사용 설명서

AWS Data Transfer Terminal

AWS Data Transfer Terminal: 사용 설명서

Table of Contents

Data Transfer Terminal이란 무엇인가요?

AWS Data Transfer Terminal은 AWS 클라우드 서비스를 통해 데이터를 빠르게 전송하기 위해 데이터 스토리지 디바이스를 가져올 수 있는 네트워크 지원 물리적 위치입니다. 원격으로 캡처된 데이터를 업로드하면 원격으로 캡처된 데이터에 더욱 쉽게 액세스할 수 있습니다.

AWS Management Console에서 물리적 Data Transfer Terminal 시설 중 하나를 예약하고, 예정된 시간에 도착하고, 자체 디바이스를 사용하여 AWS 클라우드 서비스에 데이터를 업로드합니다. 예약이 완료되고 나가게 되면 시설은 다시 보호되고, 다음 예약에 대비합니다.

> **Note**
>
> AWS Data Transfer Terminal은 현재 AWS Enterprise 고객만 사용할 수 있습니다.

Data Transfer Terminal에 액세스:

- AWS Data Transfer Terminal 콘솔: https://console.aws.amazon.com/datatransferterminal
- Data Transfer Terminal 시설: 콘솔에서 예약되면 Data Transfer Terminal 시설의 위치가 제공됩니다. 자세한 내용은 데이터 전송 섹션을 참조하세요.

Features

AWS Data Transfer Terminal을 사용하면 원격 위치에서 데이터를 AWS 클라우드 서비스로 더 쉽게 가져올 수 있습니다. 다음은 원격 데이터 업로드 요구 사항에 따른 Data Transfer Terminal의 몇 가지 이점입니다.

보안, 비공개 및 독점

각 Data Transfer Terminal 시설은 빠른 네트워크 연결을 통해 데이터 스토리지 디바이스와 AWS 서비스 간에 대규모 데이터를 전송할 수 있는 안전한 비공개 위치입니다.

전용 예약 콘솔

전송 팀에 승인된 직원을 추가하고 Data Transfer Terminal 콘솔을 사용하여 AWS Data Transfer Terminal 예약을 실시합니다.

광섬유 네트워크 연결

각 Data Transfer Terminal 시설에는 빠른 데이터 업로드 및 중복성을 위한 100기가비트(Gbps) 광섬유(LR4) 연결 2개가 포함되어 있습니다.

데이터 스토리지 디바이스 제어

Snowball 디바이스를 배송하고 데이터가 AWS 클라우드 서비스에 업로드될 때까지 기다릴 필요가 없습니다. 전체 데이터 전송 프로세스에서 물리적 데이터 스토리지 디바이스를 제어하여 이동해야 하는 위치로 데이터를 더 빠르게 가져옵니다.

주요 개념

AWS Data Transfer Terminal을 사용하려면 프로세스 소유자가 데이터 전송 전문가가 Data Transfer Terminal 시설에 액세스할 수 있도록 예약을 해야 합니다. Data Transfer Terminal 용어에 대한 자세한 내용은 다음 섹션을 참조하세요.

주제

전송 팀

전송 팀은 AWS 계정 소유자가 결정한 직원 그룹으로, 조직을 대신하여 데이터 전송을 수행하도록 선택할 수 있는 기능입니다. 전송 팀 설정에는 전송 팀에 이름을 지정하고 팀의 직원을 지정하는 작업이 포함됩니다. 단일 예약에 대해 4명 이하의 데이터 전송 전문가로 구성된 그룹을 사용하는 것이 좋습니다.

자세한 내용은 Data Transfer Terminal 예약 섹션을 참조하세요.

직원

직원은 예약을 하고 관리하거나 Data Transfer Terminal 시설로 이동하여 사용할 수 있는 개인을 의미합니다. 직원은 프로세스 소유자, 데이터 전송 전문가 또는 두 가지 모두가 될 수 있습니다.

프로세스 소유자

- 프로세스 소유자는 AWS Data Transfer Terminal 계정에서 직원을 추가, 편집 및 제거할 수 있는 AWS 계정 소유자입니다.

데이터 전송 전문가

- 데이터 전송 전문가는 데이터 업로드 트랜잭션을 위해 Data Transfer Terminal 시설로 이동할 수 있는 개인입니다. 이러한 직원은 프로세스 소유자의 승인을 받고 AWS Data Transfer Terminal 계정에 추가되어야 합니다. Data Transfer Terminal 시설에 액세스할 때는 정부에서 발급한 ID가 필요합니다.

시설

Data Transfer Terminal 시설은 하나 이상의 서비스 공급자가 공동 소유 및 관리하는 데이터 허브입니다. 각 시설은 Data Transfer Terminal 데이터 전송 전문가가 Data Transfer Terminal 스위트에 액세스하기 위해 예약 레코드와 일치해야 하는 정부에서 발급한 신원 증명을 제공해야 합니다.

예약 고려 사항

Data Transfer Terminal 콘솔에서 연중 어느 요일에나 1~6시간 동안 예약할 수 있습니다. 예약 간에 최소 1시간 간격을 두고 개별 예약을 연속으로 예약할 수 있습니다. 모든 예약은 최소 24시간 전에 이루어져야 합니다.

데이터 전송에 필요한 시간은 업로드 성능 속도에 따라 달라집니다. Data Transfer Terminal 예약을 계획하고 실시할 때 업로드 성능에 영향을 미치는 다음 요소를 고려하세요.

장비

- 일부 장비에는 업로드 성능에 영향을 미칠 수 있는 설정이 포함될 수 있습니다. 권장 업로드 성능 속도는 장비 사양을 참조하세요.

네트워크 조건

- 네트워크 트래픽이 많으면 데이터 업로드 속도에 영향을 미치므로 데이터 전송 세션 시간을 선택할 때 이를 고려해야 합니다. 사용량이 적은 시간이나 네트워크 활동이 적은 시간에 데이터 전송 세션을 계획하면 업로드 속도가 증가할 수 있습니다.

데이터 전송 크기

- Data Transfer Terminal 네트워크 연결은 대규모 데이터 전송을 위해 설계되었습니다. 하지만 전송되는 데이터의 크기는 세션의 소요 시간에 영향을 미칩니다.

사용 사례

모든 AWS Enterprise 고객이 Data Transfer Terminal 시스템에 액세스할 수 있지만 특정 사용 사례 시나리오에서는 더 큰 이점을 얻을 수 있습니다.

자율 주행 및 고급 운전자 지원 시스템(AD/ADAS): 자동차 원천 장비 제조업체(OEM) 및 공급업체는 북미, 유럽 및 ASEAN 지역 내의 수많은 대도시에서 운행하면서 데이터를 수집하는 자율 차량 플릿으로부터 대규모 데이터 세트를 생성합니다. Data Transfer Terminal을 사용하면 이러한 플릿 차량에서 수집한 데이터를 AWS 클라우드 서비스에 업로드하고 AD/ADAS 모델을 교육하는 데 사용할 수 있습니다.

