aws

개발자 가이드

# AMB 액세스 비트코인

# AMB 액세스 비트코인: 개발자 가이드

# Table of Contents

# Amazon Managed Blockchain(AMB) Access Bitcoin이란 무엇인가요?

Amazon Managed Blockchain(AMB) Access는 Ethereum 및 Bitcoin용 퍼블릭 블록체인 노드를 제공하며 Hyperledger Fabric 프레임워크를 사용하여 프라이빗 블록체인 네트워크를 생성할 수도 있습니다. 완전 관리형, 단일 테넌트(전용) 및 서버리스 다중 테넌트 API 작업부터 퍼블릭 블록체인 노드에 이르기까지 퍼블릭 블록체인에 참여할 다양한 방법 중에서 선택합니다. 액세스 제어가 중요한 사용 사례의 경우 완전 관리형 프라이빗 블록체인 네트워크 중에서 선택할 수 있습니다. 표준화된 API 작업을 통해 완전 관리형의 복원력이 뛰어난 인프라에서 즉각적인 확장성을 제공하므로 블록체인 애플리케이션을 구축할 수 있습니다.

AMB Access는 멀티테넌트 블록체인 네트워크 액세스 API 작업과 전용 블록체인 노드 및 네트워크라는 두 가지 유형의 블록체인 인프라 서비스를 제공합니다. 전용 블록체인 인프라를 사용하면 자체 용도로 퍼블릭 Ethereum 블록체인 노드와 프라이빗 Hyperledger Fabric 블록체인 네트워크를 생성하고 사용할 수 있습니다. 그러나 AMB Access Bitcoin과 같은 다중 테넌트 API 기반 상품은 기본 블록체인 노드 인프라가 고객 간에 공유되는 API 계층 뒤의 Bitcoin 노드 플릿으로 구성됩니다.

Bitcoin은 네트워크의 기본 암호화폐인 Bitcoin(BTC)에서 표시되지 않은 안전한 peer-to-peer 값 트랜잭션을 지원하는 분산형 블록체인 네트워크입니다. Bitcoin 네트워크는 개인, 금융 기관, 핀테크 회사, 정부 등이 사용합니다. Bitcoin 네트워크는 교환 수단, 투자 상품 또는 인스크립팅된 데이터에 대한 공개적으로 확인 가능하고 변경이 불가능한 원장입니다. Amazon Managed Blockchain(AMB) Access Bitcoin을 사용하면 리전 엔드포인트를 통해 Bitcoin Mainnet 및 Testnet 네트워크 풀에 액세스할 수 있습니다.이 풀을 통해 트랜잭션을 작성하고, 원장에서 데이터를 읽고, Bitcoin Core 노드 클라이언트에서 사용할 수 있는 JSON-RPC 요청을 호출할 수 있습니다. 서버리스 Bitcoin 엔드포인트를 사용하면 Bitcoin 노드 프로비저닝, 유지 관리 및 로드 밸런싱과 같은 차별화되지 않은 작업에 투자하는 대신 애플리케이션을 구축하는 데 집중할 수 있습니다. Bitcoin Wallet을 빌드하든 암호화 교환을 빌드하든 Bitcoin 블록체인 데이터를 분석하든 상관없이 AMB Access Bitcoin을 사용하여 Bitcoin 엔드포인트를 통해 수행한 요청에 대해서만 비용을 지불합니다.

## AMB Access Bitcoin을 처음 사용하십니까?

AMB Access Bitcoin을 처음 사용하는 경우 먼저 다음 섹션을 읽는 것이 좋습니다.

- 주요 개념: Amazon Managed Blockchain(AMB) Access Bitcoin
- Amazon Managed Blockchain(AMB) 액세스 Bitcoin 시작하기
- Amazon Managed Blockchain(AMB) Access Bitcoin을 사용한 Bitcoin 사용 사례

- Amazon Managed Blockchain(AMB) 액세스 Bitcoin에서 지원되는 Bitcoin JSON-RPCs

# 주요 개념: Amazon Managed Blockchain(AMB) Access Bitcoin

> **Note**
>
> 이 안내서에서는 Bitcoin에 필수적인 개념을 잘 알고 있다고 가정합니다. 이러한 개념에는 분산, 노드, 트랜잭션, proof-of-work, Wallet, 퍼블릭 및 프라이빗 키, 절반 등이 포함됩니다. Amazon Managed Blockchain(AMB) Access Bitcoin을 사용하기 전에 Bitcoin 개발 설명서 및 마스터링 Bitcoin을 검토하는 것이 좋습니다.

Amazon Managed Blockchain(AMB) Access Bitcoin은 노드를 포함한 Bitcoin 인프라를 프로비저닝하고 관리할 필요 없이 Bitcoin 블록체인에 대한 서버리스 액세스를 제공합니다. 이 관리형 서비스를 사용하여 Bitcoin 네트워크에 빠르고 온디맨드 방식으로 액세스하여 전체 소유 비용을 절감할 수 있습니다.

AMB Access Bitcoin을 사용하면 Bitcoin Core 클라이언트를 실행하는 전체 노드를 통해 Bitcoin 네트워크에 액세스할 수 있으며, Wallet 기능이 비활성화되고 여러 JSON 원격 프로시저(JSON-RPC) 호출을 지원합니다. Bitcoin JSON RPCs 호출하여 Managed Blockchain에서 관리하는 Bitcoin 노드와 통신하여 Bitcoin 네트워크와 상호 작용할 수 있습니다. Bitcoin JSON-RPCs 사용하면 Amazon Managed Blockchain 서비스를 사용하여 데이터 쿼리 및 Bitcoin 네트워크에 트랜잭션 제출을 포함한 데이터를 읽고 트랜잭션을 쓸 수 있습니다.

> **Important**
>
> Bitcoin 주소를 생성, 유지 관리, 사용 및 관리하는 것은 사용자의 책임입니다. 또한 Bitcoin 주소의 콘텐츠에 대해서도 책임이 있습니다. AWS 는 Amazon Managed Blockchain에서 Bitcoin 노드를 사용하여 배포되거나 호출된 트랜잭션에 대해서는 책임을 지지 않습니다.

## Amazon Managed Blockchain(AMB) Access Bitcoin 사용에 대한 고려 사항 및 제한 사항

- 지원되는 Bitcoin 네트워크

  AMB Access Bitcoin은 다음과 같은 퍼블릭 네트워크를 지원합니다.

- 메인넷 proof-of-work 합의로 보호되고 Bitcoin(BTC) 암호화폐가 발급 및 처리되는 퍼블릭 Bitcoin 블록체인입니다. Mainnet의 트랜잭션은 실제 값(즉, 실제 비용이 발생함)을 가지며 퍼블릭 블록체인에 기록됩니다.
- Testnet - 테스트넷은 테스트에 사용되는 대체 Bitcoin 블록체인입니다. Testnet 코인은 실제 Bitcoin(BTC)과 별개이며 일반적으로 값이 없습니다.

