi

Setelah membuat perubahan pada sumber daya Transfer Family Anda di luar Terraform (melalui konsol atau AWS CLI), Anda mengalami penyimpangan status atau kesalahan saat menjalankan `terraform plan` atau `terraform apply`

Menyebabkan

Terraform memelihara file status yang melacak sumber daya yang dikelolanya. Saat perubahan dilakukan di luar Terraform, file status menjadi tidak sinkron dengan sumber daya sebenarnya, menyebabkan kesalahan atau perilaku tak terduga selama operasi Terraform berikutnya.

Solusi

Untuk mengatasi masalah manajemen status Terraform dengan sumber daya Transfer Family:

1. Gunakan `terraform import` untuk membawa sumber daya yang ada di bawah manajemen Terraform:

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. Gunakan `terraform refresh` untuk memperbarui file status dengan infrastruktur dunia nyata saat ini
3. Untuk sumber daya yang tidak dapat diimpor atau memiliki masalah status yang rumit, pertimbangkan `terraform state rm` untuk menggunakannya untuk menghapusnya dari file status, lalu buat ulang dengan Terraform
4. Menerapkan kebijakan untuk mengelola sumber daya Transfer Family secara eksklusif melalui Terraform untuk mencegah pergeseran status di masa depan
5. Gunakan penyimpanan status jarak jauh dengan penguncian untuk mencegah modifikasi bersamaan saat bekerja dalam tim

Memecahkan masalah integrasi Firewall Aplikasi Web

Bagian ini menjelaskan kemungkinan solusi untuk masalah yang terkait dengan integrasi AWS WAF dengan Transfer Family.

Topik

- [Memecahkan masalah WAF memblokir lalu lintas yang sah](#)
- [Memecahkan masalah integrasi WAF dengan penyedia identitas khusus](#)

Memecahkan masalah WAF memblokir lalu lintas yang sah

Deskripsi

Setelah mengonfigurasi AWS WAF dengan endpoint Transfer Family Anda, pengguna yang sah tidak dapat terhubung atau mengalami kegagalan koneksi intermiten. Anda mungkin melihat respons HTTP 403 (Terlarang) di log Anda.

Menyebabkan

AWS WAF Aturan Anda mungkin terlalu ketat atau tidak dikonfigurasi dengan benar, menyebabkan kesalahan positif yang memblokir lalu lintas yang sah. Penyebab umum meliputi:

- IP-based aturan yang secara tidak sengaja memblokir jaringan perusahaan atau VPN
- Rate-based aturan dengan ambang batas yang terlalu rendah untuk pola lalu lintas normal Anda
- Grup aturan terkelola yang terlalu agresif untuk kasus penggunaan Anda

Solusi

Untuk mengatasi masalah positif palsu:

1. Aktifkan AWS WAF logging untuk mengidentifikasi aturan mana yang memicu blok. Untuk petunjuk, lihat [Mencatat lalu lintas ACL AWS WAF web](#).
2. Tinjau log Anda untuk mengidentifikasi pola dalam permintaan yang diblokir.
3. Sesuaikan aturan Anda dengan:
 - Menambahkan alamat IP atau rentang ke daftar yang diizinkan
 - Meningkatkan batas tarif untuk aturan berbasis tarif
 - Menyetel aturan khusus ke mode Hitung alih-alih mode Blok untuk memantau tanpa memblokir
 - Membuat pengecualian untuk aturan tertentu menggunakan pengecualian grup aturan
4. Uji konfigurasi yang diperbarui dengan sampel representatif lalu lintas yang sah sebelum menerapkan sepenuhnya.

Memecahkan masalah integrasi WAF dengan penyedia identitas khusus

Deskripsi

Setelah mengonfigurasi AWS WAF dengan server Transfer Family yang menggunakan penyedia identitas kustom, autentikasi gagal atau pengguna mengalami masalah autentikasi intermiten.

Menyebabkan

Saat menggunakan penyedia identitas kustom dengan API Gateway, AWS WAF aturan dapat mengganggu panggilan API antara Transfer Family dan penyedia identitas Anda. Ini bisa terjadi karena AWS WAF sedang memeriksa dan berpotensi memblokir lalu lintas API berdasarkan set aturannya.

Solusi

Untuk mengatasi masalah dengan AWS WAF dan penyedia identitas khusus:

- Pastikan AWS WAF konfigurasi Anda menyertakan pengecualian untuk titik akhir API Gateway yang digunakan oleh penyedia identitas kustom Anda.
- Tambahkan prinsipal layanan Transfer Family (transfer.amazonaws.com) ke daftar yang diizinkan dalam aturan Anda. AWS WAF
- Jika menggunakan grup aturan terkelola, tinjau mereka untuk aturan yang mungkin memengaruhi alur autentikasi API dan pertimbangkan untuk menonaktifkan aturan khusus tersebut.
- Uji penyedia identitas Anda secara langsung menggunakan operasi `TestIdentityProvider` API untuk memverifikasi bahwa penyedia identitas berfungsi dengan benar tanpa AWS WAF gangguan.

Memecahkan masalah pengguna yang dikelola layanan

Bagian ini menjelaskan kemungkinan solusi untuk masalah dengan pengguna yang dikelola layanan.

Topik

- [Memecahkan masalah pengguna yang dikelola layanan](#)

Memecahkan masalah pengguna yang dikelola layanan

Bagian ini menjelaskan kemungkinan solusi untuk masalah berikut.