미디어 및 엔터테인먼트: 스튜디오 및 기타 콘텐츠 제작자는 멀리 떨어진 곳에서 디지털 비디오 및 오디오(AV) 파일을 생성하는 경우가 많습니다. 지리적으로 분산된 제작 및 편집 팀이 워크플로를 병렬로 실시간으로 시작할 수 있도록 이러한 AV 파일을 적당한 시기에 맞춰 클라우드에 업로드하는 것이 중요합니다. Data Transfer Terminal을 사용하여 데이터를 원격으로 업로드하면 제작 타임라인을 단축하여 비용을 절감할 수 있습니다.

지도, 사진 측정 및 3D 이미지: 지도 또는 이미지 애플리케이션을 사용하는 조직은 원격 위치에서 데이터를 수집하므로 분석 또는 교육을 위해 이러한 시각적 파일을 AWS 클라우드에 업로드해야 합니다. Data Transfer Terminal은 이러한 대규모 데이터 세트를 수집 및 분석하는 데 걸리는 시간을 최소화하므로 운전자, 농부 및 해당 정보의 기타 사용자가 지리 공간 데이터를 최신 상태로 유지할 수 있습니다.

관련 서비스

다음 AWS 서비스는 Data Transfer Terminal을 사용하는 동안 최적의 환경을 제공합니다.

AWS 서비스	설명
AWS Snowball Edge	AWS Data Transfer Terminal은 AWS 클라우드에 더 빠르게 업로드할 수 있는 위치를 제공하여 Snowball 제품을 보완하고, 데이터 액세스 대기 시간을 최소화합니다.
Amazon S3()	자체 디바이스를 Data Transfer Terminal로 가져와 Amazon S3 서비스에 데이터를 빠르고 안전하게 업로드합니다.

Data Transfer Terminal 사용 기술 요구 사항

Data Transfer Terminal에서 예약을 하기 전에 네트워크 연결에 필요한 장비 및 구성이 있는지 확인해야 합니다. 최적의 네트워크 연결 및 경험은 다음 가이드라인을 참조하세요.

장비

예약을 위해 모니터, 키보드, 마우스, 컴퓨터 또는 노트북을 포함하여 연결을 위한 휴대용 디바이스를 Data Transfer Terminal 시설로 가져와야 합니다.

하드웨어가 광섬유(L4) 연결을 사용할 수 있어야 합니다.

> **Note**
>
> 데이터 보안 모범 사례에 따라 Data Transfer Terminal로 가져오는 스토리지 디바이스에서 데이터가 암호화 및 보호되어야 하고, Data Transfer Terminal 시설을 사용하는 동안 데이터 암호화 정책을 적용해야 합니다. 자세한 내용은 AWS Data Transfer Terminal의 보안을 참조하세요.

네트워크 요구 사항

업로드 중인 디바이스, 서버 또는 어플라이언스(노트북)가 네트워크에 연결할 준비가 되어 있고 DHCP를 지원해야 합니다. 최적의 데이터 업로드 경험을 위해 필요한 사항:

- Data Transfer Terminal 시설에 제공된 광섬유 케이블 연결을 위한 NIC 및 LC 커넥터와 호환되는 100G QSFP28 LR4(100GBASE-LR4) 광학 QSFP 송수신기.
- IP 주소 자동 구성 DHCP 활성화. DNS 서버가 DHCP에 의해 자동으로 할당.
- 최신 소프트웨어 및 NIC 드라이버.

성능 최적화

AWS Data Transfer Terminal을 사용하는 동안 처리량을 극대화하려면 다음 권장 사항을 고려하세요.

- 권장 하드웨어:

- 100Gbps 네트워크 인터페이스 카드
- 16코어 CPU
- 128GB RAM
- 여러 개의 NVME SSD 드라이브(RAID 어레이)

- AWS Command Line Interface 또는 AWS SDK를 사용한 업로드에는 AWS 공통 런타임(AWS CRT) 라이브러리를 사용합니다.

  아래 파라미터를 구성하여 Amazon S3 전송 설정을 최적화합니다. 기본 위치 `~/.aws/config`에서 AWS 구성 파일의 최상위 `s3` 키 아래에 이러한 값을 설정합니다.

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

  모든 Amazon S3 구성 값은 들여쓰기 처리되고 최상위 `s3` 키 아래에 중첩됩니다.

  - 선택 사항: `aws configure set` 명령을 사용하여 위의 값을 프로그래밍 방식으로 설정할 수 있습니다. 예를 들어, 기본 프로필에 대해 위의 값을 설정하려면 다음 명령을 대신 실행할 수 있습니다.

    ```
    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
    ```

- 기본값 이외의 프로필에 대해 이러한 값을 프로그래밍 방식으로 설정하려면 `--profile` 플래그를 입력합니다. 예를 들어, `test-profile`이라는 프로필에 대한 구성을 설정하려면 아래 예제와 같이 runa 명령을 실행합니다.

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

- 처리량 증가를 위해 디바이스에서 BBR(Linux)을 활성화합니다.

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

추가 정보

네트워크 연결 및 성능을 최적화하기 위한 AWS 명령줄 Amazon S3 구성에 대한 자세한 내용은 다음 리소스를 참조하세요.

- AWS CLI 명령 참조의 AWS CLI Amazon S3 구성
- Amazon S3 Java용 Amazon AppStream SDK의 고성능 Amazon S3 클라이언트 사용: AWS CRT 기반 클라이언트
- AWS 지식 센터의 AWS CLI를 사용하여 Amazon S3에 대용량 파일을 업로드할 때 성능을 최적화하려면 어떻게 해야 하나요?

시작하기

Data Transfer Terminal 시설 중 하나에서 예약하여 AWS 클라우드 서비스로 원격 데이터 전송을 시작합니다. 시작하려면 Data Transfer Terminal 시설 및 AWS Enterprise 계정에서 지원하는 장비가 필요합니다.

Data Transfer Terminal 예약 전에 이 설명서의 Data Transfer Terminal 사용 기술 요구 사항 섹션을 검토하여 데이터 전송을 위한 최적의 구성을 갖춘 장비가 있는지 확인합니다. 모든 데이터 스토리지 디바이스 및 네트워크 연결 장비가 스위트에서 사용할 수 있는 광섬유 네트워크 연결과 호환되지는 않습니다.

AWS에 가입하면 Data Transfer Terminal을 포함하여 AWS의 모든 서비스에 AWS 계정이 자동으로 등록됩니다. 사용자에게는 사용한 서비스에 대해서만 요금이 청구됩니다.

Data Transfer Terminal을 설정하려면 다음 섹션의 단계를 사용합니다.

