aws

Panduan Pengguna

AWS Terminal Transfer Data

AWS Terminal Transfer Data: Panduan Pengguna

Table of Contents

Apa itu Terminal Transfer Data? 1
Fitur 1
Konsep utama 2
Tim transfer 2
Personil 3
Fasilitas 3
Pertimbangan penjadwalan 3
Kasus penggunaan 4
Layanan terkait 4
Persyaratan Teknis 6
Peralatan 6
Persyaratan jaringan 6
Optimalisasi kinerja 7
Informasi selengkapnya 8
Memulai 9
Mendaftar untuk AWS akun 9
Jadwalkan reservasi 10
Buat tim Transfer 10
Memperbarui tim Transfer di akun Terminal Transfer Data Anda 11
Tambahkan personel 11
Memperbarui personel di akun Terminal Transfer Data Anda 12
Tentukan detail reservasi 13
Tinjau dan konfirmasi reservasi Anda 14
Membuat perubahan pada reservasi Anda 14
Lakukan transfer data 16
Apa yang harus dibawa 16
Alamat fisik fasilitas Terminal Transfer Data 16
Mengakses gedung 17
Peralatan yang diharapkan dalam rangkaian Terminal Transfer Data. 17
Memecahkan masalah koneksi jaringan 18
Masalah koneksi peralatan 18
Pemecahan masalah konektivitas 18
Linux/UNIX 19
Windows 20

Throughput jaringan 20
Keamanan 22
Perlindungan data 23
Enkripsi data 24
Enkripsi saat bergerak 24
Manajemen kunci 25
Inter-network privasi lalu lintas 25
Manajemen identitas dan akses 25
Audiens 25
Mengautentikasi dengan identitas 26
Mengelola akses menggunakan kebijakan 30
Cara kerja Terminal Transfer Data dengan IAM 33
Validasi kepatuhan 48
Ketahanan 49
CloudTrail log 50
Informasi Terminal Transfer Data di CloudTrail 50
Memahami entri file log Terminal Transfer Data 51
Keamanan Infrastruktur 52
Riwayat dokumen 53
..... liv

Apa itu Terminal Transfer Data?

AWS Terminal Transfer Data adalah lokasi fisik yang siap jaringan Anda dapat membawa perangkat penyimpanan data Anda untuk transfer data cepat ke dan dari layanan AWS Cloud Anda. Unggah data yang diambil dari jarak jauh untuk mempermudah akses data yang diambil dari jarak jauh.

Jadwalkan reservasi di salah satu fasilitas Terminal Transfer Data fisik kami dari AWS Management Console, tiba pada waktu yang dijadwalkan, dan unggah data Anda ke layanan AWS Cloud Anda dengan perangkat Anda sendiri. Setelah reservasi terjadwal Anda selesai dan Anda pergi, fasilitas diamankan kembali dan disiapkan untuk reservasi terjadwal berikutnya.

> **Note**
>
> AWS Terminal Transfer Data hanya tersedia untuk pelanggan Dukungan AWS Perusahaan saat ini. Jika Anda bukan pelanggan Dukungan Perusahaan dan ingin akses, hubungi AWS Dukungan.

Untuk mengakses Terminal Transfer Data:

- AWS Konsol Terminal Transfer Data: https://console.aws.amazon.com/datatransferterminal
- Fasilitas Terminal Transfer Data: Lokasi fasilitas Terminal Transfer Data disediakan setelah reservasi dilakukan di konsol. Untuk informasi selengkapnya, lihat Mel akukan transfer data.

Fitur

Menggunakan Terminal Transfer AWS Data membuat data Anda masuk ke layanan AWS Cloud Anda lebih mudah dari lokasi terpencil. Berikut ini adalah beberapa keunggulan Terminal Transfer Data untuk kebutuhan upload data jarak jauh Anda:

Aman, pribadi, dan eksklusif

Setiap fasilitas Terminal Transfer Data adalah lokasi pribadi yang aman bagi Anda untuk melakukan transfer data besar antara perangkat penyimpanan data Anda dan AWS layanan Anda melalui koneksi jaringan yang cepat.

Konsol reservasi khusus

Tambahkan personel yang disetujui ke tim Transfer Anda dan jadwalkan reservasi Terminal Transfer AWS Data menggunakan konsol Terminal Transfer Data.

Koneksi jaringan serat optik

Setiap fasilitas Terminal Transfer Data mencakup dua koneksi serat optik () 100 Gigabit (Gbps) untuk pengunggahan dan redundansi data yang cepat. LR4

Kontrol perangkat penyimpanan data Anda

Tidak perlu mengirimkan perangkat Snowball Anda dan menunggu data Anda diunggah ke layanan Cloud Anda AWS . Anda mengontrol perangkat penyimpanan data fisik Anda di seluruh proses transfer data, mendapatkan data Anda di tempat yang dibutuhkan lebih cepat.

Konsep utama

Menggunakan Terminal Transfer AWS Data mengharuskan pemilik Proses untuk menjadwalkan reservasi untuk spesialis transfer data untuk mengakses fasilitas Terminal Transfer Data. Lihat bagian berikut untuk mempelajari lebih lanjut tentang terminologi Terminal Transfer Data.

Topik

- Tim transfer
- Personil
- Fasilitas

Tim transfer

Tim Transfer adalah pengelompokan personel yang ditentukan oleh pemilik AWS akun yang dapat dipilih untuk melakukan transfer data atas nama organisasi Anda. Menyiapkan tim Transfer termasuk memberi nama tim Transfer dan menentukan personel untuk tim. Kami merekomendasikan grup yang terdiri dari empat atau lebih sedikit spesialis transfer data untuk satu reservasi.

Untuk informasi selengkapnya, lihat Menjadwalkan reservasi Terminal Transfer Data.

Personil

Personil mengacu pada individu yang dapat membuat dan mengelola reservasi atau dapat pergi ke dan menggunakan fasilitas Terminal Transfer Data. Personil dapat berupa pemilik Proses atau spesialis transfer data atau keduanya.

Pemilik proses

- Pemilik Proses adalah pemilik AWS akun yang dapat menambah, mengedit, dan menghapus personel dari akun Terminal Transfer AWS Data mereka.

Spesialis transfer data

- Spesialis transfer data adalah individu yang dapat pergi ke fasilitas Terminal Transfer Data untuk transaksi upload data. Personil ini harus diberi wewenang oleh pemilik Proses dan ditambahkan ke akun Terminal Transfer AWS Data Anda. Saat mengakses fasilitas Terminal Transfer Data, ID yang dikeluarkan pemerintah akan diperlukan.

Fasilitas

Fasilitas Terminal Transfer Data adalah hub data, dimiliki bersama dan dikelola oleh satu atau lebih penyedia layanan. Setiap fasilitas mewajibkan spesialis transfer data Terminal Transfer Data untuk memberikan bukti identitas yang dikeluarkan pemerintah yang harus sesuai dengan catatan reservasi mereka untuk mengakses paket Terminal Transfer Data.

Pertimbangan penjadwalan

Pemesanan dapat dilakukan di konsol Terminal Transfer Data selama satu hingga enam jam, untuk setiap hari dalam seminggu, sepanjang tahun. Pemesanan individu dapat dijadwalkan secara berurutan, dengan pemisahan minimal satu jam antar reservasi. Semua pemesanan harus dilakukan setidaknya 24 jam sebelumnya.

Jumlah waktu yang dibutuhkan untuk melakukan transfer data bervariasi tergantung pada kecepatan kinerja upload. Pertimbangkan faktor-faktor berikut yang memengaruhi kinerja pengunggahan saat Anda merencanakan dan menjadwalkan reservasi Terminal Transfer Data Anda.