Topik

- [Memecahkan masalah badan kunci publik terlalu lama](#)
- [Pemecahan masalah gagal menambahkan kunci publik SSH](#)

Memecahkan masalah badan kunci publik terlalu lama

Deskripsi

Saat Anda mencoba membuat pengguna yang dikelola layanan, Anda menerima kesalahan berikut:

```
Failed to create user (1 validation error detected:  
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or  
equal to 2048)
```

Menyebabkan

Anda mungkin memasukkan kunci PGP untuk badan kunci publik, dan AWS Transfer Family tidak mendukung kunci PGP untuk pengguna yang dikelola layanan.

Solusi

Jika kunci PGP RSA-based, Anda dapat mengonversinya ke format PEM. Misalnya, Ubuntu menyediakan alat konversi di sini: <https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

Pemecahan masalah gagal menambahkan kunci publik SSH

Deskripsi

Saat Anda mencoba menambahkan kunci publik untuk pengguna yang dikelola layanan, Anda menerima kesalahan berikut:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Menyebabkan

Anda mungkin mencoba mengimpor kunci SSH2-formatted publik, dan AWS Transfer Family tidak mendukung kunci SSH2-formatted publik untuk pengguna yang dikelola layanan.

Solusi

Anda perlu mengonversi kunci ke dalam format OpenSSH. Proses ini dijelaskan di [Mengonversi kunci SSH2 ke format kunci publik SSH](#).

Memecahkan masalah AS2

Bagian ini menjelaskan kemungkinan solusi untuk masalah dengan transfer AS2.

Topik

- [Memecahkan masalah AS2](#)
- [Masalah sertifikat AS2](#)
- [Masalah penerimaan AS2 MDN](#)
- [Masalah pemantauan kedaluwarsa sertifikat](#)

Memecahkan masalah AS2

[Kode kesalahan AS2](#), pesan, dan tips pemecahan masalah untuk server yang mendukung Pernyataan Penerapan 2 (AS2) dijelaskan di bagian kode kegagalan AS2 dalam panduan ini.

Masalah sertifikat AS2

Deskripsi

Anda mengalami kesalahan terkait sertifikat dengan transfer AS2.

Menyebabkan

Penyebab umum termasuk sertifikat kedaluwarsa, format sertifikat yang salah, atau rantai sertifikat yang tidak cocok.

Solusi

Coba solusi berikut:

- Verifikasi bahwa sertifikat Anda tidak kedaluwarsa
- Pastikan sertifikat dalam format yang benar (PEM for AWS Transfer Family)
- Periksa apakah rantai sertifikat sudah lengkap dan valid
- Konfirmasikan bahwa sertifikat penandatanganan dan enkripsi cocok antara mitra dagang
- Putar sertifikat dengan baik sebelum kedaluwarsa untuk menghindari gangguan

Masalah penerimaan AS2 MDN

Deskripsi

Anda tidak menerima Pemberitahuan Disposisi Pesan (mDNS) yang diharapkan untuk transfer AS2.

Menyebabkan

Masalah MDN dapat terjadi karena masalah konektivitas jaringan, konfigurasi titik akhir yang salah, atau ketidakcocokan format MDN.

Solusi

Pertimbangkan solusi ini:

- Verifikasi bahwa URL MDN dikonfigurasi dan dapat diakses dengan benar
- Periksa konektivitas jaringan antara server AS2 dan titik akhir MDN
- Pastikan kedua mitra dagang dikonfigurasi untuk jenis MDN yang sama (sinkron atau asinkron)
- Tinjau log AS2 untuk setiap kesalahan yang terkait dengan pemrosesan MDN
- Jika menggunakan mDNS sinkron, verifikasi bahwa batas waktu ditetapkan dengan tepat

Masalah pemantauan kedaluwarsa sertifikat

Bagian ini memberikan solusi untuk masalah umum yang terkait dengan pemantauan kedaluwarsa sertifikat dan metrik. `DaysUntilExpiry`

`DaysUntilExpiry` metrik tidak muncul

Masalah: `DaysUntilExpiry` Metrik tidak terlihat di Amazon CloudWatch setelah mengimpor sertifikat.

Solusi:

- Tunggu hingga 24 jam setelah mengimpor sertifikat. Transfer Family dapat memakan waktu hingga satu hari penuh untuk memancarkan metrik ke akun Anda.
- Pastikan Anda mencari di AWS wilayah yang benar dan di bawah `AWS/Transfer` namespace di CloudWatch

Alarm kedaluwarsa sertifikat tidak memicu

Masalah: CloudWatch alarm untuk kedaluwarsa sertifikat tidak terpicu saat diharapkan.

Solusi:

- Verifikasi bahwa alarm dikonfigurasi dengan `Maximum` statistik dan periode 1 hari.
- Periksa apakah perbandingan ambang batas diatur ke `Less than or equal to` jumlah hari yang diinginkan.

- Pastikan `Treat missing data as good (not breaching)` yang dipilih dalam konfigurasi alarm.
- Verifikasi bahwa dimensi alarm cocok dengan sertifikat `CertificateId` dan Deskripsi Anda (jika disediakan).
- Periksa apakah tindakan alarm (topik SNS, pemberitahuan email) dikonfigurasi dan aktif dengan benar.