AWS에 가입하고 Data Transfer Terminal을 설정할 때, AWS Management Console에서 표시 언어를 변경할 수 있습니다. 자세한 내용은 AWS Management Console 시작 안내서에서 AWS Management Console의 언어 변경을 참조하세요.

AWS 계정이 있으면 Data Transfer Terminal에 액세스할 수 있습니다. AWS Data Transfer Terminal 설정 및 사용에 대한 자세한 내용은 Data Transfer Terminal 예약 섹션을 참조하세요.

AWS 계정에 가입

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성하세요.

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 수 있는 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS은 사용자에게 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

AWS 계정을 등록하고, AWS 계정 루트 사용자에 보안 조치를 한 다음, AWS IAM Identity Center를 활성화하여 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔)를 참조하세요.
3. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center 활성화를 참조하세요.
4. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성을 참조하세요.
5. IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

   IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.
6. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 권한 세트 생성을 참조하세요.
7. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

Data Transfer Terminal 예약

AWS Data Transfer Terminal 사용을 시작하려면 AWS 계정이 있고 https://console.aws.amazon.com/datatransferterminal에서 Data Transfer Terminal 콘솔에 로그인해야 합니다. Data Transfer Terminal 콘솔에 로그인하면 기존 예약을 보거나 새로 예약할 수 있습니다. 예약을 하려면 다음을 수행해야 합니다.

1. 전송 팀을 생성합니다. 예약을 생성하고 Data Transfer Terminal 시설에 액세스하여 데이터를 전송하려면 지정된 사용자 그룹을 생성해야 합니다. 이 주제에 대한 자세한 내용은 전송 팀 생성을 참조하세요.
2. 팀이 구성되면 팀에 직원을 추가해야 합니다. 전송 팀에 직원을 추가하는 방법에 대한 자세한 내용은 직원 추가 섹션을 참조하세요.
3. 프로세스 소유자는 계정의 팀과 데이터 전송을 예약할 수 있습니다. 예약 방법에 대한 자세한 내용은 예약 세부 정보 지정 섹션을 참조하세요.
4. 요청을 제출하기 전에 예약 세부 정보가 올바른지 확인해야 합니다. 제출 후에는 최소 24시간 동안 예약 요청을 수정할 수 없습니다. 자세한 내용은 예약 검토 및 확인을 참조하세요.

예약이 처리 및 확인되면 전송 팀은 예약된 시간에 Data Transfer Terminal 시설에 액세스할 수 있습니다. 자세한 내용은 Data Transfer Terminal 시설에서 데이터 전송을 참조하세요.

전송 팀 생성

Data Transfer Terminal 시설에 액세스하려면 AWS Management Console에서 예약을 해야 합니다. AWS 계정에 로그인하여 Data Transfer Terminal 콘솔에 액세스하고 다음 단계를 완료하여 예약을 실시합니다.

1. Data Transfer Terminal 홈 페이지에서 시작하기 버튼을 선택합니다.
2. 계정에 전송 팀을 아직 설정하지 않은 경우 예약 생성 버튼이 비활성화됩니다. 시작하려면 전송 팀을 생성하고 이름을 지정해야 합니다.
   a. 전송 팀 생성 버튼을 선택합니다.
   b. 팀에 이름을 지정합니다.
      - 이름은 문자 또는 숫자로 시작되어야 하고 2~64자여야 합니다.
      - 문자, 숫자, 마침표 및 대시만 사용하세요. 특수 문자는 인식되지 않습니다.
      - 민감한 식별 정보는 포함하지 마세요.

c. 전송 팀의 설명을 생성합니다.

- 특정 기간, 캠페인 또는 프로젝트에 대한 팀의 목적을 설명하는 등 팀을 식별하는 데 도움이 되는 설명을 입력합니다.

d. 전송 팀 생성 버튼을 선택합니다.

전송 팀 페이지로 돌아가고 새로 생성된 팀이 전송 팀 섹션 아래에 표시됩니다.

Data Transfer Terminal 계정에서 전송 팀 업데이트

새 전송 팀을 설정하려면 이 안내서의 Data Transfer Terminal 예약 섹션을 참조하세요.

전송 팀을 수정하거나 제거하려면 다음 작업을 수행합니다.

1. 전송 팀 페이지에서 수정하려는 전송 팀을 선택합니다.
2. 전송 팀 이름 및 설명을 수정하려면 편집 버튼을 선택합니다.
3. 직원을 추가하거나 제거하려면 직원 탭을 선택하고 이 FAQ의 내 계정에서 직원을 수정, 추가 또는 제거하려면 어떻게 해야 하나요? 섹션에 설명된 단계를 완료합니다.
4. 선택한 전송 팀에 대한 예약을 추가하거나 취소하려면 이 FAQ의 Data Transfer Terminal 계정의 직원 업데이트 섹션을 참조하세요.

직원 추가

전송 팀에 프로세스 소유자와 데이터 전송 전문가를 추가하여 데이터 전송을 설정하고 Data Transfer Terminal 시설에 액세스합니다. 전송 팀에 직원을 추가하려면 다음을 수행합니다.

1. 전송 팀 페이지의 전송 팀 섹션에 나열된 카드 중에서 원하는 전송 팀 카드를 선택합니다. 전송 팀의 요약 페이지가 표시됩니다.
2. 직원 탭을 선택하고, 직원 등록 버튼을 선택하여 전송 팀에 직원을 추가합니다.
3. 직원 등록 페이지에서 전송 팀에 추가하려는 직원에 대한 필수 정보를 사용하여 필드를 작성합니다.

a. 직원 별칭: 고유한 별칭을 생성하여 직원을 식별합니다.

- 별칭은 신원을 보호하면서 직원을 식별하는 데 사용됩니다.
- 최대 64자까지 입력할 수 있고 문자, 숫자 및 대시를 포함할 수 있습니다.
- 특수 문자는 허용되지 않습니다.

b. 이름: 정부에서 발급한 신분증에 표시된 직원의 이름을 입력합니다.

c. 성: 정부에서 발급한 신분증에 표시된 직원의 성을 입력합니다.

d. 이메일 주소: Data Transfer Terminal 시설에 액세스하기 위한 예약 정보와 지침을 받을 수 있는 양호한 이메일 주소를 포함합니다.

4. 직원 등록 버튼을 선택하여 전송 팀에 직원 추가를 완료합니다.

Data Transfer Terminal 계정의 직원 업데이트

Data Transfer Terminal 콘솔에서 계정의 기존 직원을 수정하는 작업은 현재 지원되지 않습니다. AWS Data Transfer Terminal 프로세스 소유자는 현재 직원 추가 또는 삭제만 가능합니다.

Data Transfer Terminal 계정에서 직원을 제거하려면 다음 작업을 수행합니다.