Peralatan

- Beberapa peralatan mungkin menyertakan pengaturan yang dapat memengaruhi kinerja unggahan. Lihat spesifikasi peralatan Anda untuk kecepatan kinerja unggahan yang disarankan.

Kondisi jaringan

- Waktu lalu lintas jaringan yang padat akan memengaruhi kecepatan unggah data dan harus dipertimbangkan saat memilih waktu untuk sesi transfer data Anda. Merencanakan sesi transfer data Anda untuk jam-jam di luar sibuk atau selama waktu aktivitas jaringan yang lebih sedikit dapat meningkatkan kecepatan unggah Anda.

Ukuran transfer data

- Konektivitas jaringan Terminal Transfer Data dirancang untuk transfer data yang besar. Namun, ukuran data yang ditransfer akan berdampak pada berapa lama sesi berlangsung.

Kasus penggunaan

Meskipun setiap pelanggan Dukungan AWS Perusahaan dapat mengakses sistem Terminal Transfer Data, skenario kasus penggunaan tertentu mungkin mendapatkan manfaat yang lebih besar darinya.

Pengemudi Otonom dan Sistem Bantuan Pengemudi Lanjutan (AD/ADAS): Produsen Peralatan Asli Otomotif (OEM) dan pemasok menghasilkan kumpulan data besar dari armada kendaraan otonom mereka yang beroperasi dan mengumpulkan data di berbagai metro di Amerika Utara, Eropa, dan ASEAN. Dengan Terminal Transfer Data, data yang dikumpulkan oleh kendaraan armada ini dapat diunggah ke layanan AWS Cloud dan digunakan untuk melatih AD/ADAS model.

Media dan Hiburan: Studio dan pembuat konten lainnya sering menghasilkan file video dan audio digital (AV) di lokasi terpencil. Adalah penting bahwa file-file AV ini diunggah ke cloud secara tepat waktu sehingga tim produksi dan pengeditan yang tersebar secara geografis dapat memulai alur kerja secara paralel dan real-time. Dengan menggunakan Terminal Transfer Data untuk mengunggah data dari jarak jauh, jadwal produksi dapat dipersingkat, diterjemahkan ke dalam pengurangan biaya produksi.

Peta, Fotogrametri, dan citra 3D: Organisasi yang bekerja dengan aplikasi pemetaan atau citra mengumpulkan data di lokasi terpencil dan perlu mengunggah file visual ini ke AWS Cloud untuk analisis atau pelatihan. Terminal Transfer Data meminimalkan waktu antara mengumpulkan dan menganalisis kumpulan data besar ini, yang membantu menjaga data geospasial tetap mutakhir untuk pengemudi, petani, dan pengguna lain dari informasi tersebut.

Layanan terkait

AWS Layanan berikut memberikan pengalaman yang optimal saat menggunakan Terminal Transfer Data.

AWS layanan	Deskripsi
AWS Tepi Snowball	AWS Terminal Transfer Data melengkapi produk Snowball dengan menyediakan lokasi untuk mengunggah lebih cepat ke cloud AWS Anda, meminimalkan waktu tunggu untuk mengakses data Anda.
Amazon S3	Bawa perangkat Anda sendiri ke Terminal Transfer Data untuk mengunggah data Anda dengan cepat dan aman ke layanan Amazon S3 Anda.

Persyaratan teknis untuk menggunakan Terminal Transfer Data

Sebelum menjadwalkan reservasi di Terminal Transfer Data, Anda harus memastikan Anda memiliki peralatan dan konfigurasi yang diperlukan untuk terhubung ke jaringan. Lihat panduan berikut untuk konektivitas dan pengalaman jaringan yang optimal.

Peralatan

Anda harus membawa perangkat portabel untuk konektivitas termasuk monitor, keyboard, mouse, dan komputer atau laptop ke fasilitas Terminal Transfer Data untuk reservasi terjadwal Anda.

Perangkat keras Anda harus dapat bekerja dengan koneksi serat optik (L4)

> **Note**
>
> Sebagai praktik terbaik keamanan data, pastikan bahwa data Anda dienkripsi dan diamankan pada perangkat penyimpanan yang Anda bawa ke Terminal Transfer Data, dan bahwa Anda menerapkan kebijakan enkripsi data saat menggunakan fasilitas Terminal Transfer Data. Untuk informasi selengkapnya, lihat Keamanan Terminal Transfer AWS Data

Persyaratan jaringan

Pastikan perangkat upload, server, atau alat (laptop) Anda siap untuk terhubung ke jaringan dan mendukung DHCP. Anda harus memiliki yang berikut untuk mengunggah data:

- Transceiver QSFP optik 100G QSFP28 LR4 (100GBASE-LR4), kompatibel dengan konektor NIC dan LC untuk koneksi kabel serat yang disediakan di fasilitas Terminal Transfer Data.
- Konfigurasi otomatis alamat IP DHCP diaktifkan. Server DNS secara otomatis ditetapkan oleh DHCP.
- Up-to-date perangkat lunak dan driver NIC.

Optimalisasi kinerja

Untuk memaksimalkan throughput saat menggunakan Terminal Transfer AWS Data, pertimbangkan rekomendasi berikut.

- Perangkat keras yang disarankan:
  - Kartu antarmuka jaringan 100 Gbps
  - CPU 16-inti
  - 128GB RAM
  - beberapa drive SSD NVME dalam array RAID
- Gunakan pustaka Com AWS mon Runtime (AWS CRT) untuk upload menggunakan AWS Command Line Interface atau AWS SDK.

  Optimalkan pengaturan transfer Amazon S3 dengan mengonfigurasi parameter di bawah ini. Tetapkan nilai-nilai ini di bawah `s3` kunci tingkat atas di file AWS konfigurasi, lokasi default `~/.aws/config`.

  ```
  [default]
  s3 =
      preferred_transfer_client = crt
      target_bandwidth = 100Gb/s
      max_concurrent_requests = 20
      multipart_chunksize = 16MB
  ```

  Perhatikan bahwa semua nilai konfigurasi Amazon S3 diindentasi dan bersarang di bawah tombol tingkat `s3` atas.

  - Opsional: Anda dapat mengatur nilai-nilai di atas secara terprogram menggunakan perintah`aws configure set`. Misalnya, untuk mengatur nilai di atas untuk profil default, Anda dapat menjalankan perintah berikut sebagai gantinya:

    ```
    aws configure set default.s3.preferred_transfer_client crt
    aws configure set default.s3.target_bandwidth 100Gb/s
    aws configure set default.s3.max_concurrent_requests 20
    aws configure set default.s3.multipart_chunksize 16MB
    ```
- Untuk mengatur nilai-nilai ini secara terprogram untuk profil selain default, berikan tanda. `--profile` Misalnya, untuk mengatur konfigurasi untuk profil bernama`test-profile`, perintah runa seperti contoh di bawah ini.

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- Aktifkan BBR (Linux) pada perangkat untuk throughput yang lebih baik.

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

Informasi selengkapnya

Untuk informasi selengkapnya tentang konfigurasi baris AWS perintah Amazon S3 untuk mengoptimalkan konektivitas dan kinerja jaringan Anda, lihat sumber daya berikut.

- AWS Konfigurasi CLI Amazon S3 dalam Referensi Per AWS intah CLI
- Gunakan klien Amazon S3 berkinerja: AWS CRT-based klien di Amazon S3Amazon SDK untuk Java AppStream
- Bagaimana cara mengoptimalkan kinerja saat menggunakan AWS CLI untuk mengunggah file besar ke Amazon S3? di Pusat Peng AWS etahuan

Memulai

Mulailah melakukan transfer data jarak jauh ke layanan AWS Cloud Anda dengan melakukan reservasi di salah satu fasilitas Terminal Transfer Data. Untuk memulai, Anda memerlukan peralatan yang didukung oleh fasilitas Terminal Transfer Data dan akun Dukungan AWS Perusahaan.