AWS Transfer Family Referensi API

Panduan Referensi API lengkap untuk Transfer Family tersedia di [Referensi AWS Transfer Family API](#).

AWS Transfer Family adalah layanan transfer aman yang dapat Anda gunakan untuk mentransfer file masuk dan keluar dari penyimpanan Amazon Simple Storage Service (Amazon S3) melalui protokol berikut:

- Protokol Transfer File Secure Shell (SSH) (SFTP)
- Protokol Transfer File Aman (FTPS)
- Protokol Transfer File (FTP)
- Pernyataan Penerapan 2 (AS2)

Server, pengguna, dan peran semuanya diidentifikasi oleh Amazon Resource Name (ARN) mereka. Anda dapat menetapkan tag, yang merupakan pasangan nilai kunci, ke entitas dengan ARN. Tag adalah metadata yang dapat digunakan untuk mengelompokkan atau mencari entitas ini. Salah satu contoh di mana tag berguna adalah untuk tujuan akuntansi.

Konvensi berikut diamati dalam format AWS Transfer Family ID:

- `ServerId` nilai mengambil bentuk `s-01234567890abcdef`.
- `SshPublicKeyId` nilai mengambil bentuk `key-01234567890abcdef`.

Format Amazon Resource Name (ARN) mengambil bentuk berikut:

- Untuk server, ARN mengambil formulir `arn:aws:transfer:region:account-id:server/server-id`.

Contoh dari ARN server adalah: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- Untuk pengguna, ARN mengambil formulir `arn:aws:transfer:region:account-id:user/server-id/username`.

Contohnya adalah `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Entri DNS (endpoint) yang digunakan adalah sebagai berikut:

- Titik akhir API mengambil formulir `transfer.region.amazonaws.com`.
- Titik akhir server mengambil formulir `server-id.server.transfer.region.amazonaws.com`.

Referensi antarmuka API ini AWS Transfer Family berisi dokumentasi untuk antarmuka pemrograman yang dapat Anda gunakan untuk mengelola AWS Transfer Family. Struktur referensi adalah sebagai berikut:

- Untuk daftar tindakan API menurut abjad, lihat [Actions](#)
- Untuk daftar alfabet tipe data, lihat [Types](#)
- Untuk daftar parameter kueri umum, lihat [Parameter Umum](#).
- Untuk deskripsi kode kesalahan, lihat [Kesalahan Umum](#).

Tip

Daripada benar-benar menjalankan perintah, Anda dapat menggunakan `--generate-cli-skeleton` parameter dengan panggilan API apa pun untuk menghasilkan dan menampilkan templat parameter. Anda kemudian dapat menggunakan template yang dihasilkan untuk menyesuaikan dan digunakan sebagai input pada perintah selanjutnya. Untuk detailnya, lihat [Menghasilkan dan menggunakan file kerangka parameter](#).

Membuat permintaan API

Selain menggunakan konsol, Anda dapat menggunakan AWS Transfer Family API untuk mengonfigurasi dan mengelola server secara terprogram. Bagian ini menjelaskan AWS Transfer Family operasi, penandatanganan permintaan untuk otentikasi, dan penanganan kesalahan. Untuk informasi tentang wilayah dan titik akhir yang tersedia untuk Transfer Family, lihat [AWS Transfer Family titik akhir dan kuota](#) di Referensi Umum AWS

Note

Anda juga dapat menggunakan AWS SDK saat mengembangkan aplikasi dengan Transfer Family;. AWS SDK untuk Java, .NET, dan PHP membungkus Transfer Family API yang

mendasarinya, menyederhanakan tugas pemrograman Anda. Untuk informasi tentang mengunduh perpustakaan SDK, lihat [Perpustakaan kode sampel](#).

Transfer Family membutuhkan header permintaan

Bagian ini menjelaskan header yang diperlukan yang harus Anda kirim dengan setiap permintaan POST. AWS Transfer Family Anda menyertakan header HTTP untuk mengidentifikasi informasi kunci tentang permintaan termasuk operasi yang ingin Anda panggil, tanggal permintaan, dan informasi yang menunjukkan otorisasi Anda sebagai pengirim permintaan. Header tidak peka huruf besar/kecil dan urutan header tidak penting.

Contoh berikut menunjukkan header yang digunakan dalam [ListServers](#) operasi.

```
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}
```

Berikut ini adalah header yang harus disertakan dengan permintaan POST Anda ke Transfer Family. Header yang ditunjukkan di bawah ini yang dimulai dengan “x-amz” khusus untuk AWS. Semua header lain yang terdaftar adalah header umum yang digunakan dalam transaksi HTTP.

Transfer Family meminta masukan dan penandatanganan

Semua input permintaan harus dikirim sebagai bagian dari muatan JSON di badan permintaan. Untuk tindakan di mana semua bidang permintaan bersifat opsional `ListServers`, misalnya, Anda masih perlu menyediakan objek JSON kosong di badan permintaan, seperti `{}`. Struktur payload Transfer Family request/response didokumentasikan dalam referensi API yang ada, misalnya [DescribeServer](#).

Transfer Family mendukung otentikasi menggunakan AWS Signature Versi 4. Untuk detailnya, lihat [Menandatangani permintaan AWS API](#).