1. 전송 팀 페이지에서 제거하려는 직원과 연결된 전송 팀을 선택합니다.
2. 선택한 전송 팀의 요약 페이지에서 직원 탭을 선택합니다.
3. 제거하려는 별칭 옆에 있는 라디오 버튼을 클릭합니다. 프로필을 삭제할 때는 직원의 별칭만 볼 수 있습니다.
4. 삭제 버튼을 선택합니다. 선택한 직원에 대한 작업을 확인하는 경고가 표시됩니다. 삭제 버튼을 클릭하여 계속합니다. 콘솔 상단에 직원이 성공적으로 삭제되었음을 확인하는 배너가 표시됩니다.

예약 세부 정보 지정

다음 지침은 AWS Management Console에서 Data Transfer Terminal 예약 방법을 안내합니다. Data Transfer Terminal 시설 사용에 대한 자세한 내용은 데이터 전송 섹션을 참조하세요.

1. 예정된 예약 탭에서 예약하기 버튼을 선택합니다.
2. 예약 세부 정보 지정 페이지의 필드를 작성합니다.

a. 전송 팀 선택: 기본값으로 선택된 전송 팀이 먼저 표시됩니다. 다른 팀을 선택하려면 드롭다운 화살표를 클릭하여 사용 가능한 전송 팀 목록에서 선택합니다.

b. 프로세스 소유자: 예약 관리를 담당할 직원 별칭을 선택합니다.

- 예약에서는 단 한 명의 프로세스 소유자만 허용되고 AWS 계정에서 승인된 직원이어야 합니다.

  프로세스 소유자는 데이터 전송 전문가 중 한 명으로 포함되어 데이터 전송 활동을 수행할 수도 있습니다.

c. 데이터 전송 전문가: Data Transfer Terminal 시설에 액세스하여 데이터 전송 활동을 완료할 직원을 선택합니다. 필요에 따라 2명 이상의 직원을 선택할 수 있습니다.

- 전송 팀을 4명 이하의 데이터 전송 전문가로 제한하는 것이 좋습니다.

d. Data Transfer Terminal 정보: 데이터 전송 세션과 관련된 Data Transfer Terminal 시설, 원하는 날짜 및 특정 시간을 지정합니다.

i. Data Transfer Terminal 시설: 드롭다운 화살표를 클릭하여 Data Transfer Terminal 시설을 선택합니다.

> **Note**
>
> 예약 중에는 시설 설명만 제공됩니다. 예약 확인 이메일에 추가 위치 정보가 제공됩니다.

ii. Data Transfer Terminal 날짜 및 시간: 일정을 보고 예약하려면 예약 날짜 및 시간 검색을 클릭합니다.

- 예약은 최소 24시간 전, 6개월 이내의 날짜에서 이루어져야 하고, 최대 6시간까지 예약할 수 있습니다. 필요한 경우 야간 시나리오를 고려하기 위해 단일 예약 시간이 이틀에 걸칠 수 있습니다.
- 시간은 24시간제를 사용하여 표시되고 정시 단위로만 예약할 수 있습니다.
- 연속 예약을 하려면 각 데이터 전송 세션 간에 최소 1시간의 간격을 두고 예약을 생성해야 합니다.
- 자세한 내용은 예약 고려 사항 섹션을 참조하세요.

3. 예약 세부 정보가 올바른지 확인한 다음 생성 버튼을 선택하여 계속합니다. 예약 요약이 제공되는 확인 페이지로 이동합니다.

예약 검토 및 확인

예약 세부 정보를 지정한 후 다음 버튼을 선택하여 개요 페이지를 계속 확인합니다. 검토 및 생성 페이지에서 Data Transfer Terminal 예약 요청의 세부 정보를 검토합니다.

- 요청이 만족스러운 경우 생성 버튼을 선택합니다.
- 예약을 변경해야 하는 경우 이전 버튼을 선택합니다.

예약 요청이 제출되면 프로세스 소유자는 요청이 접수되었고 처리 중임을 확인하는 이메일을 받게 됩니다. 요청이 승인되면 다른 이메일로 예약이 확인되고 Data Transfer Terminal 시설을 찾고 액세스하기 위한 지침이 제공됩니다. Data Transfer Terminal 시설 액세스에 대한 자세한 내용은 데이터 전송 섹션을 참조하세요.

예약 변경

24시간 처리 기간 전에 Data Transfer Terminal 예약 요청을 변경할 수 있습니다.

처리 기간이 지나면 콘솔에서 전송 팀 페이지로 이동하여 예약을 보거나 편집하거나 삭제합니다.

1. 팀의 카드에서 원하는 예약을 찾아 선택합니다.
2. 작업 메뉴를 클릭하고 원하는 작업을 선택합니다.
   - 보기: 보기 옵션을 선택하면 날짜, 시간, 위치, 할당된 직원 등 예약 세부 정보를 볼 수 있습니다.
   - 편집: 날짜, 시간, 위치 및 할당된 직원을 포함하여 예약의 세부 정보를 수정할 수 있습니다. 원하는 예약 날짜로부터 24시간 전에 변경이 이루어져야 하며 변경 사항은 즉시 수락 및 적용되지 않습니다. 프로세스 소유자에게 업데이트된 요청에 대한 확인이 전송됩니다.
   - 삭제: 삭제 옵션을 사용하면 예약을 취소할 수 있습니다. 예약 날짜로부터 최소 24시간 전에 취소를 요청해야 합니다. 요청이 승인되면 프로세스 소유자는 예약 취소 관련 확인을 받게 됩니다.

Data Transfer Terminal 시설에서 데이터 전송

Data Transfer Terminal은 AWS 네트워크에 대한 보안 액세스를 제공하는 안전한 공동 소유 위치입니다. Data Transfer Terminal 시설에 액세스하려면 위치 설명 및 액세스 지침이 포함된 확인 이메일을 수신해야 합니다. Data Transfer Terminal 시설 액세스 및 사용에 대한 자세한 내용은 아래 주제를 참조하세요.

주제

휴대해야 하는 물품

데이터 전송 전문가는 노트북 컴퓨터, 플래시 드라이브, 솔리드 스테이트 드라이브(SSD) 및 AWS Snowball Edge 등 데이터 전송에 필요한 물품을 가져와야 합니다. Data Transfer Terminal 시설에서 광섬유 네트워크 케이블을 사용하도록 장비가 최적화되어 있어야 합니다. 최적의 장비 및 구성에 대한 자세한 내용은 Data Transfer Terminal 사용 기술 요구 사항을 참조하세요.

사용자와 동반하는 데이터 전송 전문가가 Data Transfer Terminal 시설에 가져오는 장비 및 물품의 설치, 사용 및 제거는 사용자의 책임입니다. 스위트로 가져온 모든 물품을 가지고 나가야 합니다. AWS Data Transfer Terminal에서는 잊어버리거나 분실한 물품에 대해 책임을 지지 않습니다.