Tinjau persyaratan teknis untuk menggunakan Terminal Transfer Data pada panduan ini sebelum menjadwalkan reservasi Terminal Transfer Data untuk memastikan Anda memiliki peralatan dengan konfigurasi optimal untuk transfer data. Tidak semua perangkat penyimpanan data dan peralatan koneksi jaringan kompatibel dengan koneksi jaringan serat optik yang tersedia di suite.

Saat Anda mendaftar AWS, AWS akun Anda secara otomatis terdaftar untuk semua layanan di AWS, termasuk Terminal Transfer Data. Anda hanya membayar biaya layanan yang Anda gunakan.

Untuk mengatur Terminal Transfer Data, gunakan langkah-langkah di bagian berikut.

Saat mendaftar AWS dan mengatur Terminal Transfer Data, Anda dapat secara opsional mengubah bahasa tampilan di Konsol AWS Manajemen. Untuk informasi selengkapnya, lihat Meng ubah bahasa Konsol AWS AWS Manajemen di Panduan Memulai Konsol Manajemen.

Setelah Anda memiliki AWS akun, Anda dapat mengakses Terminal Transfer Data. Untuk informasi selengkapnya tentang menyiapkan dan menggunakan Terminal Transfer AWS Data, lihat Men jadwalkan reservasi Terminal Transfer Data.

Mendaftar untuk AWS akun

Untuk memulai AWS, Anda memerlukan AWS akun. Untuk informasi tentang membuat AWS akun, lihat Memulai dengan AWS akun di Panduan Referensi Manajemen AWS Akun.

Jadwalkan reservasi Terminal Transfer Data

Untuk mulai menggunakan Terminal Transfer AWS Data, Anda harus memiliki AWS akun dan masuk ke konsol Terminal Transfer Data Anda di https://console.aws.amazon.com /datatransferterminal. Setelah Anda masuk ke konsol Terminal Transfer Data, Anda dapat melihat reservasi yang ada atau membuat yang baru. Untuk menjadwalkan reservasi, Anda harus melakukan hal berikut:

1. Buat tim Transfer. Anda perlu membuat grup pengguna yang ditunjuk untuk membuat reservasi dan mengakses fasilitas Terminal Transfer Data untuk melakukan transfer data. Untuk mempelajari lebih lanjut tentang topik ini, lihat Membuat tim Transfer.
2. Setelah tim Anda diatur, Anda perlu menambahkan personel ke dalamnya. Untuk mempelajari selengkapnya tentang menambahkan personel ke tim Transfer Anda, lihat Menambahkan personel.
3. Pemilik Proses dapat menjadwalkan transfer data dengan tim di akun. Untuk informasi selengkapnya tentang cara menjadwalkan reservasi, lihat Menentukan detail reservasi.
4. Pastikan bahwa rincian reservasi sudah benar sebelum mengirimkan permintaan Anda. Setelah dikirimkan, permintaan reservasi tidak dapat diubah setidaknya selama 24 jam. Untuk informasi selengkapnya, lihat Tinjau dan konfirmasi reservasi Anda.

Setelah reservasi Anda diproses dan dikonfirmasi, tim Transfer Anda akan dapat mengakses fasilitas Terminal Transfer Data pada waktu yang dijadwalkan. Untuk informasi selengkapnya, lihat Melakukan transfer data di fasilitas Terminal Transfer Data.

Buat tim Transfer

Untuk mengakses fasilitas Terminal Transfer Data, Anda harus menjadwalkan reservasi di AWS Management Console. Masuk ke AWS akun Anda untuk mengakses konsol Terminal Transfer Data dan selesaikan langkah-langkah berikut untuk menjadwalkan reservasi Anda.

1. Dari halaman beranda Terminal Transfer Data, pilih tombol Mulai.
2. Jika Anda belum menyiapkan tim Transfer di akun Anda, tombol Buat reservasi akan dinonaktifkan. Anda harus membuat dan memberi nama tim Transfer untuk memulai.
   a. Pilih tombol Create Transfer team.
   b. Beri nama tim.

- Nama harus antara dua dan 64 karakter, dimulai dengan huruf atau angka.
- Hanya gunakan huruf, angka, titik, dan tanda hubung. Karakter khusus tidak dikenali.
- Jangan sertakan informasi identifikasi yang sensitif.

c. Buat deskripsi tim Transfer.

- Berikan deskripsi yang membantu mengidentifikasi tim, seperti menjelaskan tujuan tim untuk periode waktu, kampanye, atau proyek tertentu.

d. Pilih tombol Create Transfer team.

Anda akan dikembalikan ke halaman tim Transfer dan tim Anda yang baru dibuat akan muncul di bawah bagian Tim transfer.

Memperbarui tim Transfer di akun Terminal Transfer Data Anda

Untuk menyiapkan tim Transfer baru, lihat bagian Jadwalkan reservasi Terminal Transfer Data pada panduan ini.

Untuk mengubah atau menghapus tim Transfer, lakukan hal berikut:

1. Pada halaman Tim transfer, pilih tim Transfer yang ingin Anda ubah.
2. Untuk mengubah nama dan deskripsi tim Transfer, pilih tombol Edit.
3. Untuk menambah atau menghapus personel, pilih tab personel dan selesaikan langkah-langkah yang dijelaskan dalam Bagaimana cara memodifikasi, menambah, atau menghapus personel dari akun saya? bagian dari FAQ ini.
4. Untuk menambah atau membatalkan reservasi untuk tim Transfer yang dipilih, lihat bagian Personel Pembaruan di akun Terminal Transfer Data Anda di FAQ ini.

Tambahkan personel

Tambahkan pemilik Proses dan spesialis transfer data ke tim Transfer Anda untuk mengatur transfer data dan mengakses fasilitas Terminal Transfer Data. Untuk menambahkan personel ke tim Transfer Anda, lakukan hal berikut:

1. Pada halaman Tim transfer, pilih kartu tim Transfer yang diinginkan dari yang tercantum di bagian Tim transfer. Halaman ringkasan tim Transfer akan muncul.
2. Pilih tab Personil, lalu tombol Daftarkan orang untuk menambahkan personel ke tim Transfer.

3. Lengkapi kolom dengan informasi yang diperlukan tentang orang yang Anda tambahkan ke tim Transfer di halaman Daftar personel.
   a. Alias personel: Buat alias unik untuk mengidentifikasi orang tersebut.
      - Alias digunakan untuk mengidentifikasi personel sekaligus melindungi identitas mereka.
      - Panjangnya bisa mencapai 64 karakter dan termasuk huruf, angka, dan tanda hubung.
      - Karakter khusus tidak diizinkan.
   b. Nama depan: Berikan nama depan orang tersebut seperti yang tertera pada identifikasi yang dikeluarkan pemerintah mereka.
   c. Nama belakang: Berikan nama belakang atau nama keluarga orang tersebut yang muncul di identifikasi yang dikeluarkan pemerintah mereka.
   d. Alamat email: Sertakan alamat email yang baik bagi orang tersebut untuk menerima informasi reservasi dan instruksi untuk mengakses fasilitas Terminal Transfer Data.
4. Pilih tombol Daftar orang untuk menyelesaikan penambahan orang tersebut ke tim Transfer Anda.