Tanggapan kesalahan

Ketika ada kesalahan, informasi header respons berisi:

- Content-Type: application/x-amz-json-1.1
- Kode status yang sesuai 4xx atau 5xx HTTP

Tubuh respons kesalahan berisi informasi tentang kesalahan yang terjadi. Contoh respon kesalahan berikut menunjukkan sintaks output elemen respon umum untuk semua respon kesalahan.

```
{
  "__type": "String",
  "Message": "String", <!-- Message is lowercase in some instances -->
  "Resource": "String",
  "ResourceType": "String",
  "RetryAfterSeconds": "String"
}
```

Tabel berikut menjelaskan bidang respons kesalahan JSON yang ditunjukkan dalam sintaks sebelumnya.

__jenis

Salah satu pengecualian dari panggilan Transfer Family API.

Tipe: String

Pesan atau pesan

Salah satu pesan kode kesalahan operasi.

Note

Beberapa pengecualian digunakan `message`, dan yang lainnya menggunakan `Message`. Anda dapat memeriksa kode untuk antarmuka Anda untuk menentukan kasus yang tepat. Atau, Anda dapat menguji setiap opsi untuk melihat mana yang berfungsi.

Tipe: String

Sumber Daya

Sumber daya yang kesalahannya dipanggil. Misalnya, jika Anda mencoba membuat pengguna yang sudah ada, itu Resource adalah nama pengguna untuk pengguna yang ada.

Tipe: String

ResourceType

Jenis sumber daya yang kesalahannya dipanggil. Misalnya, jika Anda mencoba membuat pengguna yang sudah ada, ResourceType isUser.

Tipe: String

RetryAfterSeconds

Jumlah detik untuk menunggu sebelum mencoba kembali perintah.

Tipe: String

Contoh respons kesalahan

Badan JSON berikut dikembalikan jika Anda memanggil DescribeServer API dan menentukan server yang tidak ada.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

Badan JSON berikut dikembalikan jika menjalankan API menyebabkan pelambatan terjadi.

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

Badan JSON berikut dikembalikan jika Anda menggunakan CreateServer API dan Anda tidak memiliki izin yang cukup untuk membuat server Transfer Family.

```
{
```

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

Badan JSON berikut dikembalikan jika Anda menggunakan CreateUser API dan menentukan pengguna yang sudah ada.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

Pustaka yang tersedia

AWS menyediakan pustaka, kode sampel, tutorial, dan sumber daya lainnya untuk pengembang perangkat lunak yang lebih suka membangun aplikasi menggunakan API khusus bahasa alih-alih alat baris perintah dan API Kueri. Pustaka ini menyediakan fungsi dasar (tidak termasuk dalam API), seperti otentikasi permintaan, percobaan ulang permintaan, dan penanganan kesalahan sehingga lebih mudah untuk memulai. Lihat [Alat untuk dibangun AWS](#)

Untuk pustaka dan kode sampel dalam semua bahasa, lihat [Contoh kode & pustaka](#).

Penyedia Identitas

AWS Transfer Family mendukung beberapa jenis penyedia identitas untuk mengautentikasi dan mengelola pengguna. Setiap server hanya dapat menggunakan satu metode otentikasi, yang harus dipilih ketika server dibuat.

Layanan Dikelola

Dengan metode SERVICE_MANAGED otentikasi, kredensial pengguna disimpan dan dikelola di dalamnya. AWS Transfer Family Pengguna diautentikasi menggunakan kunci publik SSH yang terkait dengan nama pengguna mereka di server.

Setiap pengguna dapat memiliki satu atau lebih kunci publik SSH yang disimpan dalam layanan. Ketika klien meminta operasi file, ia menyediakan nama pengguna dan kunci pribadi SSH, yang diautentikasi terhadap kunci publik yang disimpan.

Directory Service

Metode `AWS_DIRECTORY_SERVICE` otentikasi memungkinkan Anda untuk mengintegrasikan dengan AWS Directory Service untuk Microsoft Active Directory (AWS Directory Service for Microsoft Active Directory).

Opsi ini memungkinkan Anda untuk mengelola otentikasi pengguna dan akses melalui grup Active Directory yang ada. Pengguna dapat mengautentikasi menggunakan kredensial Direktori Aktif mereka.

Ada batas default 100 grup Active Directory per server, yang dapat ditingkatkan hingga maksimum 150 grup melalui peningkatan batas layanan.

Lambda

Metode `AWS_LAMBDA` otentikasi memungkinkan Anda untuk terhubung ke penyedia identitas kustom menggunakan AWS Lambda.

Opsi ini memberikan fleksibilitas untuk berintegrasi dengan sistem manajemen identitas Anda yang ada. Fungsi Lambda bertanggung jawab untuk mengautentikasi pengguna dan mengembalikan kebijakan akses yang sesuai.

Kustom (API Gateway)

Metode `API_GATEWAY` otentikasi (ditampilkan sebagai Kustom di konsol) memungkinkan Anda menggunakan metode otentikasi khusus yang menyediakan otentikasi pengguna dan kontrol akses.

Metode ini bergantung pada Amazon API Gateway untuk menggunakan panggilan API Anda dari penyedia identitas Anda untuk memvalidasi permintaan pengguna. Anda dapat menggunakan metode kustom ini untuk mengautentikasi pengguna terhadap layanan direktori, name/password pasangan database, atau mekanisme lainnya.

Untuk semua metode otentikasi, pengguna diberi kebijakan yang menentukan akses mereka ke bucket Amazon S3 atau sistem file Amazon Elastic File System. Server mewarisi hubungan kepercayaan dari pengguna melalui peran IAM dengan `AssumeRole` tindakan, memungkinkannya untuk melakukan operasi file atas nama pengguna.