Data Transfer Terminal 시설의 물리적 주소

Data Transfer Terminal 시설의 물리적 주소는 제공되지 않습니다. 대신 예약에 지정된 프로세스 소유자 및 데이터 전송 전문가에게 Data Transfer Terminal 시설의 검색 가능한 공개 이름이 포함된 이메일이 전송됩니다. AWS Data Transfer Terminal은 AWS Direct Connect와 동일한 위치 식별 시스템을 사용하므로 인터넷에서 공개 이름을 검색하여 Data Transfer Terminal 시설을 찾을 수 있습니다. 이 정보가 포함된 이메일을 수신하지 못한 경우 AWS Data Transfer Terminal 계정 관리자에게 전송 팀의 일원이면서 이메일 정보가 올바른지 확인합니다.

건물 액세스

Data Transfer Terminal 시설에 액세스하려면 각 데이터 전송 전문가가 신원 증명 또는 정부 발행 신분증을 제공해야 합니다. 건물 출입이 승인되면 보안 요원이 Data Transfer Terminal 스위트로 안내합니다.

Data Transfer Terminal 스위트에 있는 장비.

각 Data Transfer Terminal 시설에는 2개의 광섬유 케이블, 탁자나 책상, 의자만 있어야 합니다. 방에 다른 장비나 물품이 있는 경우 즉시 Support에 신고하세요.

네트워크 연결 문제 해결

인터넷에 연결할 수 없거나 연결 속도가 느린 경우와 같이 AWS Data Transfer Terminal을 사용하는 동안 네트워크 연결 문제가 발생하는 경우 다음 문제 해결 팁을 고려하세요.

주제

장비 연결 문제

Data Transfer Terminal 스위트에 있는 동안 물리적 연결 설정에 문제가 있는 경우 다음 사항을 고려하세요.

- 각 Data Transfer Terminal 시설에는 2개의 단일 모드 LC 광섬유 케이블이 있습니다. 케이블 중 하나 또는 둘 다 없는 경우 AWS Support에 즉시 문의하세요.
- 광섬유 케이블 하나가 작동하지 않는 경우 먼저 케이블을 감아보세요. 여전히 첫 번째 케이블에 연결할 수 없는 경우 다른 케이블을 사용해 보세요.

여전히 케이블을 사용하여 연결할 수 없는 경우 AWS Support에 즉시 문의하세요.

연결 문제 해결

장비를 연결할 수 있지만 네트워크에 연결할 수 없는 경우 다음 문제 해결 제안을 시도해 보세요.

- 장비 구성이 지정된 네트워크 요구 사항을 충족하는지 확인합니다. 자세한 내용은 Data Transfer Terminal 사용 기술 요구 사항을 참조하세요.
- 다른 광섬유 케이블로 전환하고 연결합니다.
- 광섬유 케이블이 연결된 상태에서 디바이스를 재부팅합니다.
- 디바이스에서 기본 네트워크 진단을 수행하여 다음 사항을 확인합니다.
  - DHCP가 활성화됨
  - 연결된 네트워크 인터페이스에 IP 주소가 할당됨
  - DNS 서버가 구성됨

- 시스템 클록이 NTP와 동기화됨

여전히 연결할 수 없는 경우 AWS Support에 문의하여 디바이스에서 실행 중인 운영 체제(OS)에 따라 다음 출력을 제공합니다.

Linux/Unix

- 터미널 또는 명령줄 인터페이스(CLI)에서 IP 주소 및 라우팅 정보를 가져옵니다. 네트워크 인터페이스에 IP 주소가 할당되고, 기본 게이트웨이 주소가 있는 기본 경로가 라우팅 테이블에 추가되었는지 확인합니다.

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

  - 아니면 `iproute2`가 디바이스에 설치되어 있지 않고 `ip` 명령을 사용할 수 없는 경우 다음 명령을 사용합니다.

```
ifconfig
netstat -rn
```

- DNS 서버 정보를 수집합니다. `nameserver` 키워드로 시작하는 IP 주소 2개가 표시되어야 합니다.

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

- 기본 연결 테스트의 출력을 수집합니다. `default_gateway_address`를 할당된 기본 게이트웨이의 IP 주소로 바꿉니다.

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

- HTTPS 연결 테스트의 출력을 수집합니다. 다음 명령에서 Amazon S3의 `HTTP 200 OK` 응답이 표시되어야 합니다.

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

Windows

- 명령 프롬프트에서 IP 주소, 라우팅 및 DNS 서버 정보를 가져옵니다. 네트워크 인터페이스에 IP 주소가 할당되고, DNS 서버 2개가 할당되고, 기본 게이트웨이 주소가 있는 기본 경로가 라우팅 테이블에 추가되었는지 확인합니다.

```
ipconfig /all
route print
```

- 명령 프롬프트에서 기본 연결 테스트의 출력을 수집합니다. `default_gateway_address`를 할당된 기본 게이트웨이의 IP 주소로 바꿉니다.

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

- PowerShell에서 HTTPS 연결 테스트의 출력을 수집합니다. 다음 명령에서 `HTTP 200 OK` 응답이 표시되어야 합니다.

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

네트워크 처리량

네트워크의 실제 데이터 전송 속도를 측정하는 네트워크 처리량은 다양한 요인의 영향을 받을 수 있습니다. 데이터 전송 속도에 영향을 미칠 수 있는 요소:

- 하드웨어: 디바이스의 하드웨어 구성 요소로 인해 데이터를 업로드할 때 연결 속도가 저하될 수 있습니다. 디바이스에 사용되는 CPU 및 디스크가 성능 제한에 도달할 수 있습니다. RAID 배열에서 NVME SSD를 사용하는 것이 좋습니다. 성능을 개선하고 CPU 사용량을 줄이려면 AWS CRT 라이브러리를 사용해야 합니다.
- 암호화 오버헤드: HTTPS와 같은 보안 전송을 사용하면 암호화 오버헤드로 인해 처리 시간이 증가합니다.
- 지연 시간: 지연 시간은 데이터 패킷이 소스에서 대상으로 이동하는 데 걸리는 시간을 의미합니다. 다른 지리적 리전의 Amazon S3 버킷에 업로드할 때 지연 시간이 길어질 수 있고, 이로 인해 데이터 전송이 지연되면서 처리량이 낮아질 수 있습니다. 가능하면 동일한 리전 내에서 데이터를 전송하는 것이 좋습니다.
- 패킷 손실: 손실된 패킷을 다시 전송해야 하므로 데이터 전송 속도가 느려집니다.

AWS Data Transfer Terminal의 보안

AWS Data Transfer Terminal은 AWS 클라우드에서 데이터를 주고받을 수 있는 안전한 환경을 제공합니다. 다른 물리적 네트워크 광섬유 연결과 마찬가지로 Data Transfer Terminal 연결은 기본 암호화를 제공하지 않습니다. 따라서 안전한 데이터 전송을 위해 데이터 암호화 모범 사례를 적용할 책임이 있습니다.