Memperbarui personel di akun Terminal Transfer Data Anda

Memodifikasi personel yang ada di akun Anda di konsol Terminal Transfer Data saat ini tidak didukung. AWS Pemilik Proses Terminal Transfer Data hanya dapat menambah atau menghapus personel saat ini.

Untuk menghapus personel dari akun Terminal Transfer Data Anda, lakukan hal berikut:

1. Pada halaman Tim transfer, pilih tim Transfer yang terkait dengan personel yang ingin Anda hapus.
2. Pada halaman ringkasan tim Transfer yang dipilih, pilih tab personel.
3. Klik tombol radio di sebelah alias yang ingin Anda hapus. Perhatikan bahwa Anda hanya akan dapat melihat alias orang tersebut saat menghapus profil mereka.
4. Pilih tombol Hapus. Peringatan akan muncul untuk mengkonfirmasi tindakan yang dimaksudkan untuk personel yang dipilih. Klik tombol Hapus untuk melanjutkan. Spanduk akan muncul di bagian atas konsol yang mengonfirmasi bahwa personel berhasil dihapus.

Tentukan detail reservasi

Petunjuk berikut memandu Anda melalui cara menjadwalkan reservasi Terminal Transfer Data di Konsol AWS Manajemen. Untuk informasi tentang penggunaan fasilitas Terminal Transfer Data, lihat Melakukan transfer data.

1. Pilih tombol Buat reservasi di tab Reservasi Men datang.
2. Lengkapi kolom pada halaman T entukan detail reservasi.
   a. Pemilihan tim transfer: Tim Transfer yang dipilih sebagai default muncul terlebih dahulu. Jika Anda ingin memilih tim yang berbeda, klik panah drop-down untuk memilih dari daftar tim Transfer yang tersedia.
   b. Pemilik proses: Pilih alias personel yang ingin Anda tanggung jawab untuk mengelola reservasi.
      - Hanya satu pemilik Proses yang diizinkan untuk melakukan reservasi dan mereka harus menjadi personel resmi di AWS akun Anda.

        Pemilik Proses dapat dimasukkan sebagai salah satu spesialis transfer data untuk melakukan aktivitas transfer data juga.
   c. Spesialis transfer data: Pilih personel yang ingin Anda akses ke fasilitas Terminal Transfer Data untuk menyelesaikan aktivitas transfer data. Anda dapat memilih lebih dari satu personel, sesuai kebutuhan.
      - Praktik terbaik adalah membatasi tim Transfer Anda menjadi tidak lebih dari empat (4) spesialis transfer data.
   d. Informasi Terminal Transfer Data: Tentukan fasilitas Terminal Transfer Data, tanggal yang diinginkan, dan waktu spesifik untuk sesi transfer data.
      i. Fasilitas Terminal Transfer Data: Klik panah drop-down untuk memilih fasilitas Terminal Transfer Data.

         > **Note**
         >
         > Hanya deskripsi fasilitas yang akan diberikan saat melakukan reservasi. Informasi lokasi tambahan akan diberikan dalam email konfirmasi reservasi.

      ii. Tanggal dan waktu Terminal Transfer Data: Klik ke kolom Cari tanggal dan waktu untuk reservasi Anda untuk melihat kalender dan menjadwalkan reservasi Anda.

- Pemesanan harus dilakukan minimal 24 jam sebelumnya dan tidak lebih dari enam (6) bulan dan hanya bisa maksimal 48 jam. Satu reservasi dapat berlangsung lebih dari satu hari untuk memperhitungkan skenario bermalam, jika perlu.
- Waktu ditunjukkan menggunakan jam 24 jam dan hanya dapat dipesan dalam penambahan satu jam penuh.
- Untuk melakukan reservasi berturut-turut, Anda harus membuat reservasi terpisah dengan setidaknya satu jam antara setiap sesi transfer data.
- Untuk informasi selengkapnya, lihat Pertimbangan penjadwalan.

3. Konfirmasikan detail reservasi sudah benar dan kemudian pilih tombol Buat untuk melanjutkan. Ini akan membawa Anda ke halaman konfirmasi, yang menyediakan ringkasan reservasi Anda.

Tinjau dan konfirmasi reservasi Anda

Setelah menentukan detail reservasi Anda, pilih tombol Berikutnya untuk melanjutkan melihat halaman ikhtisar. Tinjau detail permintaan reservasi Terminal Transfer Data Anda di halaman Ulasan dan buat.

- Jika Anda puas dengan permintaan tersebut, pilih tombol Buat.
- Jika Anda perlu mengubah reservasi Anda, pilih tombol Sebelumnya.

Setelah permintaan reservasi diajukan, pemilik Proses akan menerima email yang mengonfirmasi bahwa permintaan telah diterima dan sedang diproses. Setelah permintaan disetujui, email lain akan mengkonfirmasi reservasi dan memberikan instruksi untuk menemukan dan mengakses fasilitas Terminal Transfer Data. Untuk informasi tentang mengakses fasilitas Terminal Transfer Data, lihat Melakukan transfer data.

Membuat perubahan pada reservasi Anda

Ada periode pemrosesan 24 jam sebelum perubahan dapat dilakukan pada permintaan reservasi Terminal Transfer Data Anda.

Setelah periode pemrosesan, untuk melihat, mengedit, atau menghapus reservasi Anda, buka halaman Tim transfer di konsol.

1. Cari dan pilih reservasi yang diinginkan pada kartu tim.
2. Klik menu Tindakan dan pilih tindakan yang diinginkan.

- Melihat: Memilih opsi tampilan memungkinkan Anda untuk melihat detail reservasi Anda termasuk tanggal, waktu, lokasi, dan personel yang ditugaskan.
- Sunting: Anda dapat merevisi detail reservasi termasuk tanggal, waktu, lokasi, dan personel yang ditugaskan. Perhatikan bahwa perubahan harus dilakukan 24 jam sebelum tanggal reservasi yang diinginkan dan bahwa revisi tidak segera diterima dan diterapkan. Pemilik Proses Anda akan menerima konfirmasi atas permintaan yang diperbarui.
- Hapus: Opsi hapus memungkinkan Anda untuk membatalkan reservasi Anda. Permintaan pembatalan harus dilakukan minimal 24 jam sebelum tanggal reservasi yang dijadwalkan. Pemilik Proses akan menerima konfirmasi reservasi yang dibatalkan ketika permintaan disetujui.

Melakukan transfer data di fasilitas Terminal Transfer Data

Terminal Transfer Data adalah lokasi yang aman dan dimiliki bersama yang menyediakan akses aman ke AWS jaringan. Untuk mengakses fasilitas Terminal Transfer Data, pastikan Anda memiliki email konfirmasi dengan deskripsi lokasi dan petunjuk akses. Lihat topik di bawah ini untuk informasi lebih lanjut tentang mengakses dan menggunakan fasilitas Terminal Transfer Data.

Topik

- Apa yang harus dibawa
- Alamat fisik fasilitas Terminal Transfer Data
- Mengakses gedung
- Peralatan yang diharapkan dalam rangkaian Terminal Transfer Data.

Apa yang harus dibawa

Spesialis transfer data harus membawa item yang diperlukan untuk melakukan transfer data, seperti komputer laptop, flash drive, Solid State Drives (SSDs), dan AWS Snowball Edge. Pastikan peralatan Anda dioptimalkan untuk menggunakan kabel jaringan serat di fasilitas Terminal Transfer Data. Untuk informasi selengkapnya tentang peralatan dan konfigurasi optimal, lihat Persyaratan teknis untuk menggunakan Terminal Transfer Data.