Konvensi Penamaan

AWS Transfer Family menggunakan format standar untuk pengidentifikasi sumber daya dan Amazon Resource Names (ARN). Memahami konvensi ini penting saat bekerja dengan AWS Transfer Family API.

Format ID

Konvensi berikut diamati dalam format AWS Transfer Family ID:

ID Server

`ServerId` nilai mengambil bentuk `s-01234567890abcdef`.

ID Kunci Publik SSH

`SshPublicKeyId` nilai mengambil bentuk `key-01234567890abcdef`.

ID konektor

`ConnectorId` nilai mengambil bentuk `c-01234567890abcdef`.

ID Alur Kerja

`WorkflowId` nilai mengambil bentuk `w-01234567890abcdef`.

ID Profil

`ProfileId` nilai mengambil bentuk `p-01234567890abcdef`.

WebApp ID

`WebAppId` nilai mengambil bentuk `webapp-01234567890abcdef`.

Format ARN

Format Amazon Resource Name (ARN) mengambil bentuk berikut:

Server ARN

Untuk server, ARN mengambil formulir `arn:aws:transfer:region:account-id:server/server-id`.

Contoh: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

ARN Pengguna

Untuk pengguna, ARN mengambil formulir `arn:aws:transfer:region:account-id:user/server-id/username`.

Contoh: `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Konektor ARN

Untuk konektor, ARN mengambil formulir `arn:aws:transfer:region:account-id:connector/connector-id`.

Contoh: `arn:aws:transfer:us-east-1:123456789012:connector/c-01234567890abcdef`.

ARN Alur Kerja

Untuk alur kerja, ARN mengambil formulir `arn:aws:transfer:region:account-id:workflow/workflow-id`.

Contoh: `arn:aws:transfer:us-east-1:123456789012:workflow/w-01234567890abcdef`.

WebApp ARN

Untuk aplikasi web, ARN mengambil formulir `arn:aws:transfer:region:account-id:webapp/webapp-id`.

Contoh: `arn:aws:transfer:us-east-1:123456789012:webapp/webapp-01234567890abcdef`.

Anda dapat menetapkan tag, yang merupakan pasangan nilai kunci, ke entitas dengan ARN. Tag adalah metadata yang dapat digunakan untuk mengelompokkan atau mencari entitas ini. Salah satu contoh di mana tag berguna adalah untuk tujuan akuntansi.

DNS dan Endpoint

AWS Transfer Family menggunakan konvensi penamaan DNS standar untuk titik akhir API dan titik akhir server. Memahami titik akhir ini sangat penting untuk mengonfigurasi klien dan melakukan panggilan API.

Titik Akhir API

Titik akhir API digunakan untuk membuat panggilan API untuk mengelola AWS Transfer Family sumber daya. Titik akhir ini mengambil bentuk berikut:

Titik Akhir API Standar

Titik akhir API standar mengambil formulir `transfer.region.amazonaws.com`.

Contoh: `transfer.us-east-1.amazonaws.com`

Dual-Stack Titik Akhir API

AWS Transfer Family menawarkan titik akhir API dual-stack yang dapat diakses menggunakan permintaan IPv4 atau IPv6:

- `https://transfer.region-code.api.aws`
- `https://transfer-fips.region-code.api.aws`

Titik Akhir Server

Endpoint server digunakan oleh klien transfer file untuk terhubung ke AWS Transfer Family server. Titik akhir ini mengambil bentuk berikut:

Titik Akhir Server Standar

Titik akhir server standar mengambil formulir `server-id.server.transfer.region.amazonaws.com`.

Contoh: `s-01234567890abcdef.server.transfer.us-east-1.amazonaws.com`

Nama Host Kustom

Anda juga dapat mengonfigurasi nama host khusus untuk AWS Transfer Family server Anda. Nama host khusus dapat digunakan untuk memberikan pengalaman yang lebih ramah pengguna atau bermerek bagi pengguna Anda.

Untuk menggunakan nama host khusus, Anda harus:

1. Memiliki nama domain
2. Berikan sertifikat yang valid
3. Konfigurasi catatan DNS untuk menunjuk ke server Anda AWS Transfer Family

Untuk daftar lengkap AWS Transfer Family titik akhir menurut AWS Wilayah, lihat [AWS Transfer Family titik akhir dan kuota](#) di. Referensi Umum AWS

Riwayat dokumen untuk AWS Transfer Family

Tabel berikut menjelaskan dokumentasi untuk rilis ini AWS Transfer Family.