AWS에서 클라우드 보안은 가장 중요합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 빌드된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS과 사용자의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS Cloud에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Data Transfer Terminal에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내 AWS 서비스 섹션을 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Data Transfer Terminal을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 Data Transfer Terminal을 사용하는 동안 데이터를 보호하는 방법을 보여줍니다. 또한 Data Transfer Terminal 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

AWS Data Transfer Terminal의 데이터 보호

AWS 공동 책임 모델을 AWS Data Transfer Terminal의 데이터 보호에 적용하는 방법을 알아봅니다. 이 모델에서 설명하는 것처럼 AWS은(는) 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 통제를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)를 사용해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정합니다. AWS 활동 캡처에 CloudTrail 추적을 사용하는 방법에 대한 자세한 내용은 AWS 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-3 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 Data Transfer Terminal 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

데이터 암호화

AWS Data Transfer Terminal을 사용하면 자체 관리형 스토리지 시스템과 AWS 스토리지 서비스 간에 데이터를 안전하게 전송할 수 있는 고속 네트워크 연결에 액세스할 수 있습니다. 전송 중 스토리지 데

이터를 암호화하는 방법은 디바이스에서 활성화된 정책과 데이터가 전송되는 서비스에 따라 일부분 달라집니다. 데이터의 관리와 전송 중 암호화는 Data Transfer Terminal을 사용하는 개인의 책임입니다.

저장 시 암호화

AWS Data Transfer Terminal은 모든 저장 데이터를 암호화합니다.

Data Transfer Terminal은 참석 및 예약하도록 지정된 개인의 이름과 성, 이메일 주소를 포함하여 예약에 필요한 데이터만 확보합니다. 이 데이터 수집의 목적은 예약 세부 정보를 확인하고 데이터 전송을 수행할 수 있는 공간에 대한 액세스를 보장하는 것입니다. 이 트랜잭션 정보는 35일 이내에 백업되지만 AWS 계정 정보는 10년 동안 보존됩니다.

전송 중 암호화

AWS Data Transfer Terminal은 전송 중인 데이터를 암호화하지 않습니다. 전송 팀을 설정하고, 직원을 추가하고, 콘솔에서 예약하기 위해 Data Transfer Terminal API 엔드포인트와 상호 작용하면 데이터가 전송 중 암호화됩니다. AWS 공동 책임 모델의 일부로 Data Transfer Terminal을 통해 AWS 서비스에 연결하는 방법을 선택할 수 있습니다. TLS 1.2 및 1.3과 같은 강력한 전송 중 암호화를 사용하여 AWS 서비스에 연결하는 것이 좋습니다.

예를 들어, 아래의 버킷 정책에서 설명하는 것과 같이 Amazon S3 버킷 정책의 aws:SecureTransport 조건을 사용하여 HTTPS(TLS)를 통한 암호화된 연결만 사용하는 것이 좋습니다.

Amazon S3와 같은 다른 AWS 서비스를 사용한 전송 중 데이터 암호화에 대한 자세한 내용은 Amazon S3 사용 설명서의 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

키 관리

AWS Data Transfer Terminal은 고객 관리형 키를 직접 지원하지 않습니다. Data Transfer Terminal 예약 중에 연결하는 AWS 서비스에 사용할 수 있는 고객 관리형 키 지원을 사용하세요. AWS Key Management Service 개발자 안내서의 AWS KMS 키 섹션에서 고객 관리형 키와 저장 데이터를 암호화하는 방법을 자세히 알아봅니다.

인터네트워크 트래픽 개인 정보 보호

Data Transfer Terminal 콘솔 액세스는 게시된 서비스 API를 통해 이루어집니다. Data Transfer Terminal 리소스는 가상 프라이빗 클라우드(VPC)와는 독립적입니다.

Data Transfer Terminal ID 및 액세스 관리

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 관리자의 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 Data Transfer Terminal 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한이 있음) 대상을 관리합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

대상

AWS Identity and Access Management(IAM)를 사용하는 방법은 Data Transfer Terminal에서 수행하는 작업에 따라 달라집니다.

서비스 사용자 - Data Transfer Terminal 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Data Transfer Terminal 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Data Transfer Terminal에서 기능에 액세스할 수 없는 경우 AWS Data Transfer Terminal ID 및 액세스 문제 해결을 참조하세요.

서비스 관리자 - 회사에서 Data Transfer Terminal 리소스를 책임지고 있다면 Data Transfer Terminal에 대한 완전한 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Data Transfer Terminal 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Data Transfer Terminal에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Data Transfer Terminal과 IAM의 작동 방식 섹션을 참조하세요.

IAM 관리자 – IAM 관리자라면 Data Transfer Terminal에 대한 액세스 관리 정책 작성 방법을 자세히 알고 있어야 합니다. IAM에서 사용할 수 있는 Data Transfer Terminal ID 기반 정책을 보려면 AWS Data Transfer Terminal의 ID 기반 정책 예제를 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자나 IAM 사용자로 또는 IAM 역할을 수임하여 인증(AWS에 로그인)되어야 합니다.

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 AWS에 로그인할 수 있습니다. AWS IAM ID 센터 사용자, 회사의 통합 인증, Google 또는 Facebook 자격 증명은 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임합니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. AWS 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서에서 AWS 계정에 로그인하는 방법을 참조하세요.

AWS에 프로그래밍 방식으로 액세스하는 경우, AWS에서는 보안 인증 정보를 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK) 및 명령줄 인터페이스(CLI)를 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용 AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 IAM의 AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 ID로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구합니다.

페더레이션 ID는 엔터프라이즈 사용자 디렉터리, 웹 ID 제공업체, AWS Directory Service, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하

는 모든 사용자입니다. 페더레이션 ID는 AWS 계정에 액세스할 때 역할을 수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정 및 애플리케이션에서 사용하기 위해 고유한 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정 내 ID입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS 계정 내 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. AWS Management Console에서 일시적으로 IAM 역할을 수임하려면 사용자에서 IAM 역할로 전환(콘솔)하면 됩니다. AWS CLI 또는 AWS API 작업을 직접 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다.

인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스를 사용하면 역할을 (프록시로 사용하는 대신) 리소스에 정책을 직접 연결할 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 – 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어, 서비스에서 직접 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 주체의 권한을 요청하는 AWS 서비스와 결합하여 다운스트림 서비스에 요청합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 – 서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 생성하고 AWS ID 또는 리소스에 연결하여 AWS에서 내 액세스를 제어합니다. 정책은 ID 또는 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 AWS에 JSON 문서로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWSJSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 보유한 사용자는 AWS Management Console, AWS CLI 또는 AWS API에서 역할에 대한 정보를 얻을 수 있습니다.