Anda bertanggung jawab atas pemasangan, penggunaan, dan penghapusan peralatan dan barang yang Anda dan spesialis transfer Data yang menyertainya bawa ke fasilitas Terminal Transfer Data. Apa pun yang dibawa ke suite harus dihapus saat pergi. AWS Terminal Transfer Data tidak bertanggung jawab atas barang yang terlupakan atau hilang.

Alamat fisik fasilitas Terminal Transfer Data

Alamat fisik untuk fasilitas Terminal Transfer Data tidak akan diberikan. Sebagai gantinya, pemilik Proses dan spesialis transfer Data yang ditentukan dalam reservasi akan menerima email dengan nama publik yang dapat dicari dari fasilitas Terminal Transfer Data. AWS Data Transfer Terminal menggunakan sistem identifikasi lokasi yang sama dengan AWS Direct Connect sehingga Anda dapat mencari nama publik di internet untuk menemukan fasilitas Terminal Transfer Data. Jika Anda tidak memiliki email dengan informasi ini, konfirmasikan dengan manajer akun Terminal Transfer AWS Data Anda bahwa Anda termasuk dalam tim Transfer dan bahwa informasi email Anda benar.

Mengakses gedung

Untuk mengakses fasilitas Terminal Transfer Data, setiap spesialis transfer Data harus memberikan bukti identitas atau ID yang dikeluarkan pemerintah. Setelah masuk ke gedung, keamanan akan mengantar Anda ke suite Terminal Transfer Data Anda.

Peralatan yang diharapkan dalam rangkaian Terminal Transfer Data.

Setiap fasilitas Terminal Transfer Data hanya boleh memiliki dua (2) kabel serat optik, meja atau meja, dan kursi. Jika ada peralatan atau barang lain di dalam ruangan, segera laporkan ke Support.

Memecahkan masalah koneksi jaringan

Jika Anda mengalami masalah saat terhubung ke jaringan saat menggunakan Terminal Transfer AWS Data, seperti tidak dapat menghubungkan internet atau kecepatan koneksi yang lambat, pertimbangkan tips pemecahan masalah berikut.

Topik

- Masalah koneksi peralatan
- Pemecahan masalah konektivitas
- Throughput jaringan

Masalah koneksi peralatan

Jika Anda mengalami kesulitan membuat koneksi fisik saat berada di rangkaian Terminal Transfer Data, pertimbangkan hal berikut:

- Setiap fasilitas Terminal Transfer Data akan memiliki dua (2) kabel serat LC mode tunggal. Jika salah satu atau kedua kabel ini hilang, segera hubungi AWS Support.
- Jika salah satu kabel serat optik tidak berfungsi, coba gulung kabel terlebih dahulu. Jika Anda masih tidak dapat terhubung dengan kabel pertama, coba gunakan kabel lainnya.

Jika Anda masih tidak dapat menggunakan kabel untuk terhubung, segera hubungi AWS Support.

Pemecahan masalah konektivitas

Jika Anda dapat menghubungkan peralatan Anda tetapi tidak dapat terhubung ke jaringan, coba saran pemecahan masalah berikut.

- Konfirmasikan bahwa konfigurasi peralatan Anda memenuhi persyaratan jaringan yang ditentukan. Untuk informasi selengkapnya, lihat Persyaratan teknis untuk menggunakan Terminal Transfer Data
- Beralih ke kabel serat optik lainnya untuk terhubung.
- Nyalakan ulang perangkat Anda sambil menjaga kabel serat optik tetap terhubung.
- Lakukan diagnostik jaringan dasar pada perangkat untuk memastikan hal berikut:
  - DHCP diaktifkan

- Alamat IP ditetapkan ke antarmuka jaringan yang terhubung
- Server DNS dikonfigurasi
- Jam sistem disinkronkan dengan NTP

Jika Anda masih tidak dapat terhubung, hubungi AWS Support dan berikan output berikut kepada mereka tergantung pada sistem operasi (OS) apa yang berjalan di perangkat Anda.

Linux/UNIX

- Dapatkan alamat IP dan informasi perutean di terminal atau antarmuka baris perintah (CLI). Verifikasi bahwa alamat IP ditetapkan ke antarmuka jaringan, dan rute default dengan alamat gateway default ditambahkan dalam tabel rute.

```
ip address show
ip route show
```

  - Atau, jika `iproute2` tidak diinstal pada perangkat dan `ip` perintah tidak tersedia, gunakan perintah berikut:

```
ifconfig
netstat -rn
```

- Kumpulkan informasi server DNS. Ini harus menunjukkan dua alamat IP yang dimulai dengan `nameserver` kata kunci.

```
cat /etc/resolv.conf
```

- Kumpulkan output dari tes konektivitas dasar. Ganti `default_gateway_address` dengan alamat IP gateway default yang ditetapkan.

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- Kumpulkan output dari tes konektivitas HTTPS. Perintah berikut harus menunjukkan `HTTP 200` OK respons dari Amazon S3.

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- Dapatkan alamat IP, perutean, dan informasi server DNS di prompt perintah. Verifikasi bahwa alamat IP ditetapkan ke antarmuka jaringan, dua server DNS ditetapkan, dan rute default dengan alamat gateway default ditambahkan dalam tabel rute.

```
ipconfig /all
route print
```

- Kumpulkan output dari tes konektivitas dasar di command prompt. Ganti `default_gateway_address` dengan alamat IP dari gateway default yang ditetapkan.

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- Kumpulkan output dari tes konektivitas HTTPS di PowerShell. Perintah berikut harus menunjukkan `HTTP 200 OK` respons.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

Throughput jaringan

Throughput jaringan, yang mengukur kecepatan transfer data aktual dalam jaringan, dapat dipengaruhi oleh berbagai faktor. Berikut ini dapat memengaruhi kecepatan transfer data Anda:

- Perangkat keras: Komponen perangkat keras perangkat dapat menyebabkan kecepatan koneksi berkurang saat mengunggah data. CPU dan disk yang digunakan dalam perangkat dapat mencapai batas kinerjanya. Pertimbangkan untuk menggunakan NVME SSDs dalam array RAID. Pastikan Anda menggunakan perpustakaan AWS CRT untuk kinerja yang lebih baik dan untuk menurunkan penggunaan CPU.
- Overhead enkripsi: Transmisi aman, seperti HTTPS, meningkatkan waktu pemrosesan karena overhead enkripsi.
- Latensi: Latensi mengacu pada waktu yang dibutuhkan untuk paket data untuk melakukan perjalanan dari sumber ke tujuan. Latensi tinggi dapat diamati saat mengunggah ke bucket Amazon S3 di wilayah geografis yang berbeda, yang dapat menyebabkan penundaan transfer data

dan throughput yang lebih rendah. Praktik terbaik adalah melakukan transfer data dalam wilayah yang sama, bila memungkinkan.

- Kehilangan paket: Paket yang hilang memerlukan transmisi ulang, memperlambat transfer data.

Keamanan dari AWS Terminal Transfer Data

AWS Terminal Transfer Data menyediakan lingkungan yang aman untuk melakukan transfer data ke dan dari AWS Cloud. Seperti koneksi serat jaringan fisik lainnya, koneksi Terminal Transfer Data tidak menyediakan enkripsi default. Oleh karena itu, Anda akan bertanggung jawab untuk menegakkan praktik terbaik enkripsi data untuk memastikan transfer data Anda aman.

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 AWS antara Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Terminal Transfer AWS Data, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Terminal Transfer Data. Topik berikut menunjukkan cara mengamankan data Anda saat menggunakan layanan Terminal Transfer Data. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Terminal Transfer Data Anda.