> **Note**
>
> 프라이빗 네트워크는 지원되지 않습니다.

- 지원되는 리전

  다음은이 서비스에 지원되는 리전입니다.

| 리전 이름 | 코드 | 리전 |
|---|---|---|
| 미국 동부(버지니아 북부) | IAD | us-east-1 |
| 아시아 태평양(도쿄) | ™ | ap-northeast-1 |
| 아시아 태평양(서울) | ICN | ap-northeast-2 |
| 아시아 태평양(싱가포르) | SIN | ap-southeast-1 |
| 유럽(아일랜드) | DUB | eu-west-1 |
| 유럽(런던) | LHR | eu-west-2 |

- Service endpoints

  다음은 AMB Access Bitcoin의 서비스 엔드포인트입니다. 서비스와 연결하려면 지원되는 리전 중 하나가 포함된 엔드포인트를 사용해야 합니다.

  - `mainnet.bitcoin.managedblockchain.`*`Region`*`.amazonaws.com`
  - `testnet.bitcoin.managedblockchain.`*`Region`*`.amazonaws.com`

  예: `mainnet.bitcoin.managedblockchain.eu-west-2.amazonaws.com`

- 채굴이 지원되지 않음

  AMB Access Bitcoin은 Bitcoin(BTC) 마이닝을 지원하지 않습니다.

- Bitcoin JSON-RPC 호출의 서명 버전 4 서명

  Amazon Managed Blockchain에서 Bitcoin JSON-RPCs를 호출할 때 서명 버전 4 서명 프로세스를 사용하여 인증된 HTTPS 연결을 통해 호출할 수 있습니다. 즉, 계정의 AWS 승인된 IAM 보안 주체만 Bitcoin JSON-RPC를 호출할 수 있습니다. 이렇게 하려면 호출과 함께 AWS 자격 증명(액세스 키 ID 및 보안 액세스 키)을 제공해야 합니다.

  > **Important**
  > - 사용자 대면 애플리케이션에 클라이언트 자격 증명을 포함시키지 마십시오.
  > - IAM 정책을 사용하여 개별 Bitcoin JSON-RPCs에 대한 액세스를 제한할 수 없습니다.

- 원시 트랜잭션 제출만 지원됩니다.

  `sendrawtransaction` JSON-RPC를 사용하여 Bitcoin 블록체인 상태를 업데이트하는 트랜잭션을 제출합니다.

- AWS CloudTrail 로깅 지원

  Bitcoin JSON-RPC를 로깅하도록 CloudTrail을 구성할 수 있습니다.RPCs 자세한 내용은 를 사용하여 Amazon Managed Blockchain(AMB) 액세스 Bitcoin 이벤트 로깅 AWS CloudTrail 섹션을 참조하세요.

# Amazon Managed Blockchain(AMB) 액세스 Bitcoin 설정

Amazon Managed Blockchain(AMB) Access Bitcoin을 처음 사용하기 전에이 섹션의 단계에 따라 AWS 계정을 생성합니다. 다음 장에서는 AMB Access Bitcoin 사용을 시작하는 방법을 설명합니다.

## 필수 조건 및 고려 사항

AWS 를 처음 사용하려면 먼저이 있어야 합니다 AWS 계정.

### 에 가입 AWS

에 가입하면 Amazon Managed Blockchain(AMB) Access Bitcoin을 AWS 서비스포함한 모든에 AWS 가 자동으로 등록 AWS 계정 됩니다. 사용한 서비스에 대해서만 청구됩니다.

가 AWS 계정 이미 있는 경우 다음 단계로 이동합니다. AWS 계정이 없는 경우에는 다음 절차에 따라 계정을 만드세요.

AWS 계정을 생성하려면

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

   가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

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

## 적절한 권한을 가진 IAM 사용자 생성

AMB Access Bitcoin을 생성하고 사용하려면 필요한 관리형 블록체인 작업을 허용하는 권한이 있는 AWS Identity and Access Management (IAM) 보안 주체(사용자 또는 그룹)가 있어야 합니다.

IAM 보안 주체만 Bitcoin JSON-RPC 호출을 수행할 수 있습니다. Amazon Managed Blockchain에서 Bitcoin JSON-RPCs를 호출할 때 서명 버전 4 서명 프로세스를 사용하여 인증된 HTTPS 연결을 통해

호출할 수 있습니다. 즉, 계정의 AWS 승인된 IAM 보안 주체만 Bitcoin JSON-RPC를 호출할 수 있습니다. 이렇게 하려면 호출과 함께 AWS 자격 증명(액세스 키 ID 및 보안 액세스 키)을 제공해야 합니다.

IAM 사용자를 생성하는 방법에 대한 자세한 내용은 계정에서 IAM 사용자 생성을 참조하세요 AWS. 사용자에게 권한 정책을 연결하는 방법에 대한 자세한 내용은 IAM 사용자의 권한 변경을 참조하세요. 사용자에게 AMB Access Bitcoin 작업 권한을 부여하는 데 사용할 수 있는 권한 정책의 예는 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

## AWS Command Line Interface설치 및 구성

아직 설치하지 않은 경우 터미널의 AWS 리소스로 작업할 최신 AWS 명령줄 인터페이스(CLI)를 설치합니다. 자세한 내용은 최신 버전의 AWS CLI설치 또는 업데이트를 참조하세요.

> **Note**
>
> CLI 액세스를 위해서는 액세스 키 ID 및 비밀 액세스 키가 필요합니다. 가능하다면 장기 액세스 키 대신 임시 보안 인증 정보를 사용하세요. 임시 보안 인증도 액세스 키 ID와 비밀 액세스 키로 구성되지만 보안 인증이 만료되는 시간을 나타내는 보안 토큰이 포함되어 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 리소스에서 임시 자격 증명 사용을 참조하세요.

# Amazon Managed Blockchain(AMB) 액세스 Bitcoin 시작하기

이 섹션의 step-by-step 자습서를 사용하여 Amazon Managed Blockchain(AMB) Access Bitcoin을 사용하여 작업을 수행하는 방법을 알아봅니다. 이 예제에서는 몇 가지 사전 조건을 완료해야 합니다. AMB Access Bitcoin을 처음 사용하는 경우이 가이드의 설정 섹션을 검토하여 이러한 사전 조건을 완료했는지 확인하세요. 자세한 내용은 Amazon Managed Blockchain(AMB) 액세스 Bitcoin 설정 단원을 참조하십시오.