자격 증명 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 AWS 계정에 속한 다수의 사용자, 그룹 및 역할에게 독립적으로 추가할 수 있는 정책입니다. 관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함되어 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연합된 사용자 또는 AWS 서비스가 포함될 수 있습니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3, AWS WAF 및 Amazon VPC는 ACL을 지원하는 대표적인 서비스입니다. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS는 비교적 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) – SCP는 AWS조직에서 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations는 비즈니스가 소유하는 여러 AWS 계정을 그룹화하고 중앙에서 관리할 수 있는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자를 비롯하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. SCP에 대한 자세한 내용은 AWS 조직 사용 설명서에서 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 관계없이 AWS 계정 루트 사용자를 포함한 ID에 대한 유효 권한에 영향을 줄 수 있습니다. RCP를 지원하는 AWS 서비스 목록을 포함하여 Organizations 및 RCP에 대한 자세한 내용은 AWS 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의

자격 증명 기반 정책과 세션 정책의 교집합입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련될 때 AWS가 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용자 설명서의 정책 평가 로직을 참조하세요.

Data Transfer Terminal과 IAM의 작동 방식

IAM을 사용하여 Data Transfer Terminal에 대한 액세스를 관리할 수 있도록 Data Transfer Terminal에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM 특성	Data Transfer Terminal 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	예
위탁자 권한	아니요
서비스 역할	아니요
서비스 연결 역할	아니요

Data Transfer Terminal 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

Data Transfer Terminal의 ID 기반 정책

자격 증명 기반 정책 지원: 예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Data Transfer Terminal의 ID 기반 정책 예제

Data Transfer Terminal ID 기반 정책의 예제를 보려면 AWS Data Transfer Terminal의 ID 기반 정책 예제를 참조하세요.

Data Transfer Terminal 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연합된 사용자 또는 AWS 서비스가 포함될 수 있습니다.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 위탁자와 리소스가 서로 다른 AWS 계정에 있는 경우, 신뢰할 수 있는 계정의 IAM 관리자는 위탁자 엔터티(사용자 또는 역할)에도 리소스 액세스 권한을 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Data Transfer Terminal의 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Data Transfer Terminal 작업 목록을 보려면 서비스 승인 참조의 AWS Data Transfer Terminal에서 정의한 작업을 참조하세요.

Data Transfer Terminal의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
datatransferterminal
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

Data Transfer Terminal ID 기반 정책의 예제를 보려면 AWS Data Transfer Terminal의 ID 기반 정책 예제를 참조하세요.

Data Transfer Terminal의 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 명령문이 모든 리소스에 적용됨을 나타냅니다.

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

Data Transfer Terminal 리소스 유형 및 해당 ARN 목록을 보려면 서비스 승인 참조에서 AWS Data Transfer Terminal에서 정의한 리소스 섹션을 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Data Transfer Terminal에서 정의한 작업을 참조하세요.

Data Transfer Terminal ID 기반 정책의 예제를 보려면 AWS Data Transfer Terminal의 ID 기반 정책 예제를 참조하세요.

Data Transfer Terminal의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` 요소는 선택 사항입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우, AWS는 논리적 `OR` 작업을 사용하여 조건을 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Data Transfer Terminal 조건 키 목록을 보려면 서비스 승인 참조의 AWS Data Transfer Terminal의 조건 키 섹션을 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS Data Transfer Terminal에서 정의한 작업을 참조하세요.

Data Transfer Terminal ID 기반 정책의 예제를 보려면 AWS Data Transfer Terminal의 ID 기반 정책 예제를 참조하세요.

Data Transfer Terminal의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Data Transfer Terminal을 사용한 ABAC

ABAC 지원(정책의 태그): 아니요

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티(사용자 또는 역할) 및 많은 AWS리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 :`aws:ResourceTag/[replaceable]key-name `, , or aws:TagKeys condition keys.`을 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. 서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우 해당 서비스의 값은 Yes입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다. ABAC에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용자 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Data Transfer Terminal에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요.

사용자 이름과 암호를 제외한 다른 방법을 사용하여 AWS에 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 사용하여 AWS에 액세스하면 해당 프로세스에서 자동으로 임시 보안 인증 정보를 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 AWS에 액세스할 수 있습니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Data Transfer Terminal의 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 아니요

IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 위탁자로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 주체의 권한을 요청하는 AWS 서비스와 결합하여 다운스트림 서비스에 요청합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Data Transfer Terminal의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Data Transfer Terminal 기능에 문제가 발생할 수 있습니다. Data Transfer Terminal에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Data Transfer Terminal의 서비스 연결 역할

서비스 연결 역할 지원: 아니요

서비스 연결 역할은 AWS서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는 AWS서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS Data Transfer Terminal의 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Data Transfer Terminal 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용해 태스크를 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조에서 작업을 참조하세요.

주제

- 정책 모범 사례
- Data Transfer Terminal 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Data Transfer Terminal 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책 또는 AWS직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용자 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS CloudFormation와 같이, 특정 AWS 서비스를 통해 사용되는 경

우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 IAM 사용자 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용자 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우, 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용자 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용자 설명서의 IAM의 보안 모범 사례를 참조하세요.

Data Transfer Terminal 콘솔 사용

AWS Data Transfer Terminal 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한은 AWS 계정에서 Data Transfer Terminal 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Data Transfer Terminal 콘솔을 계속 사용할 수 있도록 하려면 *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결해야 합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Data Transfer Terminal ID 및 액세스 문제 해결

다음 정보를 사용하여 Data Transfer Terminal 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Data Transfer Terminal에서 작업을 수행할 권한이 없음
- AWS 계정 외부의 사람이 Data Transfer Terminal 리소스에 액세스할 수 있도록 허용하고 싶음

Data Transfer Terminal에서 작업을 수행할 권한이 없음

AWS Data Transfer Terminal 콘솔에서 예약을 보거나 예약할 수 없는 경우 필요한 권한이 없을 수 있습니다. 계정 관리자에게 문의하여 액세스 권한과 적절한 권한을 부여하는 IAM ID 정책을 구성합니다.

AWS 계정 외부의 사람이 Data Transfer Terminal 리소스에 액세스할 수 있도록 허용하고 싶음

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Data Transfer Terminal에서 이러한 기능을 지원하는지 여부를 알아보려면 Data Transfer Terminal과 IAM의 작동 방식 섹션을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 서드 파티 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 서드 파티가 소유한 AWS 계정에 대한 액세스 제공을참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용자 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용자 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Data Transfer Terminal API 참조: 작업 및 리소스

AWS Identity and Access Management(IAM) 정책을 생성할 때 이 페이지는 AWS Data Transfer Terminal API 작업, 수행할 권한을 부여할 수 있는 해당 작업, 권한을 부여할 수 있는 해당 작업, 권한을 부여할 수 있는 대상 AWS 리소스 간의 관계를 이해하는 데 도움이 될 수 있습니다.

일반적으로 정책에 Data Transfer Terminal 권한을 추가하는 방법은 다음과 같습니다.