Topik

- Perlindungan data di AWS Terminal Transfer Data
- Identitas dan manajemen akses untuk Terminal Transfer Data
- Validasi kepatuhan untuk AWS Terminal Transfer Data
- Ketahanan di AWS Terminal Transfer Data
- Pencatatan dan pemantauan di Terminal Transfer Data

- Keamanan Infrastruktur di AWS Terminal Transfer Data

Perlindungan data di AWS Terminal Transfer Data

Model tanggung jawab AWS bersama berlaku untuk perlindungan AWS data di Terminal Transfer Data. 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. Anda juga bertanggung jawab atas 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 Tang AWS gung Jawab Bersama dan posting blog GDPR di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi kredenSIAL AWS akun dan mengatur pengguna individu dengan Pusat Identitas AWS IAM atau AWS Manajemen Identitas dan Akses (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Terminal Transfer Data atau AWS layanan lain

menggunakan konsol, API, AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data

AWS Terminal Transfer Data menyediakan akses ke koneksi jaringan berkecepatan tinggi bagi Anda untuk mentransfer data dengan aman antara sistem penyimpanan yang dikelola sendiri dan layanan AWS penyimpanan. Cara data penyimpanan Anda dienkripsi saat transit sebagian bergantung pada kebijakan yang diaktifkan pada perangkat Anda dan layanan ke mana data Anda ditransfer. Pengelolaan data dan enkripsi dalam transit adalah tanggung jawab individu yang menggunakan Terminal Transfer Data.

Enkripsi saat diam

AWS Terminal Transfer Data mengenkripsi semua data saat istirahat.

Terminal Transfer Data hanya menangkap data yang diperlukan untuk pemesanan termasuk nama depan dan belakang serta alamat email dari individu yang ditentukan untuk menghadiri dan menjadwalkan reservasi. Tujuan pengumpulan data ini adalah untuk mengkonfirmasi detail reservasi dan memastikan akses ke kamar untuk melakukan transfer data. Informasi transaksional ini dicadangkan tidak lebih dari 35 hari, namun informasi AWS akun disimpan selama 10 tahun.

Enkripsi saat bergerak

AWS Terminal Transfer Data tidak mengenkripsi data dalam transit. Data dienkripsi dalam perjalanan saat Anda berinteraksi dengan titik akhir API Terminal Transfer Data untuk menyiapkan tim Transfer, menambahkan personel, dan menjadwalkan reservasi di konsol. Sebagai bagian dari model tanggung jawab AWS bersama, Anda memiliki pilihan tentang bagaimana Anda terhubung ke AWS layanan melalui Terminal Transfer Data. Kami sangat menyarankan Anda memilih untuk terhubung ke AWS layanan menggunakan enkripsi dalam transit yang kuat, seperti TLS 1.2 dan 1.3.

Misalnya, gunakan hanya koneksi terenkripsi melalui HTTPS (TLS) dengan menggunakan SecureTransport kondisi aws: dalam kebijakan bucket Amazon S3 Anda, seperti yang diilustrasikan dalam kebijakan bucket di bawah ini.

Untuk mempelajari selengkapnya tentang enkripsi data saat transit dengan AWS layanan lain, seperti Amazon S3, lihat Melindungi data dengan enkripsi sisi server di Panduan Pengguna Amazon S3.

Manajemen kunci

AWS Terminal Transfer Data tidak secara langsung mendukung kunci yang dikelola Pelanggan. Gunakan dukungan kunci yang dikelola Pelanggan yang tersedia untuk AWS layanan yang Anda sambungkan selama reservasi Terminal Transfer Data. Pelajari lebih lanjut tentang kunci yang dikelola pelanggan dan cara mengenkripsi data Anda saat diam di bagian kunci AWS KMS pada Panduan Pengembang Layanan Manajemen Kunci. AWS

Inter-network privasi lalu lintas

Akses ke konsol Terminal Transfer Data adalah melalui API layanan yang diterbitkan. Sumber daya Terminal Transfer Data independen dari cloud pribadi virtual (VPC).

Identitas dan manajemen akses untuk Terminal Transfer Data

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan di otorisasi (memiliki izin) untuk menggunakan sumber daya Terminal Transfer Data. IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara kerja Terminal Transfer Data dengan IAM

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Terminal Transfer Data.

Pengguna layanan — Jika Anda menggunakan layanan Terminal Transfer Data untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredentif dan izin yang Anda butuhkan. Saat

Anda menggunakan lebih banyak fitur Terminal Transfer Data untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Terminal Transfer Data, lihat Memec ahkan AWS Masalah identitas dan akses Terminal Transfer Data.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Terminal Transfer Data di perusahaan Anda, Anda mungkin memiliki akses penuh ke Terminal Transfer Data. Adalah tugas Anda untuk menentukan fitur dan sumber daya Terminal Transfer Data mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Terminal Transfer Data, lihat Bagaimana Terminal Transfer Data bekerja dengan I AM.

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang bagaimana Anda dapat menulis kebijakan untuk mengelola akses ke Terminal Transfer Data. Untuk melihat contoh kebijakan berbasis identitas Terminal Transfer Data yang dapat Anda gunakan di IAM, lihat contoh Identity-based kebijakan untuk Terminal Transfer AWS Data.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredentif identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai pengguna root AWS akun, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredentif yang disediakan melalui sumber identitas. AWS Pengguna Pusat Identitas IAM (Pusat Identitas IAM), otentikasi masuk tunggal perusahaan Anda, dan kredentif Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Tergantung pada jenis pengguna Anda, Anda dapat masuk ke Konsol AWS Manajemen atau portal AWS akses. Untuk informasi selengkapnya tentang AWS masuk, lihat Cara masuk ke AWS akun Anda di Panduan AWS Sign-In Pengguna.

Jika Anda mengakses secara AWS terprogram, AWS menyediakan perangkat pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredenSIAL Anda. Jika Anda tidak menggunakan AWS

alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Multi-factor otentikasi di Panduan Pengguna Pusat Identitas AWS IAM dan AWS Multi-factor otentikasi di IAM di Panduan Pengguna IAM.

AWS pengguna root akun

Saat membuat AWS akun, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredenSIAL sementara.

Identi tas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, Layanan AWS Direktori, direktori Pusat Identitas, atau pengguna apa pun yang mengakses AWS layanan dengan menggunakan kredenSIAL yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses AWS akun, mereka mengambil peran, dan peran tersebut memberikan kredenSIAL sementara.

Untuk manajemen akses terpusat, sebaiknya gunakan Pusat Identi AWS tas IAM. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua AWS akun dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna Pusat Identitas AWS IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam AWS akun Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam AWS akun Anda yang memiliki izin tertentu. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk sementara mengambil peran IAM di Konsol AWS Manajemen, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL khusus. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang kumpulan izin, lihat Kumpulan izin di Panduan Pengguna Pusat Identitas AWS IAM.

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Cross-account akses — Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (kepala sekolah tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Cross-service akses — Beberapa AWS layanan menggunakan fitur di AWS layanan lain. Misalnya, saat Anda melakukan panggilan di layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Layanan mungkin melakukan ini menggunakan izin kepala panggil, menggunakan peran layanan, atau menggunakan peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai kepala sekolah. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari kepala sekolah yang memanggil AWS layanan, dikombinasikan dengan AWS layanan yang meminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan AWS layanan atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM.
  - Service-linked role — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di AWS akun Anda dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredenSIAL sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat permintaan

AWS CLI atau API. AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instance EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Gunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izin mereka. AWS mengevaluasi kebijakan ini ketika seorang kepala sekolah (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

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.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat dikategorikan lebih lanjut sebagai kebijakan sebaris atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di AWS akun Anda. Kebijakan terkelola mencakup kebijakan AWS terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah 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. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau AWS layanan.