- Versi API: transfer-2018-11-05
- Pembaruan dokumentasi terbaru: November 19, 2025

Ubah	Deskripsi	Date
Dukungan endpoint VPC untuk aplikasi web Transfer Family	AWS Transfer Family aplikasi web sekarang mendukung titik akhir yang dihosting VPC, memungkinkan Anda meng-host titik akhir aplikasi web Anda di dalam cloud pribadi virtual untuk transfer data pribadi ke dan dari Amazon S3 tanpa melintasi internet publik. Lihat perinciannya di Membuat aplikasi web Transfer Family di VPC .	November 19, 2025
Dukungan IPv6	AWS Transfer Family sekarang mendukung titik akhir dual-stack (IPv4 dan IPv6) untuk titik akhir publik SFTP, titik akhir untuk, konektor SFTP dan AS2, dan VPC-internal titik akhir API. SFTP/FTPS/FTP/AS2 Lihat perinciannya di Dukungan IPv6 untuk server Transfer Family .	Juni 30, 2025

Ubah	Deskripsi	Date
Penyempurnaan pada pengalaman pengguna konektor SFTP	- Kemampuan untuk melayani sendiri pengaturan koneksi bersamaan untuk konektor Anda - Kemampuan untuk menyediakan kunci pribadi SSH dalam format OpenSSH yang digunakan untuk mengautentikasi koneksi - Kemampuan untuk menemukan kunci host publik dari server jarak jauh menggunakan konektor SFTP mereka Lihat perinciannya di Buat konektor SFTP dengan jalan keluar yang dikelola layanan.	April 9, 2025
Kemampuan konektor SFTP untuk menghapus, mengganti nama, dan memindahkan file di server SFTP jarak jauh	Anda sekarang dapat mengatur file yang disimpan di server SFTP jarak jauh dengan menghapus, mengganti nama, atau memindahkan file sumber ke lokasi arsip setelah disalin dari server jarak jauh. Lihat perinciannya di Memindahkan atau mengganti nama file atau direktori di server SFTP jarak jauh.	April 7, 2025

Ubah	Deskripsi	Date
Support untuk aplikasi AWS Transfer Family web	AWS Transfer Family aplikasi web adalah sumber daya baru yang dapat digunakan pelanggan untuk membuat antarmuka sederhana untuk mengakses data mereka di Amazon S3 melalui browser web. Lihat perinciannya di Aplikasi web Transfer Family .	Desember 1, 2024
Memindahkan Referensi API ke dalam panduan terpisah	Untuk meningkatkan pengalaman pelanggan , Referensi API sekarang diterbitkan secara terpisah dari panduan pengguna. Untuk referensi API terpisah, lihat Selamat datang di AWS Transfer Family API .	Juli 31, 2024
Kemampuan untuk konektor SFTP untuk membuat daftar file dan direktori jarak jauh	Transfer Family telah menambahkan kemampuan bagi pelanggan kami untuk menggunakan konektor SFTP untuk membuat daftar file yang disimpan di server SFTP jarak jauh. Untuk detailnya, lihat Daftar isi direktori jarak jauh	April 23, 2024

Ubah	Deskripsi	Date
Kemampuan untuk menggunakan sertifikat TLS yang ditandatangani sendiri oleh mitra dagang dengan pertukaran pesan AS2	AWS Transfer Family telah menambahkan opsi untuk mengimpor dan menggunakan sertifikat TLS publik mitra dagang yang ditandatangani sendiri untuk mengirim pesan Applicability Statement 2 (AS2) ke server mereka melalui HTTPS.	April 12, 2024
Penambahan kebijakan keamanan untuk konektor SFTP	AWS Transfer Family telah menambahkan kebijakan keamanan untuk digunakan dengan konektor SFTP. Lihat perinciannya di Kebijakan keamanan untuk AWS Transfer Family Konektor SFTP .	April 5, 2024
Integrasikan dengan Amazon EventBridge	AWS Transfer Family sekarang secara otomatis menerbitkan acara ke Amazon EventBridge untuk semua operasi transfer file. Lihat perinciannya di Mengelola Transfer Family acara menggunakan Amazon EventBridge .	Februari 8, 2024

Ubah	Deskripsi	Date
Penambahan kebijakan keamanan baru	AWS Transfer Family telah menambahkan kebijakan keamanan FIPS dan non-FIPS baru. Selain itu, kebijakan keamanan default yang ditetapkan ke server selalu merupakan kebijakan keamanan terbaru. Lihat perinciannya di Kebijakan keamanan untuk AWS Transfer Family server .	Februari 5, 2024
Support untuk alamat IP statis untuk konektor SFTP dan AS2	Transfer Family sekarang menyediakan alamat IP statis untuk konektor SFTP dan AS2. Ini memungkinkan koneksi dengan server SFTP jarak jauh yang diamankan oleh kontrol IP allowlisting. Untuk AS2, kami memperkenalkan alamat IP statis untuk respons MDN asinkron dari server AS2.	Januari 16, 2024
Panduan pengguna telah diatur ulang untuk menyelaraskan lebih dekat dengan versi terbaru. AWS Transfer Family	Transfer Family telah menambahkan beberapa fitur sejak panduan ini berasal, yang mengharuskan restrukturisasi panduan.	Januari 3, 2024

Ubah	Deskripsi	Date
Penyempurnaan pemetaan direktori logis Pengoptimalan kinerja daftar Amazon S3	Transfer Family sekarang mendukung pemetaan direktori logis hingga 2,1 MB. Anda juga sekarang dapat mendeklarasikan apakah pemetaan pengguna ke file. Untuk informasi selengkapnya, lihat Aturan untuk menggunakan direktori logis. Saat membuat atau memperbarui server yang menggunakan Amazon S3 untuk penyimpanan, Anda sekarang dapat mengoptimalkan kinerja daftar direktori (atau folder) S3 Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP.	17 November 2023
Port alternatif untuk server SFTP dengan titik akhir virtual private cloud (VPC)	Sekarang Anda dapat mengaktifkan port non-standar alternatif untuk server SFTP Transfer Family Anda yang memiliki titik akhir VPC. Untuk informasi selengkapnya, lihat Buat server di cloud pribadi virtual.	17 November 2023