주제

- Bitcoin JSON-RPCs에 액세스하기 위한 IAM 정책 생성
- 를 사용하여 AMB Access RPC 편집기에서 Bitcoin 원격 프로시저 호출(RPC) 요청 AWS Management Console
- 를 사용하여 awscurl에서 AMB Access Bitcoin JSON-RPC 요청 AWS CLI
- Node.js에서 Bitcoin JSON-RPC 요청
- 에서 AMB Access Bitcoin 사용 AWS PrivateLink

## Bitcoin JSON-RPCs에 액세스하기 위한 IAM 정책 생성

Bitcoin Mainnet 및 Testnet의 퍼블릭 엔드포인트에 액세스하여 JSON-RPC 호출을 수행하려면 Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 적절한 IAM 권한이 있는 사용자 자격 증명(AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY)이 있어야 합니다. 이 AWS CLI 설치된 터미널에서 다음 명령을 실행하여 두 Bitcoin 엔드포인트에 모두 액세스하는 IAM 정책을 생성합니다.

```
cat <<EOT > ~/amb-btc-access-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AMBBitcoinAccessPolicy",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
```

```
EOT
aws iam create-policy --policy-name AmazonManagedBlockchainBitcoinAccess --policy-
document file://$HOME/amb-btc-access-policy.json
```

> **Note**
>
> 이전 예제에서는 Bitcoin Mainnet과 Testnet 모두에 대한 액세스 권한을 제공합니다. 특정 엔드포인트에 액세스하려면 다음 `Action` 명령을 사용합니다.
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

정책을 생성한 후 해당 정책을 IAM 사용자의 역할에 연결하면 정책이 적용됩니다.
에서 IAM 서비스로 AWS Management Console이동하여 IAM 사용자에게 할당된 `AmazonManagedBlockchainBitcoinAccess` 역할에 정책을 연결합니다. 자세한 내용은 역할 생성 및 IAM 사용자에게 할당을 참조하세요.

# 를 사용하여 AMB Access RPC 편집기에서 Bitcoin 원격 프로시저 호출(RPC) 요청 AWS Management Console

AMB 액세스를 AWS Management Console 사용하여에서 원격 프로RPCs)을 편집하고 제출할 수 있습니다. 이러한 RPCs 사용하면 Bitcoin 네트워크에서 데이터를 읽고, 쓰고, 트랜잭션을 제출할 수 있습니다.

Example

다음 예제에서는 `getBlock` RPC를 사용하여 `00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09blockhash`에 대한 정보를 가져오는 방법을 보여줍니다. 강조 표시된 변수를 자체 입력으로 바꾸거나 나열된 다른 RPC 방법 중 하나를 선택하고 필요한 관련 입력을 입력합니다.

1. https://console.aws.amazon.com/managedblockchain/://https://https://https://https://https://https://https://https://https://https
2. RPC 편집기를 선택합니다.
3. 요청 섹션에서를 블록체인 네트워크*BITCOIN_MAINNET*로 선택합니다.
4. RPC 메*getblock*서드로를 선택합니다.

5. 블록 번호로 *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09*를 입력하고 세부 정보로 *0*를 선택합니다.
6. 그런 다음 RPC 제출을 선택합니다.
7. 이 페이지의 응답 섹션에 결과가 표시됩니다. 그런 다음 전체 원시 트랜잭션을 복사하여 추가 분석을 수행하거나 애플리케이션의 비즈니스 로직에 사용할 수 있습니다.

자세한 내용은 AMB Access Bitcoin에서 지원하는 RPCs.

# 를 사용하여 awscurl에서 AMB Access Bitcoin JSON-RPC 요청 AWS CLI

Example

서명 버전 4(SigV4)를 사용하여 IAM 사용자 자격 증명으로 요청에 서명하여 AMB 액세스 Bitcoin 엔드포인트에 대한 Bitcoin JSON-RPC 호출을 수행합니다. awscurl 명령줄 도구는 SigV4를 사용하여 AWS 서비스에 대한 요청에 서명하는 데 도움이 될 수 있습니다. 자세한 내용은 awscurl README.md을 참조하세요.

운영 체제에 적합한 방법을 사용하여 awscurl을 설치합니다. macOS에서는 HomeBrew가 권장되는 애플리케이션입니다.

```
brew install awscurl
```

AWS CLI를 이미 설치하고 구성한 경우 IAM 사용자 자격 증명과 기본 AWS 리전이 환경에 설정되고 awscurl에 액세스할 수 있습니다. awscurl을 사용하여 `getblock` RPC를 호출하여 Bitcoin Mainnet과 Testnet 모두에 요청을 제출합니다. 이 호출은 정보를 검색하려는 블록 해시에 해당하는 문자열 파라미터를 수락합니다.

다음 명령은 `params` 배열의 블록 해시를 사용하여 헤더를 검색할 특정 블록을 선택하여 Bitcoin Mainnet에서 블록 헤더 데이터를 검색합니다. 이 예제에서는 `us-east-1` 엔드포인트를 사용합니다. 이를 Amazon Managed Blockchain(AMB) Access Bitcoin에서 지원하는 선호하는 Bitcoin JSON-RPC 및 AWS 리전으로 바꿀 수 있습니다. 또한 명령에서를 로 대체하여 Mainnet이 아닌 Testnet 네트워크에 대해 요청할 수 `mainnet` `testnet` 있습니다.

```
awscurl -X POST -d '{ "jsonrpc": "1.0", "id": "getblockheader-curltest", "method":
 "getblockheader", "params":
```

```
["000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0"] }' --service
managedblockchain https://mainnet.bitcoin.managedblockchain.us-east-1.amazonaws.com
--region us-east-1 -k
```

결과에는 블록 헤더의 세부 정보와 요청된 블록에 포함된 트랜잭션 해시 목록이 포함됩니다. 다음 예를 참조하세요.

```
{"result":{"hash":"000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0",
      "confirmations":2,"height":799243,"version":664485888,"versionHex":"279b4000",
      "merkleroot":"568e79752e1921ecf40c961435abb41bc5700fe2833ecadc4abfc2f615ddc1b8",
      "time":1689684290,"mediantime":1689681317,"nonce":2091174943,"bits":"17053894",
      "difficulty":53911173001054.59,
      "chainwork":"0000000000000000000000000000000000000004f375cf72ff64e2404c1589c",
      "nTx":2135,

 "previousblockhash":"00000000000000000002ffe4efe07ae74ec8b92c7696f5e12b5da506f015ba6b",

 "nextblockhash":"00000000000000000038f05ddcf3f483fdcb74f4be606c022bcb673424fa4ca"},
      "error":null,"id":"curltest"}
```

# Node.js에서 Bitcoin JSON-RPC 요청

HTTPS를 사용하여 Bitcoin Mainnet 및 Testnet 엔드포인트에 액세스하고 Node.js의 기본 https 모듈을 사용하여 JSON-RPC API를 호출하거나 AXIOS와 같은 타사 라이브러리를 사용하여 서명된 요청을 제출할 수 있습니다. 다음 예제에서는 AMB Access Bitcoin 엔드포인트에 Bitcoin JSON-RPC 요청을 수행하는 방법을 보여줍니다.

