aws

개발자 가이드

AMB 액세스 비트코인

AMB 액세스 비트코인: 개발자 가이드

Table of Contents

아마존 매니지드 블록체인 (AMB) 액세스 비트코인이란 무엇입니까?

Amazon Managed Blockchain (AMB) Access는 이더리움과 비트코인을 위한 퍼블릭 블록체인 노드를 제공하며, 하이퍼레저 패브릭 프레임워크를 사용하여 프라이빗 블록체인 네트워크를 생성할 수도 있습니다. 퍼블릭 블록체인 노드에 대한 완전 관리형, 싱글 테넌트 (전용), 서버리스 멀티테넌트 API 운영 등 다양한 방법 중에서 선택하여 퍼블릭 블록체인을 사용할 수 있습니다. 액세스 제어가 중요한 사용 사례의 경우 완전 관리형 사설 블록체인 네트워크 중에서 선택할 수 있습니다. 표준화된 API 운영을 통해 복원력이 뛰어난 완전 관리형 인프라에서 즉각적인 확장성을 제공하므로 블록체인 애플리케이션을 구축할 수 있습니다.

AMB Access는 멀티테넌트 블록체인 네트워크 액세스 API 운영과 전용 블록체인 노드 및 네트워크라는 두 가지 유형의 블록체인 인프라 서비스를 제공합니다. 전용 블록체인 인프라를 통해 퍼블릭 이더리움 블록체인 노드와 프라이빗 Hyperledger Fabric 블록체인 네트워크를 직접 만들어 사용할 수 있습니다. 그러나 AMB Access Bitcoin과 같은 멀티테넌트, API 기반 오퍼링은 기본 블록체인 노드 인프라가 고객 간에 공유되는 API 계층 뒤에 있는 일련의 비트코인 노드로 구성됩니다.

비트코인은 네트워크의 고유 암호화폐인 비트코인 (BTC) 으로 표시된 가치의 안전한 peer-to-peer 거래를 가능하게 하는 분산형 블록체인 네트워크입니다. 비트코인 네트워크는 개인, 금융 기관, 핀테크 기업, 정부 등에서 사용됩니다. 비트코인 네트워크는 교환 매체, 투자 상품 또는 공개적으로 검증 가능하고 변경 불가능한 등록 데이터 원장입니다. Amazon Managed Blockchain (AMB) Access Bitcoin을 사용하면 지역 엔드포인트를 통해 비트코인 메인넷 및 테스트넷 네트워크 풀에 액세스할 수 있으며, 이를 통해 거래를 작성하고, 원장에서 데이터를 읽고, 비트코인 코어 노드 클라이언트에서 사용 가능한 JSON-RPC 요청을 호출할 수 있습니다. 서버리스 비트코인 엔드포인트를 사용하면 비트코인 노드 프로비저닝, 유지 관리, 로드 밸런싱과 같은 차별화되지 않은 작업에 투자하는 대신 애플리케이션 구축에 집중할 수 있습니다. 비트코인 지갑을 구축하든, 암호화폐 거래소를 구축하든, 비트코인 블록체인 데이터를 분석하든 AMB Access Bitcoin을 사용하면 비트코인 엔드포인트를 통해 요청한 만큼만 비용을 지불하면 됩니다.

AMB 액세스 비트코인을 처음 사용하시나요?

AMB Access 비트코인을 처음 사용하는 경우 다음 섹션을 먼저 읽어 보는 것이 좋습니다.

- 주요 개념: 아마존 매니지드 블록체인 (AMB) 액세스 비트코인
- 아마존 매니지드 블록체인 (AMB) 액세스 비트코인 시작하기
- 아마존 관리형 블록체인 (AMB) 액세스 비트코인을 활용한 비트코인 사용 사례

- 아마존 관리형 블록체인 (AMB) 액세스 비트코인을 지원하는 비트코인 JSON-RPC

주요 개념: 아마존 매니지드 블록체인 (AMB) 액세스 비트코인

> **Note**
>
> 이 가이드에서는 여러분이 비트코인의 필수 개념을 잘 알고 있다고 가정합니다. 이러한 개념에는 탈중앙화, 노드, 트랜잭션, 지갑 proof-of-work, 공개 및 개인 키, 반감기 등이 포함됩니다. Amazon Managed Blockchain (AMB) 액세스 비트코인을 사용하기 전에 비트코인 개발 설명서 및 비트코인 마스터링을 검토하는 것이 좋습니다.