Resource-based kebijakan adalah kebijakan sebaris 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 kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran

IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan kebijakan berbasis identitas entitas dan batas izinnya. Resource-based kebijakan yang menentukan pengguna atau peran di `Principal` bidang tidak dibatasi oleh batas izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) - SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organisasi. AWS Organisasi adalah layanan untuk mengelompokkan dan mengelola beberapa AWS akun secara terpusat yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk setiap pengguna root AWS akun. Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Kebijakan kontrol layanan di Panduan AWS Pengguna Organisasi.
- Kebijakan kontrol sumber daya (RCP) – RCP adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk pengguna root AWS akun, terlepas dari apakah mereka milik organisasi Anda. Untuk informasi selengkapnya tentang Organisasi dan RCP, termasuk daftar AWS layanan yang mendukung RCP, lihat Kebijakan kontrol sumber daya (RCP) di Panduan Pengguna AWS Organisasi.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah persimpangan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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 ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Cara kerja Terminal Transfer Data dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Terminal Transfer Data, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Terminal Transfer Data.

Fitur IAM	Dukungan Terminal Transfer Data
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin principal	Tidak
Peran layanan	Tidak
Service-linked peran	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Terminal Transfer Data dan AWS layanan lainnya bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk Terminal Transfer Data

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi

seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan prinsip dalam kebijakan berbasis identitas karena berlaku untuk pengguna atau peran yang dilampirkan. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk Terminal Transfer Data

Untuk melihat contoh kebijakan berbasis identitas Terminal Transfer Data, lihat contoh Identity-based kebijakan untuk Terminal Transfer AWS Data.

Resource-based kebijakan dalam Terminal Transfer Data

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah 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. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau AWS layanan.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam 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, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Terminal Transfer Data

Mendukung tindakan kebijakan: Ya

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. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Terminal Transfer Data, lihat Tindakan yang D itetapkan oleh Terminal Transfer AWS Data di Referensi Otorisasi Layanan.

Tindakan kebijakan di Terminal Transfer Data menggunakan awalan berikut sebelum tindakan:

```
datatransferterminal
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Terminal Transfer Data, lihat contoh Identity-based kebijakan untuk Terminal Transfer AWS Data.

Sumber daya kebijakan untuk Terminal Transfer Data

Mendukung sumber daya kebijakan: Ya

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. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, seperti operasi daftar, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Terminal Transfer Data dan ARN-nya, lihat Sumber Daya yang Ditet apkan oleh Terminal Transfer AWS Data di Refer ensi O torisasi Layanan. Untuk mempelajari tindakan mana Anda dapat menentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditetapkan oleh Terminal Transfer AWS Data.

Untuk melihat contoh kebijakan berbasis identitas Terminal Transfer Data, lihat contoh Identity-based kebijakan untuk Terminal Transfer AWS Data.

Kunci kondisi kebijakan untuk Terminal Transfer Data

Mendukung kunci kondisi kebijakan khusus layanan: Yes

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.

`Condition`Elemen (atau `Condition` *`block`*`) lets you specify conditions in which a statement is in effect. The `Condition` elemen adalah opsional. 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.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk kunci kondisi tunggal, AWS mengevaluasi

kondisi menggunakan 0R operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Terminal Transfer Data, lihat Kunci Kondisi untuk Terminal Transfer AWS Data di Referensi O torisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana Anda dapat menggunakan kunci kondisi, lihat Tindakan yang Ditetapkan oleh Terminal Transfer AWS Data.

Untuk melihat contoh kebijakan berbasis identitas Terminal Transfer Data, lihat contoh Identity-based kebijakan untuk Terminal Transfer AWS Data.

ACL di Terminal Transfer Data

Mendukung ACL: Tidak

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.

ABAC dengan Terminal Transfer Data

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang kebijakan ABAC untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengontrol akses berdasarkan tag, Anda memberikan informasi tag dalam elemen https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html kondisi kebijakan menggunakan `aws:ResourceTag/[replaceable]` nama kunci `` `, , or aws:TagKeys condition keys. `` Jika layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, maka nilainya adalah Ya untuk layanan. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial. Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredenSIAL sementara dengan Terminal Transfer Data

Mendukung kredensial sementara: Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredenSIAL sementara. Untuk informasi tambahan, termasuk AWS layanan mana yang bekerja dengan kredenSIAL sementara, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredenSIAL sementara jika masuk ke Konsol AWS Manajemen menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, saat Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses itu secara otomatis membuat kredenSIAL sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenSIAL sementara secara manual menggunakan AWS CLI atau AWS API. Anda kemudian dapat menggunakan kredenSIAL sementara tersebut untuk mengakses AWS. AWS merekomendasikan agar Anda secara dinamis membuat kredenSIAL sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Cross-service izin utama untuk Terminal Transfer Data

Mendukung sesi akses maju (FAS): Tidak

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan di AWS, Anda dianggap sebagai kepala sekolah. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin kepala sekolah yang memanggil AWS layanan, dikombinasikan dengan

AWS layanan yang meminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan AWS layanan atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Terminal Transfer Data

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di Panduan Pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Terminal Transfer Data. Edit peran layanan hanya jika Terminal Transfer Data memberikan panduan untuk melakukannya.

Service-linked peran untuk Terminal Transfer Data

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke layanan. AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di AWS akun Anda dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan layanan dalam tabel yang menyer `Yes` takan kolom Service-linked peran. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based Contoh kebijakan untuk AWS Terminal Transfer Data

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Terminal Transfer Data. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk

memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan di Refer ensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Terminal Transfer Data
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Terminal Transfer Data di akun Anda. Tindakan ini dapat menimbulkan biaya untuk AWS akun Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS ola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di AWS akun Anda. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus 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 kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui AWS layanan tertentu, seperti AWS 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 memerlukan pengguna IAM atau pengguna root di AWS akun 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 konsol Terminal Transfer Data

Untuk mengakses konsol Terminal Transfer AWS Data, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Terminal Transfer Data di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Terminal Transfer Data, lampirkan juga Terminal Transfer Data `ConsoleAccess` atau kebijakan ter `ReadOnly` AWS kelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna 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 secara terprogram menggunakan AWS CLI atau API. 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": "*"
        }
    ]
}
```

Pemecahan masalah AWS Identitas dan akses Terminal Transfer Data

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Terminal Transfer Data dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Terminal Transfer Data
- Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses sumber daya Terminal Transfer Data saya

Saya tidak berwenang untuk melakukan tindakan di Terminal Transfer Data

Jika Anda tidak dapat melihat atau menjadwalkan reservasi di konsol Terminal Transfer AWS Data, Anda mungkin tidak memiliki izin yang diperlukan. Hubungi administrator akun Anda untuk mengonfigurasi kebijakan identitas IAM yang memberi Anda akses dan izin yang sesuai.

Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses sumber daya Terminal Transfer Data saya

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 Terminal Transfer Data mendukung fitur-fitur ini, lihat Cara kerja Terminal Transfer Data dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh AWS akun yang Anda miliki, lihat Men yediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda ke AWS akun pihak ketiga, lihat Menye diakan akses ke AWS akun yang dimiliki oleh pihak ketiga di 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.

Referensi API Terminal Transfer Data: Tindakan dan sumber daya

Saat membuat kebijakan AWS Identitas dan Manajemen Akses (IAM), halaman ini dapat membantu Anda memahami hubungan antara operasi API Terminal Transfer AWS Data, tindakan terkait yang dapat Anda berikan izin untuk dilakukan, dan AWS sumber daya yang dapat Anda berikan izin.