Example

이 예제 Node.js 스크립트를 실행하려면 다음 사전 조건을 적용합니다.

1. 시스템에 노드 버전 관리자(nvm) 및 Node.js가 설치되어 있어야 합니다. 여기에서 OS에 대한 설치 지침을 확인할 수 있습니다.
2. `node --version` 명령을 사용하여 노드 버전 14 이상을 사용하고 있는지 확인합니다. 필요한 경우 `nvm install 14` 명령을 사용한 다음 `nvm use 14` 명령을 사용하여 버전 14를 설치할 수 있습니다.
3. 환경 변수 `AWS_ACCESS_KEY_ID` 및 에는 계정과 연결된 자격 증명이 포함되어야 `AWS_SECRET_ACCESS_KEY` 합니다. 환경 변수에는 AMB Access Bitcoin 엔드포인트가 포함되어야 `AMB_HTTP_ENDPOINT` 합니다.

다음 명령을 사용하여 이러한 변수를 클라이언트의 문자열로 내보냅니다. 다음 문자열에서 강조 표시된 값을 IAM 사용자 계정의 적절한 값으로 바꿉니다.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
```

모든 사전 조건을 완료한 후 편집기를 사용하여 다음 `package.json` 파일과 `index.js` 스크립트를 로컬 환경에 복사합니다.

package.json

```
{
  "name": "bitcoin-rpc",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "@aws-crypto/sha256-js": "^4.0.0",
    "@aws-sdk/credential-provider-node": "^3.360.0",
    "@aws-sdk/protocol-http": "^3.357.0",
    "@aws-sdk/signature-v4": "^3.357.0",
    "axios": "^1.4.0"
  }
}
```

index.js

```
const axios = require('axios');
const SHA256 = require('@aws-crypto/sha256-js').Sha256
const defaultProvider = require('@aws-sdk/credential-provider-node').defaultProvider
const HttpRequest = require('@aws-sdk/protocol-http').HttpRequest
const SignatureV4 = require('@aws-sdk/signature-v4').SignatureV4

// define a signer object with AWS service name, credentials, and region
const signer = new SignatureV4({
```

```
  credentials: defaultProvider(),
  service: 'managedblockchain',
  region: 'us-east-1',
  sha256: SHA256,
});


const rpcRequest = async () => {

  // create a remote procedure call (RPC) request object definig the method, input
 params
  let rpc = {
    jsonrpc: "1.0",
    id: "1001",
    method: 'getblock',
    params: ["00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09"]
  }

  //bitcoin endpoint
  let bitcoinURL = 'https://mainnet.bitcoin.managedblockchain.us-
east-1.amazonaws.com/';

  // parse the URL into its component parts (e.g. host, path)
  const url = new URL(bitcoinURL);

  // create an HTTP Request object
  const req = new HttpRequest({
    hostname: url.hostname.toString(),
    path: url.pathname.toString(),
    body: JSON.stringify(rpc),
    method: 'POST',
    headers: {
      'Content-Type': 'application/json',
      'Accept-Encoding': 'gzip',
      host: url.hostname,
    }
  });


  // use AWS SignatureV4 utility to sign the request, extract headers and body
  const signedRequest = await signer.sign(req, { signingDate: new Date() });

  try {
    //make the request using axios
```

```
    const response = await axios({...signedRequest, url: bitcoinURL, data: req.body})

    console.log(response.data)
  } catch (error) {
    console.error('Something went wrong: ', error)
    throw error
  }


}

rpcRequest();
```

이전 샘플 코드는 Axios를 사용하여 Bitcoin 엔드포인트에 RPC 요청을 하고 공식 AWS SDK v3 도구를 사용하여 적절한 서명 버전 4(SigV4) 헤더로 해당 요청에 서명합니다. 코드를 실행하려면 파일과 동일한 디렉터리에서 터미널을 열고 다음을 실행합니다.

```
npm i
node index.js
```

생성된 결과는 다음과 유사합니다.

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
    confirmations":784126,"height":1000, "version":1,"versionHex":"00000001",
    "merkleroot":"fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33",
    "time":1232346882,
    "mediantime":1232344831,"nonce":2595206198,"bits":"1d00ffff","difficulty":1,
    "chainwork":"0000000000000000000000000000000000000000000000000000000000000003e903e903e9",
    "nTx":1,

 "previousblockhash":"0000000008e647742775a230787d66fdf92c46a48c896bfbc85cdc8acc67e87d",
    "nextblockhash":"00000000a2887344f8db859e372e7e4bc26b23b9de340f725afbf2edb265b4c6",
    "strippedsize":216,"size":216,"weight":864,
    "tx":["fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33"]},
    "error":null,"id":"1001"}
```

> **Note**
>
> 이전 스크립트의 샘플 요청은 를 사용하여 awscurl에서 AMB Access Bitcoin JSON-RPC 요청 AWS CLI 예제와 동일한 입력 파라미터 블록 해시를 사용하여 `getblock` 호출합니다. 다른 호

출을 수행하려면 스크립트의 `rpc` 객체를 다른 Bitcoin JSON-RPC로 수정합니다. 호스트 속성 옵션을 Bitcoin으로 변경하여 해당 엔드포인트에서 호출`testnet`할 수 있습니다.

# 에서 AMB Access Bitcoin 사용 AWS PrivateLink

AWS PrivateLink 는 VPC에 있는 것처럼 VPC를 서비스에 비공개로 연결하는 데 사용할 수 있는 가용성과 확장성이 뛰어난 기술입니다. 프라이빗 서브넷에서 서비스와 통신하기 위해 인터넷 게이트웨이, NAT 디바이스, 퍼블릭 IP 주소, AWS Direct Connect 연결 또는 AWS Site-to-Site VPN 연결을 사용할 필요가 없습니다. AWS PrivateLink 또는에 대한 자세한 내용은 란 무엇입니까 AWS PrivateLink?를 AWS PrivateLink참조하십시오.

VPC 엔드포인트를 사용하여를 AWS PrivateLink 통해 AMB Access Bitcoin에 Bitcoin JSON-RPC 요청을 보낼 수 있습니다. 이 프라이빗 엔드포인트에 대한 요청은 개방형 인터넷을 통해 전달되지 않으므로 동일한 SigV4 인증을 사용하여 Bitcoin 엔드포인트로 직접 요청을 보낼 수 있습니다. 자세한 내용은를 통한 AWS 서비스 액세스를 AWS PrivateLink 참조하세요.