- `Action` 요소에 작업을 지정합니다. 값에는 `datatransferterminal:`접두사와 API 작업 이름이 포함됩니다. 예를 들어 `datatransferterminal:CreateTask`입니다.
- `Resource`요소의 작업과 관련된 AWS리소스를 지정합니다.

Data Transfer Terminal 정책에서 AWS조건 키를 사용할 수도 있습니다. AWS 키의 전체 목록은 IAM 사용 설명서의 사용 가능한 키를 참조하십시오.

Data Transfer Terminal API 작업 및 해당 작업

CreateTransferTeam

- 작업: `datatransferterminal:CreateTransferTeam`

  리소스: `None`

GetTransferTeam

- 작업: `datatransferterminal:GetTransferTeam`

  리소스: `arn:aws:::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

UpdateTransferTeam

- 작업: `datatransferterminal:UpdateTransferTeam`

  리소스: `arn:aws:::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

DeleteTransferTeam

- 작업: `datatransferterminal:DeleteTransferTeam`

  리소스: `arn:aws:::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

ListTransferTeams

- 작업: `datatransferterminal:ListTransferTeams`

  리소스: `None`

RegisterPerson

- 작업: `datatransferterminal:RegisterPerson`

  리소스: `arn:aws:::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

GetPerson

- 작업: `datatransferterminal:GetPerson`

리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

종속 작업: datatransferterminal:GetTransferTeam

종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId````

DeregisterPerson

- 작업: datatransferterminal:DeregisterPerson

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  종속 작업: datatransferterminal:GetTransferTeam

  종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListPersons

- 작업: datatransferterminal:ListPersons

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

CreateReservation

- 작업: datatransferterminal:CreateReservation

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

  종속 작업: datatransferterminal:GetTransferTeam

종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId````

종속 작업: datatransferterminal:GetPerson

종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

종속 작업: datatransferterminal:GetFacility

종속 리소스: arn:aws::
$[replaceable]Partition:datatransferterminal:::facility/
$[replaceable]FacilityId````

GetReservation

- 작업: datatransferterminal:GetReservation

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  종속 작업: datatransferterminal:GetTransferTeam

  종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

UpdateReservation

- 작업: datatransferterminal:UpdateReservation

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  종속 작업: datatransferterminal:GetTransferTeam

종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId````

종속 작업: datatransferterminal:GetPerson

종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

DeleteReservation

- 작업: datatransferterminal:DeleteReservation

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  종속 작업: datatransferterminal:GetTransferTeam

  종속 리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListReservations

- 작업: datatransferterminal:ListReservations

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListFacilities

- 작업: datatransferterminal:ListFacilities

  리소스: None

GetFacility

- 작업: datatransferterminal:GetFacility

  리소스: arn:aws::$[replaceable]Partition:datatransferterminal:::facility/
  $[replaceable]FacilityId````

GetFacilityAvailability

- 작업: `datatransferterminal:GetFacilityAvailability`

  리소스: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

  종속 작업: `datatransferterminal:GetFacility`

  종속 리소스: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

AWS Data Transfer Terminal의 규정 준수 검증

AWS 서비스가 특정 규정 준수 프로그램의 범위 내에 있는지 확인하려면 규정 준수 프로그램별 범위 내 AWS 서비스를 참조하고 관심 있는 규정 준수 프로그램을 선택하세요. 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact의 보고서 다운로드를 참조하세요.

AWS 서비스를 사용할 때 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS는 규정 준수를 지원하기 위해 다음과 같은 리소스를 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모든 AWS 서비스가 HIPAA에 적합한 것은 아닙니다.
- AWS 규정 준수 리소스 – 사용자의 업계와 위치에 해당할 수 있는 워크북 및 안내서 모음입니다.
- https://d1-awsstatic-com-whitepapers-compliance-AWS-Customer-Compliance-Guides-pdf[AWS 고객 규정 준수 안내서] – 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에서는 AWS 서비스를 보호하기 위한 모범 사례를 요약하고 여러 프레임워크(미국 표준 기술 연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제 표준화기구(ISO) 등)에서 보안 제어에 대한 지침을 매핑합니다.
- AWS 구성 개발자 가이드의 규칙으로 리소스 평가하기 - AWS 구성 서비스는 리소스 구성이 내부 관행, 업계 가이드라인 및 규정을 얼마나 잘 준수하는지 평가합니다.

- AWS 보안 허브- 이 AWS 서비스는 AWS 내의 보안 상태에 대한 포괄적인 보기를 제공합니다. Security Hub는 보안 컨트롤을 사용하여 AWS리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 이 AWS 서비스는 의심스럽고 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager – 이 AWS 서비스는 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 산업 표준의 준수를 관리하는 방법을 간소화하는 데 도움이 됩니다.

AWS Data Transfer Terminal의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS글로벌 인프라를 참조하세요.

AWS Data Transfer Terminal은 전 세계 여러 위치에서 사용할 수 있습니다. 인터넷에서 액세스할 수 있는 AWS 리전에 연결할 수 있습니다.

Data Transfer Terminal의 로깅 및 모니터링

AWS Data Transfer Terminal은 Data Transfer Terminal에서 사용자, 역할, AWS 서비스가 수행한 작업의 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Data Transfer Terminal에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Data Transfer Terminal 콘솔로부터의 호출과 Data Transfer Terminal API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Data Transfer Terminal 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Data Transfer Terminal에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간, 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Data Transfer Terminal 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Data Transfer Terminal에서 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하십시오.

Data Transfer Terminal 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려는 경우 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS Region에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Data Transfer Terminal 작업은 CloudTrail에서 로깅되고 이 설명서의 Data Transfer Terminal API 참조: 작업 및 리소스 섹션에 설명되어 있습니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자 자격 증명으로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지 여부.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Data Transfer Terminal 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타

내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출에 대한 순서가 지정된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

AWS Data Transfer Terminal의 인프라 보안

관리형 서비스인 AWS Data Transfer Terminal은 {https---d0-awsstatic-com-whitepapers-Security-AWS-Security-Whitepaper-pdf}[Amazon Web Services: Overview of Security Processes] 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS에서 게시한 API 직접 호출을 사용하여 네트워크를 통해 Data Transfer Terminal에 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 시크릿 액세스 키를 사용하여 서명해야 합니다. AWS 보안 토큰 서비스(AWS STS)를 사용하여 요청에 서명하기 위한 임시 보안 자격 증명을 생성할 수도 있습니다.

Data Transfer Terminal 사용 설명서 문서 기록

다음 표는 이 안내서에 대한 문서 기록을 설명합니다.

변경 사항	설명	날짜
레이아웃 업데이트	문서 레이아웃과 사소한 문구 업데이트 및 콘텐츠 편집.	2025년 1월 1일
최초 게시	원본 설명서 게시 날짜.	2024년 12월 1일