Secara umum, berikut cara menambahkan izin Terminal Transfer Data ke kebijakan Anda:

- Tentukan tindakan dalam `Action` elemen. Nilai termasuk `datatransferterminal:` awalan dan nama operasi API. Misalnya, `datatransferterminal:CreateTask`.
- Tentukan AWS sumber daya yang terkait dengan tindakan dalam `Resource` elemen.

Anda juga dapat menggunakan kunci AWS kondisi dalam kebijakan Terminal Transfer Data Anda. Untuk daftar AWS kunci lengkap, lihat Kunci yang tersedia di Panduan Pengguna IAM.

Operasi API Terminal Transfer Data dan tindakan terkait

CreateTransferTeam

- Tindakan: `datatransferterminal:CreateTransferTeam`

  Sumber daya: `None`

GetTransferTeam

- Tindakan: `datatransferterminal:GetTransferTeam`

  Sumber: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

UpdateTransferTeam

- Tindakan: `datatransferterminal:UpdateTransferTeam`

  Sumber: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

DeleteTransferTeam

- Tindakan: `datatransferterminal:DeleteTransferTeam`

Sumber: Akun Wil `arn:aws::$[replaceable] :datatransferterminal: $[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

ListTransferTeams

- Tindakan: `datatransferterminal:ListTransferTeams`

  Sumber daya: None

RegisterPerson

- Tindakan: `datatransferterminal:RegisterPerson`

  Sumber: Akun Wil `arn:aws::$[replaceable] :datatransferterminal: $[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

GetPerson

- Tindakan: `datatransferterminal:GetPerson`

  Sumber: Akun Wil `arn:aws::$[replaceable] :datatransferterminal: $[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable] :datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

DeregisterPerson

- Tindakan: `datatransferterminal:DeregisterPerson`

  Sumber: Akun Wil `arn:aws::$[replaceable] :datatransferterminal: $[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable] :datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

ListPersons

- Tindakan: `datatransferterminal:ListPersons`

  Sumber: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

CreateReservation

- Tindakan: `datatransferterminal:CreateReservation`

  Sumber: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

  Tindakan tergantung: `datatransferterminal:GetPerson`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Tindakan tergantung: `datatransferterminal:GetFacility`

  Sumber daya tergantung: `arn:aws::$[replaceable]` Partisi `:datatransferterminal:::facility/$[replaceable]` FacilityId ````

GetReservation

- Tindakan: `datatransferterminal:GetReservation`

  Sumber: Akun Wil `arn:aws::$[replaceable]` `:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/reservation/$[replaceable]` ReservationId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

UpdateReservation

- Tindakan: `datatransferterminal:UpdateReservation`

  Sumber: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/reservation/$[replaceable]` ReservationId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

  Tindakan tergantung: `datatransferterminal:GetPerson`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

DeleteReservation

- Tindakan: `datatransferterminal:DeleteReservation`

  Sumber: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Tindakan tergantung: `datatransferterminal:GetTransferTeam`

  Sumber daya tergantung: Akun Wil `arn:aws::$[replaceable]:datatransferterminal:$[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

ListReservations

- Tindakan: `datatransferterminal:ListReservations`

Sumber: Akun Wil `arn:aws::$[replaceable] :datatransferterminal: $[replaceable]` ayah `:$[replaceable]` Partisi `:transfer-team/$[replaceable]` TransferTeamId ````

ListFacilities

- Tindakan: `datatransferterminal:ListFacilities`

  Sumber daya: None

GetFacility

- Tindakan: `datatransferterminal:GetFacility`

  Sumber: `arn:aws::$[replaceable]` Partisi `:datatransferterminal:::facility/ $[replaceable]` FacilityId ````

GetFacilityAvailability

- Tindakan: `datatransferterminal:GetFacilityAvailability`

  Sumber: `arn:aws::$[replaceable]` Partisi `:datatransferterminal:::facility/ $[replaceable]` FacilityId `/availability`

  Tindakan tergantung: `datatransferterminal:GetFacility`

  Sumber daya tergantung: `arn:aws::$[replaceable]` Partisi `:datatransferterminal:::facility/$[replaceable]` FacilityId `/availability`

Validasi kepatuhan untuk AWS Terminal Transfer Data

Untuk mengetahui apakah suatu AWS layanan berada dalam lingkup program kepatuhan tertentu, lihat AWS layanan di Lingkup berdasarkan Program Kepatuhan dan pilih program kepatuhan yang Anda minati. 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 Artefak.

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA – Daftar layanan yang memenuhi syarat HIPAA. Tidak semua AWS layanan memenuhi syarat HIPAA.
- AWS Sumber Daya Kepatuhan — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- https://d1-awsstatic-com-whitepapers-compliance-AWS- Customer-Compliance-Guides-pdf [Panduan AWS Kepatuhan Pelanggan] - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan AWS layanan dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan AWS di Panduan Pengembang Konfigurasi — Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub — AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — AWS Layanan ini mendeteksi potensi ancaman terhadap AWS akun, beban kerja, wadah, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Manajer Audit — AWS Layanan ini membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Terminal Transfer Data

Infrastruktur AWS global dibangun di sekitar Wil AWS ayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Zona Ketersediaan 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 fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Zona Ketersediaan, lihat Infrastruktur AWS Global.

AWS Terminal Transfer Data tersedia di berbagai lokasi di seluruh dunia. Anda dapat terhubung ke Wil AWS ayah mana pun yang dapat diakses dari internet.

Pencatatan dan pemantauan di Terminal Transfer Data

AWS Terminal Transfer Data terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Terminal Transfer Data. CloudTrail menangkap semua panggilan API untuk Terminal Transfer Data sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari konsol Terminal Transfer Data dan panggilan kode ke operasi API Terminal Transfer Data. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Terminal Transfer Data. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Ri wayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Terminal Transfer Data, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan itu dibuat, dan detail tambahan.

Untuk mempelajari selengkap CloudTrail nya, lihat Panduan AWS CloudTrail Pengguna.

Informasi Terminal Transfer Data di CloudTrail

CloudTrail diaktifkan pada AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Terminal Transfer Data, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam ri wayat acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat acara dengan CloudTrail riwayat acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Terminal Transfer Data, buat jejak. Jej ak CloudTrail memungkinkan pengiriman file log ke bucket

Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wil AWS ayah. 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 bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- M CloudTrail enerima file log dari beberapa wilayah dan Mener CloudTrail ima file log dari beberapa akun

Semua tindakan Terminal Transfer Data dicatat oleh CloudTrail dan didokumentasikan di Referensi API Terminal Transfer Data: Tindakan dan sumber daya bagian panduan ini.

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 kredentif pengguna root atau AWS Identity and Access Management (IAM).
- 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 .

Memahami entri file log Terminal Transfer Data

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 apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Keamanan Infrastruktur di AWS Terminal Transfer Data

Sebagai layanan terkelola, Terminal Transfer AWS Data dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper {https---d0-awsstatic-com-whitepapers-security- -} [Amazon Web Services: Overview of Security Processes].AWS Security-Whitepaper-pdf

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses Terminal Transfer Data melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite sandi dengan kerahasiaan maju sempurna (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.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredentif keamanan sementara untuk menandatangani permintaan.

Riwayat dokumen untuk Panduan Pengguna Terminal Transfer Data

Tabel berikut menjelaskan riwayat dokumen untuk panduan ini.

Perubahan	Deskripsi	Tanggal
Perbarui tata letak	Pembaruan tata letak dokumen dan verbiage kecil dan pengeditan konten.	Januari 1, 2025
Publikasi awal	Tanggal peluncuran dokumentasi asli.	Desember 1, 2024

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.