서비스 이름의 경우 AWS 서비스 열에서 Amazon Managed Blockchain을 찾습니다. 자세한 내용은 AWS 와 통합되는 서비스를 AWS PrivateLink 참조하세요. 엔드포인트의 서비스 이름은 형식입니다`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

예를 들어 `com.amazonaws.`*`us-east-1`*`.managedblockchain.bitcoin.`*`testnet`*입니다.

# Amazon Managed Blockchain(AMB) Access Bitcoin을 사용한 Bitcoin 사용 사례

이 주제에서는 AMB Access Bitcoin 사용 사례 목록을 제공합니다.

주제



## BTC를 보내고 받을 Bitcoin(BTC) 지갑 구축

Bitcoin 네트워크의 기본 암호화폐인 BTC는 네트워크 보안 모델의 필수 구성 요소입니다. 또한 기관, 기업 및 개인이 널리 사용하는 상품 및 교환 매체 역할을 합니다. 따라서 많은 지갑 애플리케이션은 Bitcoin 노드를 사용하여 Bitcoin 블록체인과 상호 작용합니다. 이러한 애플리케이션은 지정된 주소 집합에 대해 소비되지 않은 출력(UTXOs)의 밸런스를 계산하고, 트랜잭션에 서명하여 Bitcoin 네트워크로 전송하고, 과거 트랜잭션에 대한 데이터를 검색합니다.

다음은 Amazon Managed Blockchain(AMB) Access Bitcoin이 BTC Wallet 트랜잭션에 대해 지원하는 일부 Bitcoin JSON-RPCs의 샘플입니다.

- `estimatesmartfee`
- `createmultisig`
- `createrawtransaction`
- `sendrawtransaction`

자세한 내용은 지원되는 JSON-RPCs 단원을 참조하십시오.

## Bitcoin 블록체인에서 활동 분석

`getchaintxstats` JSON-RPC 메서드를 사용하여 Bitcoin 블록체인에서 트랜잭션 활동의 볼륨을 분석할 수 있습니다. 이 JSON-RPC를 사용하면 초당 평균 트랜잭션 속도, 총 트랜잭션 수, 블록 수 등과

같은 지표에 액세스할 수 있습니다. 원하는 경우 블록 번호 창 또는 블록 해시를 구분 기호로 정의하여 네트워크의 특정 블록 세트에 대해 이러한 통계를 계산할 수도 있습니다.

자세한 내용은 지원되는 JSON-RPCs 단원을 참조하십시오.

## Bitcoin 키 페어를 사용하여 서명된 메시지 확인

비트코인 지갑에는 프라이빗 키와 키 페어를 구성하는 퍼블릭 키가 있습니다. 이러한 키는 트랜잭션에 서명하고 블록체인에서 사용자의 자격 증명 역할을 하는 데 사용됩니다. 퍼블릭 키는 표준화된 영숫자 식별자(27~34자)인 주소를 생성하는 데 사용됩니다. 이러한 주소는 BTC 출력을 수신하고 트랜잭션 또는 메시지를 처리하는 데 사용됩니다.

Bitcoin Wallet을 사용하면 사용자가 암호화 방식으로 메시지에 서명하고 확인할 수도 있습니다. 이 프로세스는 종종 특정 지갑 주소 및 이와 연결된 BTC의 소유권을 증명하는 데 사용됩니다. `verifymessage` Bitcoin JSON-RPC를 사용하면 다른 지갑에서 서명한 메시지의 신뢰성과 유효성을 확인할 수 있습니다. 특히 Bitcoin 노드를 사용하여 서명된 메시지 자체 내에서 제공된 퍼블릭 키 파생 주소에 해당하는 프라이빗 키를 사용하여 메시지가 서명되었는지 확인할 수 있습니다.

자세한 내용은 지원되는 JSON-RPCs 단원을 참조하십시오.

## Bitcoin 멤풀 검사

많은 애플리케이션에서 보류 중인 트랜잭션을 추적하거나, 보류 중인 모든 트랜잭션 목록을 가져오거나, 트랜잭션의 출처를 확인하려면 멤풀에 액세스해야 합니다. 이를 위해이 활동을 지원하는 , `getmempoolancestors` `getmempoolentry`및 같은 Bitcoin JSON-RPCs`getrawmempool`가 있습니다. 이러한 Bitcoin JSON-RPCs 애플리케이션이 멤풀에서 필요한 정보를 얻는 데 도움이 됩니다.

Amazon Managed Blockchain(AMB) Access Bitcoin은 `testmempoolaccept` Bitcoin JSON-RPCs도 지원하므로 트랜잭션이 프로토콜 규칙을 충족하는지, 제출하기 전에 노드에서 수락할 것인지 확인할 수 있습니다. Bitcoin 블록체인에 직접 트랜잭션을 제출하는 지갑, 교환 및 기타 엔터티는 이러한 Bitcoin JSON-RPCs 사용합니다.

자세한 내용은 지원되는 JSON-RPCs 단원을 참조하십시오.

# Amazon Managed Blockchain(AMB) 액세스 Bitcoin에서 지원되는 Bitcoin JSON-RPCs

이 주제에서는 관리형 블록체인이 지원하는 Bitcoin JSON-RPCs의 목록과 참조를 제공합니다. 지원되는 각 JSON-RPC에는 사용에 대한 간략한 설명이 있습니다.

Note

- 서명 버전 4(SigV4) 서명 프로세스를 사용하여 관리형 블록체인에서 Bitcoin JSON-RPCs를 인증할 수 있습니다. 즉, AWS 계정의 승인된 IAM 보안 주체만 Bitcoin JSON-RPCs. 호출과 함께 AWS 자격 증명(액세스 키 ID 및 보안 액세스 키)을 제공합니다.
- HTTP 응답이 10MB보다 크면 오류가 발생합니다. 이를 수정하려면 압축 헤더를 로 설정해야 합니다`Accept-Encoding:gzip`. 그러면 클라이언트가 수신하는 압축된 응답에는 `Content-Type: application/json` 및 헤더가 포함됩니다`Content-Encoding: gzip`.
- Amazon Managed Blockchain(AMB) Access Bitcoin은 잘못된 JSON-RPC 요청에 대해 400 오류를 생성합니다.
- `sendrawtransaction` JSON-RPC를 사용하여 Bitcoin 블록체인 상태를 업데이트하는 트랜잭션을 제출합니다.
- AMB Access Bitcoin의 기본 요청 한도는 AWS 리전별로 별로 초당 요청(RPS) `100NETWORK_TYPE`개입니다.

  할당량을 늘리려면 AWS 지원팀에 문의해야 합니다. AWS 지원에 문의하려면 AWS 지원 센터 콘솔에 로그인합니다. 사례 생성을 선택합니다. 기술을 선택합니다. 관리형 블록체인을 서비스로 선택합니다. 액세스:비트코인을 범주로 선택하고 일반 지침을 심각도로 선택합니다. RPC 할당량을 제목으로 입력하고 설명 텍스트 상자에 리전별 Bitcoin 네트워크당 RPS로 요구 사항에 해당하는 할당량 제한을 나열합니다. 사례를 제출합니다.