Ubah	Deskripsi	Date
Support untuk konektor SFTP	Konektor SFTP memperluas kemampuan AWS Transfer Family untuk berkomunikasi dengan server jarak jauh baik di cloud maupun di tempat. Untuk informasi selengkapnya, lihat Menggunakan konektor SFTP .	25 Juli 2023
Support untuk otentikasi AS2 Basic	Transfer Family sekarang mendukung penggunaan otentikasi Dasar untuk server yang menggunakan protokol Applicability Statement 2 (AS2). Untuk informasi selengkapnya, lihat Otentikasi dasar untuk konektor AS2 .	Juni 30, 2023
Support untuk logging JSON terstruktur	Transfer Family sekarang mendukung pengiriman log JSON terstruktur ke Amazon CloudWatch, mengelompokkan steam log ke dalam grup log kustom, dan melakukan kueri log umum di seluruh protokol. Untuk informasi selengkapnya, lihat Amazon CloudWatch logging untuk AWS Transfer Family server .	Juni 24, 2023

Ubah	Deskripsi	Date
Support untuk beberapa metode otentikasi	Transfer Family memiliki dukungan untuk otentikasi dengan menggunakan kata sandi, public/private key pair, atau keduanya. Ini tersedia untuk server yang menggunakan protokol SFTP dan penyedia identitas khusus. Untuk informasi selengkapnya, lihat Buat SFTP-enabled server .	17 Mei 2023
Support untuk dekripsi Pretty Good Privacy (PGP) dengan file yang diproses Transfer Family dengan alur kerja	Transfer Family memiliki dukungan bawaan untuk dekripsi Pretty Good Privacy (PGP). Anda dapat menggunakan dekripsi PGP pada file yang diunggah melalui SFTP, FTPS, atau FTP ke Amazon Simple Storage Service (Amazon S3) atau Amazon Elastic File System (Amazon EFS). Untuk informasi selengkapnya, lihat Hasilkan kunci PGP dan Gunakan dekripsi PGP dalam alur kerja Anda .	21 Desember 2022

Ubah	Deskripsi	Date
Dukungan yang dikelola sepenuhnya untuk protokol transfer file Applicability Statement 2 (AS2) dengan server Transfer Family	Anda dapat membuat server yang menggunakan protokol AS2 untuk mengirim dan menerima informasi ke dan dari mitra dagang yang berada di dalam atau di luar AWS lingkungan. Untuk informasi selengkapnya, lihat Mengkonfigurasi AS2 .	25 Juli 2022
Support untuk display banner saat membuat server	Anda dapat menambahkan pesan yang disesuaikan saat membuat server. Anda dapat menampilkan pesan pra-otentikasi (semua protokol), dan pesan pasca-otentikasi (untuk server FTP dan FTPS). Untuk informasi selengkapnya, lihat Buat SFTP-enabled server , Buat FTPS-enabled server , atau Buat FTP-enabled server .	Februari 17, 2022

Ubah	Deskripsi	Date
Support untuk AWS Lambda sebagai penyedia identitas	Anda sekarang dapat terhubung ke penyedia identitas khusus menggunakan an AWS Lambda server Transfer Family mereka. Sebelumnya, Anda harus menyediakan Amazon API Gateway URL untuk mengintegrasikan penyedia identitas khusus. Untuk informasi selengkapnya, lihat Menggunakan AWS Lambda untuk mengintegrasikan penyedia identitas Anda .	November 16, 2021
Support untuk Alur Kerja Transfer File Terkelola	Alur Kerja Transfer File Terkelola memberi Anda abstraksi pemrosesan pasca-unggah untuk tugas umum yang saat ini Anda lakukan secara manual. Untuk informasi selengkapnya, lihat AWS Transfer Family alur kerja terkelola .	2 September 2021

Ubah	Deskripsi	Date
Support untuk AWS Directory Service for Microsoft Active Directory	Selain penyedia identitas terkelola layanan dan kustom, Anda sekarang dapat menggunakan AWS Directory Service for Microsoft Active Directory untuk mengelola akses pengguna untuk otentikasi dan otorisasi. Untuk informasi selengkapnya, lihat Menggunakan AWS Directory Service untuk Microsoft Active Directory .	24 Mei 2021
Baru Wilayah AWS	AWS Transfer Family sekarang tersedia di Wilayah Afrika (Cape Town). Untuk informasi selengkapnya tentang titik akhir Transfer Family, lihat AWS Transfer Family titik akhir dan kuota di Referensi Umum AWS	24 Februari 2021
Baru Wilayah AWS	AWS Transfer Family sekarang tersedia di Wilayah Asia Pasifik (Hong Kong) dan Timur Tengah (Bahrain). Untuk informasi selengkapnya tentang titik akhir Transfer Family, lihat AWS Transfer Family titik akhir dan kuota di Referensi Umum AWS	17 Februari 2021