## 지원되는 JSON-RPCs

AMB Access Bitcoin은 다음 Bitcoin JSON-RPCs 지원합니다. 지원되는 각 호출에는 사용에 대한 간략한 설명이 있습니다.

| 범주 | JSON-RPC | 설명 |
| --- | --- | --- |
| 블록체인 RPCs | getbestblockhash | 가장 잘 작동하고 완전히 검증된 체인에서 최상의 (팁) 블록의 해시를 반환합니다. |
| | getblock | 세부도가 0인 경우 블록 '해시'에 대해 직렬화된 16진수 인코딩 데이터를 반환합니다. 세부 정보가 1인 경우 블록 '해시'에 대한 정보가 포함된 객체를 반환합니다. 세부 정보가 2인 경우는 블록 '해시'에 대한 정보와 각 트랜잭션에 대한 정보가 포함된 객체를 반환합니다. 세부 정보가 3인 경우는 블록 '해시'에 대한 정보와 입력 정보를 포함하여 각 트랜잭션에 대한 `prevout` 정보가 포함된 객체를 반환합니다. |
| | getblockchaininfo | 블록체인 처리와 관련된 다양한 상태 정보가 포함된 객체를 반환합니다. |
| | getblockcount | 가장 잘 작동하고 완전히 검증된 체인의 높이를 반환합니다. 발생 블록의 높이는 0입니다. |
| | getblockfilter | 블록 해시를 사용하여 특정 블록에 대한 BIP 157 콘텐츠 필터를 검색합니다. |
| | getblockhash | 제공된 높이의 best-block-chain해시를 반환합니다. |
| | getblockheader | verbose가 false인 경우 블록헤더 '해시'에 대해 직렬화된 16진수 인코딩 데이터를 반환합니다. verbose가 true인 경우는 블록헤더 '해시'에 대한 정보가 포함된 객체를 반환합니다. |
| | getblockstats | 지정된 기간에 대한 블록당 계산 통계입니다. 모든 양은 사토시스로 표시됩니다. 잘라내기를 사용하는 일부 높이에서는 작동하지 않습니다. |

| 범주 | JSON-RPC | 설명 |
| --- | --- | --- |
| | getchaintip | 기본 체인 및 분리된 브랜치를 포함하여 블록 트리에서 알려진 모든 팁에 대한 정보를 반환합니다. |
| | getchaintxstats | 체인의 총 트랜잭션 수와 비율에 대한 통계를 계산합니다. |
| | getdifficulty | proof-of-work 난이도를 최소 난이도의 배수로 반환합니다. |
| | getmempoolancestors | txid가 mempool에 있는 경우는 모든 인 mempool 상위 항목을 반환합니다. |
| | getmempooldescendants | txid가 mempool에 있는 경우는 모든 인 mempool 하위 항목을 반환합니다. |
| | getmempoolentry | 지정된 트랜잭션에 대한 mempool 데이터를 반환합니다. |
| | getmempoolinfo | TX 메모리 풀의 활성 상태에 대한 세부 정보를 반환합니다. |
| | getrawmempool | 메모리 풀의 모든 트랜잭션 IDs 문자열 트랜잭션 IDs.<br><br>Note<br>`verbose = true`는 지원되지 않습니다. |
| | gettxout | 미사용 트랜잭션 출력에 대한 세부 정보를 반환합니다. |
| | gettxoutproof | 블록에 “txid”가 포함되었음을 나타내는 16진수 인코딩 증명을 반환합니다. |

| 범주 | JSON-RPC | 설명 |
| --- | --- | --- |
| 원시 트랜잭션 RPCs | createrawtransaction | 지정된 입력을 사용하고 새 출력을 생성하는 트랜잭션을 생성합니다. |
| | decoderawtransaction | 직렬화된 16진수 인코딩 트랜잭션을 나타내는 JSON 객체를 반환합니다. |
| | 디코딩 | 16진수 인코딩 스크립트를 디코딩합니다. |
| | getrawtransaction | 원시 트랜잭션 데이터를 반환합니다. |
| | sendrawtransaction | 원시 트랜잭션(직렬화, 16진수 인코딩)을 로컬 노드 및 네트워크에 제출합니다. |
| | testmempoolaccept | 원시 트랜잭션(직렬화, 16진수 인코딩)을 밈풀에서 수락할지 여부를 나타내는 밈풀 수락 테스트 결과를 반환합니다. 이렇게 하면 트랜잭션이 합의 또는 정책 규칙을 위반하는지 확인합니다. |
| 사용률 RPCs | createmultisig | m 키의 n 서명이 필요한 다중 서명 주소를 생성합니다. |
| | estimatemartfee | 가능하면 트랜잭션이 conf_target 블록 내에서 확인을 시작하는 데 필요한 킬로바이트당 대략적인 요금을 추정하고 추정이 유효한 블록 수를 반환합니다. BIP 141에 정의된 가상 트랜잭션 크기를 사용합니다(증인 데이터는 할인됨). |
| | validateaddress | 지정된 비트코인 주소에 대한 정보를 반환합니다. |
| | verifymessage | 서명된 메시지를 확인합니다. |

# Amazon Managed Blockchain(AMB) Access Bitcoin의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Amazon Managed Blockchain(AMB) Access Bitcoin에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 AWS 준수 프로그램 제공 범위 내 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 사용자는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

Amazon Managed Blockchain은 데이터 보호, 인증 및 액세스 제어를 제공하기 위해 Managed Blockchain에서 실행되는 오픈 소스 프레임워크의 기능과 기능을 사용합니다 AWS .

이 설명서는 AMB Access Bitcoin을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 AMB Access Bitcoin을 구성하는 방법을 보여줍니다. 또한 AMB Access Bitcoin 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- Amazon Managed Blockchain(AMB) Access Bitcoin의 데이터 보호
- Amazon Managed Blockchain(AMB) Access Bitcoin의 ID 및 액세스 관리

## Amazon Managed Blockchain(AMB) Access Bitcoin의 데이터 보호

AWS 공동 책임 모델 Amazon Managed Blockchain(AMB) Access Bitcoin의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 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 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(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 AMB Access Bitcoin 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 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

데이터 암호화는 권한이 없는 사용자가 블록체인 네트워크 및 관련 데이터 스토리지 시스템에서 데이터를 읽지 못하도록 하는 데 도움이 됩니다. 여기에는 전송 중인 데이터라고 하는 네트워크를 이동할 때 가로챌 수 있는 데이터가 포함됩니다.

## 전송 중 암호화

기본적으로 관리형 블록체인은 HTTPS/TLS 연결을 사용하여를 실행하는 AWS CLI 클라이언트 컴퓨터에서 AWS 서비스 엔드포인트로 전송되는 모든 데이터를 암호화합니다.

HTTPS/TLS 사용을 활성화하기 위해 어떤 조치도 필요하지 않습니다. `--no-verify-ssl` 명령을 사용하여 개별 AWS CLI 명령에 대해 명시적으로 비활성화하지 않는 한 항상 활성화됩니다.

# Amazon Managed Blockchain(AMB) Access Bitcoin의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와주는 입니다. IAM 관리자는 AMB Access Bitcoin 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제



## 대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 AMB Access Bitcoin에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - AMB Access Bitcoin 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 AMB Access Bitcoin 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. AMB Access Bitcoin의 기능에 액세스할 수 없는 경우 섹션을 참조하세요Amazon Managed Blockchain(AMB) 액세스 Bitcoin 자격 증명 및 액세스 문제 해결.

서비스 관리자 - 회사에서 AMB Access Bitcoin 리소스를 책임지고 있는 경우 AMB Access Bitcoin에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 AMB Access Bitcoin 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 AMB Access Bitcoin에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin이 IAM과 작동하는 방식.

IAM 관리자 - IAM 관리자인 경우 AMB Access Bitcoin에 대한 액세스를 관리하는 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. IAM에서 사용할 수 있는 AMB Access Bitcoin 자격 증명

기반 정책 예제를 보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

# ID를 통한 인증

인증은 자격 증명 AWS 으로에 로그인하는 방법입니다. , AWS 계정 루트 사용자 IAM 사용자 또는 IAM 역할을 수임하여 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다 AWS IAM Identity Center (.IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하는 경우 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

## AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 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 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명이 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

## IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 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 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 AWS Management Console수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 수 있습니다. 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 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. 페

더레이션 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 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른의 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하려면 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 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 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 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 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그

램이 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 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결 AWS 될 때 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 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 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

### ID 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 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 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 관리자

는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

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 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.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

### 기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 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 ID 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) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 기업이 소유한 여러 AWS 계정 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 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 AWS 계정 루트 사용자관계없이를 포함한 자격 증명의 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을

포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)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 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

### 여러 정책 유형

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

## Amazon Managed Blockchain(AMB) Access Bitcoin이 IAM과 작동하는 방식

IAM을 사용하여 AMB Access Bitcoin에 대한 액세스를 관리하기 전에 AMB Access Bitcoin에서 사용할 수 있는 IAM 기능을 알아봅니다.

Amazon Managed Blockchain(AMB) Access Bitcoin과 함께 사용할 수 있는 IAM 기능

| IAM 기능 | AMB Access Bitcoin 지원 |
|---|---|
| ID 기반 정책 | 예 |
| 리소스 기반 정책 | 아니요 |
| 정책 작업 | 예 |
| 정책 리소스 | 아니요 |
| 정책 조건 키 | 아니요 |
| ACL | 아니요 |
| ABAC(정책 내 태그) | 아니요 |
| 임시 보안 인증 | 아니요 |

| IAM 기능 | AMB Access Bitcoin 지원 |
| --- | --- |
| 보안 주체 권한 | 아니요 |
| 서비스 역할 | 아니요 |
| 서비스 연결 역할 | 아니요 |

AMB Access Bitcoin 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

## AMB Access Bitcoin에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

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.

IAM ID 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 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

AMB Access Bitcoin에 대한 자격 증명 기반 정책 예제

AMB Access Bitcoin 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

## AMB Access Bitcoin 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니

다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 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.

## AMB Access Bitcoin에 대한 정책 작업

정책 작업 지원: 예

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

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 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.

AMB Access Bitcoin 작업 목록을 보려면 서비스 승인 참조의 Amazon Managed Blockchain(AMB) Access Bitcoin에서 정의한 작업을 참조하세요.

AMB Access Bitcoin의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
managedblockchain:
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `InvokeRpcBitcoin`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "managedblockchain::InvokeRpcBitcoin*"
```

AMB Access Bitcoin 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

## AMB Access Bitcoin에 대한 정책 리소스

정책 리소스 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 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 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

AMB Access Bitcoin 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 Amazon Managed Blockchain(AMB) Access Bitcoin에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon Managed Blockchain(AMB) Access Bitcoin에서 정의한 작업을 참조하세요.

AMB Access Bitcoin 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

## AMB Access Bitcoin에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

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

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 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.

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

AMB Access Bitcoin 조건 키 목록을 보려면 서비스 승인 참조의 Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon Managed Blockchain(AMB) Access Bitcoin에서 정의한 작업을 참조하세요.

AMB Access Bitcoin 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제.

## AMB Access BitcoinACLs

ACL 지원: 아니요

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.

## AMB 액세스 Bitcoin이 포함된 ABAC

ABAC 지원(정책의 태그): 아니요

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할)와 많은 AWS 리소스에 태그를 연

결할 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.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

## AMB Access Bitcoin에서 임시 자격 증명 사용

임시 자격 증명 지원: 아니요

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 포함한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는를 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 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 장기 액세스 키를 사용하는 대신 동적으로 임시 자격 증명을 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

## AMB Access Bitcoin에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 아니요

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호

출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하려면 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

### AMB Access Bitcoin의 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 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 AMB Access Bitcoin 기능이 중단될 수 있습니다. AMB Access Bitcoin이 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

### AMB Access Bitcoin에 대한 서비스 연결 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

## Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AMB Access Bitcoin 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 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 ARNs 형식을 포함하여 AMB Access Bitcoin에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Amazon Managed Blockchain(AMB) Access Bitcoin에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- AMB Access Bitcoin 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Bitcoin 네트워크 액세스

## 정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 AMB Access Bitcoin 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 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 사용 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 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 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 제공하

여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.

- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

## AMB Access Bitcoin 콘솔 사용

Amazon Managed Blockchain(AMB) Access Bitcoin 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 AMB Access Bitcoin 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(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 여전히 AMB Access Bitcoin 콘솔을 사용할 수 있도록 하려면 AMB Access Bitcoin *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 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 CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 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": "*"
        }
    ]
}
```

## Bitcoin 네트워크 액세스

> **Note**
>
> Bitcoin의 퍼블릭 엔드포인트에 액세스`mainnet`하고 JSON-RPC 호출`testnet`을 수행하려면 AMB Access Bitcoin에 대한 적절한 IAM 권한이 있는 사용자 자격 증명(`AWS_ACCESS_KEY_ID` 및 `AWS_SECRET_ACCESS_KEY`)이 필요합니다.