Ubah	Deskripsi	Date
Support untuk Amazon EFS sebagai penyimpanan data	Transfer Family sekarang mendukung transfer file masuk dan keluar dari Amazon Elastic File System (Amazon EFS). Amazon EFS adalah sistem file NFS elastis yang sederhana, dapat diskalakan, dan dikelola sepenuhnya. Untuk informasi selengkapnya, lihat Konfigurasi sistem file Amazon EFS .	Januari 06, 2021
Support untuk AWS WAF	Transfer Family sekarang mendukung AWS WAF, firewall aplikasi web yang membantu melindungi aplikasi web dan operasi API dari serangan. Untuk informasi selengkapnya, lihat Tambahkan firewall aplikasi web .	24 November 2020
Support untuk beberapa grup keamanan di virtual private cloud (VPC)	Anda sekarang dapat melampirkan beberapa grup keamanan ke server di VPC. Untuk informasi selengkapnya, lihat Buat server di cloud pribadi virtual .	15 Oktober 2020

Ubah	Deskripsi	Date
Baru Wilayah AWS	Transfer Family sekarang tersedia di AWS GovCloud (US) Wilayah. Untuk informasi selengkapnya tentang titik akhir Transfer Family untuk AWS GovCloud (US) Wilayah, lihat AWS Transfer Family titik akhir dan kuota di. Referensi Umum AWS Untuk informasi tentang penggunaan Transfer Family di AWS GovCloud (US) Wilayah, lihat AWS Transfer Family di Panduan AWS GovCloud (US) Pengguna.	30 September 2020
Kebijakan keamanan dengan algoritma kriptografi yang didukung sekarang dapat dilampirkan ke server Anda	Anda sekarang dapat melampirkan kebijakan keamanan yang berisi serangkaian algoritma kriptografi yang didukung ke server Anda. Untuk informasi selengkapnya, lihat Kebijakan keamanan untuk AWS Transfer Family server .	12 Agustus 2020

Ubah	Deskripsi	Date
Dukungan untuk titik akhir Federal Information Processing Standard (FIPS)	FIPS-enabled Endpoint sekarang tersedia di Amerika Wilayah AWS Utara. Untuk Wilayah yang tersedia, lihat AWS Transfer Family titik akhir dan kuota di. Referensi Umum AWS Untuk mengaktifkan FIPS untuk titik akhir SFTP-enabled server, lihat. Buat SFTP-enabled server Untuk mengaktifkan FIPS untuk titik akhir FTPS-enabled server, lihat. Buat FTPS-enabled server Untuk mengaktifkan FIPS untuk titik akhir FTP-enabled server, lihat. Buat FTP-enabled server	12 Agustus 2020
Peningkatan panjang karakter nama pengguna dan karakter tambahan yang diizinkan	Nama pengguna sekarang dapat berisi tanda (@) dan periode (.), dan dapat memiliki panjang maksimum 100 karakter. Untuk menambahkan pengguna, lihat Mengelola pengguna untuk titik akhir server .	12 Agustus 2020

Ubah	Deskripsi	Date
Support untuk pembuatan peran Amazon CloudWatch logging AWS Identity and Access Management (IAM) otomatis	Transfer Family sekarang mendukung pembuatan otomatis peran IAM CloudWatch logging untuk melihat aktivitas pengguna akhir. Untuk informasi selengkapnya, lihat Buat SFTP-enabled server , Buat FTPS-enabled server , atau Buat FTP-enabled server .	30 Juli 2020
AWS Transfer Family sekarang mendukung Source IP sebagai faktor otorisasi.	Transfer Family menambahkan dukungan untuk menggunakan alamat IP sumber pengguna akhir sebagai faktor otorisasi, memungkinkan Anda untuk menerapkan lapisan keamanan tambahan saat mengotorisasi akses melalui Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), atau File Transfer Protocol (FTP). Untuk informasi selengkapnya, lihat Bekerja dengan penyedia identitas khusus .	9 Juni 2020

Ubah	Deskripsi	Date
AWS Transfer untuk SFTP sekarang AWS Transfer Family dan menambahkan dukungan untuk FTP dan FTPS.	Anda sekarang dapat menggunakan dua protokol tambahan untuk transfer file pengguna Anda: File Transfer Protocol Secure (FTPS) dan File Transfer Protocol (FTP). Pengguna dapat memindahkan, menjalankan, mengamankan, dan mengintegrasikan FTP melalui SSL (FTPS) dan alur kerja berbasis FTP plaintext AWS, di samping dukungan Secure File Transfer Protocol (SFTP) yang ada.	23 April 2020
Support untuk grup keamanan virtual private cloud (VPC) dan alamat IP Elastis	Anda sekarang dapat membuat daftar yang diizinkan untuk alamat IP yang masuk menggunakan grup keamanan, memberikan lapisan keamanan tambahan untuk server. Anda juga dapat mengaitkan alamat IP Elastis dengan titik akhir server Anda. Dengan melakukan ini, Anda dapat mengaktifkan pengguna di belakang firewall untuk mengizinkan akses ke titik akhir tersebut. Untuk informasi selengkapnya, lihat Buat server di cloud pribadi virtual .	10 Januari 2020

Ubah	Deskripsi	Date
Support untuk bekerja di VPC	Anda sekarang dapat membuat server di VPC. Anda dapat menggunakan server Anda untuk mentransfer data melalui klien Anda ke dan dari bucket Amazon S3 tanpa melalui internet publik. Untuk informasi selengkapnya, lihat Buat server di cloud pribadi virtual .	27 Maret 2019
Versi pertama yang AWS Transfer Family dirilis.	Rilis awal ini mencakup pengaturan arah, menjelaskan cara memulai, dan memberikan informasi tentang konfigurasi klien, konfigurasi pengguna, dan aktivitas pemantauan.	November 25, 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.