### Example 모든 Bitcoin 네트워크에 액세스하기 위한 IAM 정책

이 예제에서는의 IAM 사용자에게 모든 Bitcoin 네트워크에 대한 AWS 계정 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessAllBitcoinNetworks",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Example Bitcoin Testnet 네트워크에 액세스하기 위한 IAM 정책

이 예제에서는 사용자의 IAM 사용자에게 Bitcoin `testnet` 네트워크에 대한 AWS 계정 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessBitcoinTestnet",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcBitcoinTestnet"
            ],
            "Resource": "*"
        }
    ]
}
```

# Amazon Managed Blockchain(AMB) 액세스 Bitcoin 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AMB Access Bitcoin 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- AMB Access Bitcoin에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 AMB Access Bitcoin 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

## AMB Access Bitcoin에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 managedblockchain::*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 managedblockchain::GetWidget on resource: my-example-widget
```

이 경우, managedblockchain::*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

## iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AMB Access Bitcoin에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 AMB Access Bitcoin에서 작업을 수행marymajor하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

## 내 외부의 사람이 내 AMB Access Bitcoin 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하세요.

- AMB Access Bitcoin이 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요Amazon Managed Blockchain(AMB) Access Bitcoin이 IAM과 작동하는 방식.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유의에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

# 를 사용하여 Amazon Managed Blockchain(AMB) 액세스 Bitcoin 이벤트 로깅 AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain(AMB) Access Bitcoin은 관리 이벤트를 지원하지 않습니다.

Amazon Managed Blockchain은 Managed Blockchain의 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 관리형 블록체인에 대한 AMB 액세스 비트코인 엔드포인트를 데이터 영역 이벤트로 호출한 사용자를 캡처합니다.

원하는 데이터 영역 이벤트를 수신하도록 구독하는 적절하게 구성된 추적을 생성하면 AMB Access Bitcoin 관련 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AMB Access Bitcoin 엔드포인트 중 하나에 요청이 이루어졌는지, 요청이 시작된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 기타 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

## CloudTrail의 AMB Access Bitcoin 정보

AWS CloudTrail 는를 생성할 때 기본적으로 활성화됩니다 AWS 계정. 그러나 AMB Access Bitcoin 엔드포인트를 호출한 사용자를 확인하려면 데이터 영역 이벤트를 로깅하도록 CloudTrail을 구성해야 합니다.

AMB Access Bitcoin에 대한 데이터 영역 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성해야 합니다. 추적을 통해 CloudTrail은 Amazon S3 버킷에 로그 파일을 전송합니다. 기본적으로에서 추적을 생성하면 추적 AWS Management Console이 모든에 적용됩니다 AWS 리전. 추적은 AWS 파티션에서 지원되는 모든 리전의 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한이 데이터를 추가로 분석하고 CloudTrail 로그에서 수집된 이벤트 데이터에 대해 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- CloudTrail을 사용하여 Bitcoin JSON-RPCs 추적
- 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

CloudTrail 데이터 이벤트를 분석하여 AMB Access Bitcoin 엔드포인트를 호출한 사용자를 모니터링할 수 있습니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청했는지 여부
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

# AMB Access Bitcoin 로그 파일 항목 이해

데이터 영역 이벤트의 경우 추적은 이벤트를 지정된 S3 버킷에 로그 파일로 전송할 수 있는 구성입니다. 각 CloudTrail 로그 파일에는 모든 소스의 단일 요청을 나타내는 하나 이상의 로그 항목이 포함되어 있습니다. 이러한 항목은 작업의 날짜 및 시간, 연결된 요청 파라미터를 포함하여 요청된 작업에 대한 세부 정보를 제공합니다.

> **Note**
>
> 로그 파일의 CloudTrail 데이터 이벤트는 AMB Access Bitcoin API 호출의 순서가 지정된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

## CloudTrail을 사용하여 Bitcoin JSON-RPCs 추적

CloudTrail을 사용하여 계정에서 AMB Access Bitcoin 엔드포인트를 호출한 사람과 데이터 이벤트로 호출된 JSON-RPC를 추적할 수 있습니다. 기본적으로 추적을 생성하면 데이터 이벤트가 로깅되지 않습니다. AMB Access Bitcoin 엔드포인트를 CloudTrail 데이터 이벤트로 호출한 사용자를 기록하려면 활동을 수집하려는 지원되는 리소스 또는 리소스 유형을 추적에 명시적으로 추가해야 합니다. Amazon Managed Blockchain은 AWS Management Console, AWS SDK 및를 사용하여 데이터 이벤트 추가를

지원합니다 AWS CLI. 자세한 내용은 AWS CloudTrail 사용 설명서의 고급 선택기를 사용하여 이벤트 로깅을 참조하세요.

추적에 데이터 이벤트를 로깅하려면 추적을 생성한 후 put-event-selectors 작업을 사용합니다. `--advanced-event-selectors` 옵션을 사용하여 데이터 이벤트 로깅을 시작하여 AMB Access Bitcoin 엔드포인트를 호출한 사용자를 결정하기 위한 `AWS::ManagedBlockchain::Network` 리소스 유형을 지정합니다.

Example 계정의 모든 AMB 액세스 Bitcoin 엔드포인트 요청의 데이터 이벤트 로그 항목

다음 예제에서는 `put-event-selectors` 작업을 사용하여 `us-east-1` 리전의 추적에 대한 계정의 모든 AMB Access Bitcoin 엔드포인트 요청을 로깅`my-bitcoin-trail`하는 방법을 보여줍니다.

```
aws cloudtrail put-event-selectors \

--region us-east-1 \
--trail-name my-bitcoin-trail  \
--advanced-event-selectors '[{
    "Name": "Test",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::ManagedBlockchain::Network"] } ]}]'
```

구독한 후 이전 예제에서 지정한 추적에 연결된 S3 버킷의 사용량을 추적할 수 있습니다.

다음 결과는 CloudTrail에서 수집한 정보의 CloudTrail 데이터 이벤트 로그 항목을 보여줍니다. Bitcoin JSON-RPC 요청이 AMB Access Bitcoin 엔드포인트 중 하나, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 기타 추가 세부 정보 중 하나에 이루어졌는지 확인할 수 있습니다.

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA554UO62RJ7KSB7FAX:777777777777",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/777777777777",
            "accountId": "111122223333"
        },
        "eventTime": "2023-04-12T19:00:22Z",
        "eventSource": "managedblockchain.amazonaws.com",
        "eventName": "getblock",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "111.222.333.444",
```

```
        "userAgent": "python-requests/2.28.1",
        "errorCode": "-",
        "errorMessage": "-",
        "requestParameters": {
            "jsonrpc": "2.0",
            "method": "getblock",
            "params": [],
            "id": 1
        },
        "responseElements": null,
        "requestID": "DRznHHEjIAMFSzA=",
        "eventID": "baeb232d-2c6b-46cd-992c-0e4033aace86",
        "readOnly": true,
        "resources": [{
            "type": "AWS::ManagedBlockchain::Network",
            "ARN": "arn:aws:managedblockchain:::networks/n-bitcoin-mainnet"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data"
}
```

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.