Amazon Managed Blockchain (AMB) Access 비트코인은 노드를 포함한 비트코인 인프라를 프로비저닝하고 관리할 필요 없이 비트코인 블록체인에 대한 서버리스 액세스를 제공합니다. 이 관리형 서비스를 사용하면 비트코인 네트워크에 온디맨드로 빠르게 액세스할 수 있어 전체 소유 비용을 줄일 수 있습니다.

AMB Access 비트코인은 지갑 기능을 비활성화하고 여러 JSON 원격 프로시저 (JSON-RPC) 호출을 지원하는 비트코인 코어 클라이언트를 실행하는 풀 노드를 통해 비트코인 네트워크에 액세스할 수 있도록 합니다. 비트코인 JSON RPC를 호출하여 관리형 블록체인이 관리하는 비트코인 노드와 통신하여 비트코인 네트워크와 상호작용할 수 있습니다. 비트코인 JSON-RPC를 사용하면 Amazon Managed Blockchain 서비스를 사용하여 데이터를 읽고 트랜잭션을 작성할 수 있습니다. 여기에는 데이터를 쿼리하고 비트코인 네트워크에 트랜잭션을 제출하는 것도 포함됩니다.

> **Important**
>
> 비트코인 주소를 생성, 유지, 사용 및 관리하는 것은 귀하의 책임입니다. 또한 비트코인 주소의 내용에 대한 책임도 귀하에게 있습니다. AWS Amazon Managed Blockchain에서 비트코인 노드를 사용하여 배포되거나 호출된 트랜잭션에 대해서는 책임을 지지 않습니다.

아마존 관리형 블록체인 (AMB) 액세스 비트코인 사용에 대한 고려 사항 및 제한

- 지원되는 비트코인 네트워크

  AMB Access 비트코인은 다음과 같은 공용 네트워크를 지원합니다.

- 메인넷 — proof-of-work 합의에 의해 보호되고 비트코인 (BTC) 암호화폐가 발행되고 거래되는 퍼블릭 비트코인 블록체인입니다. 메인넷에서의 거래는 실제 가치를 가지며 (즉, 실제 비용이 발생함) 퍼블릭 블록체인에 기록됩니다.
- 테스트넷 — 테스트넷은 테스트에 사용되는 대체 비트코인 블록체인입니다. 테스트넷 코인은 실제 비트코인 (BTC) 과는 별개이며 구별되며 일반적으로 가치가 없습니다.

> **Note**
>
> 사설 네트워크는 지원되지 않습니다.

- 지원되는 리전

  이 서비스가 지원되는 지역은 다음과 같습니다.

지역명	코드	리전
미국 동부(버지니아 북부)	IAD	`us-east-1`
아시아 태평양(도쿄)	NRT	ap-northeast-1
아시아 태평양(서울)	아이콘	ap-northeast-2
아시아 태평양(싱가포르)	SIN	ap-southeast-1
유럽(아일랜드)	DUB	eu-west-1
유럽(런던)	LHR	eu-west-2

- Service endpoints

  AMB 액세스 비트코인의 서비스 엔드포인트는 다음과 같습니다. 서비스에 연결하려면 지원되는 지역 중 하나를 포함하는 엔드포인트를 사용해야 합니다.

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

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

- 마이닝은 지원되지 않습니다.

  AMB 액세스 비트코인은 비트코인 (BTC) 채굴을 지원하지 않습니다.

- 비트코인 JSON-RPC 호출의 시그니처 버전 4 서명

  Amazon Managed Blockchain에서 비트코인 JSON-RPC를 호출할 때는 서명 버전 4 서명 프로세스를 사용하여 인증된 HTTPS 연결을 통해 호출할 수 있습니다. 즉, 계정 내 승인된 IAM 주체만 비트코인 JSON-RPC 호출을 할 수 있습니다. AWS 이를 위해서는 호출과 함께 AWS 자격 증명 (액세스 키 ID 및 비밀 액세스 키) 을 제공해야 합니다.

  > **Important**
  > - 사용자 대상 애플리케이션에는 클라이언트 자격 증명을 내장하지 마십시오.
  > - IAM 정책을 사용하여 개별 비트코인 JSON-RPC에 대한 액세스를 제한할 수는 없습니다.

- 원시 트랜잭션의 제출만 지원됩니다.

  `sendrawtransaction`JSON-RPC를 사용하여 비트코인 블록체인 상태를 업데이트하는 트랜잭션을 제출하십시오.

- AWS CloudTrail 로깅 지원

  비트코인 JSON-RPC를 CloudTrail 기록하도록 구성할 수 있습니다. 자세한 내용은 를 사용하여 Amazon Managed Blockchain (AMB) 액세스 비트코인 이벤트 로깅 AWS CloudTrail 단원을 참조하세요.

아마존 매니지드 블록체인 (AMB) 액세스 비트코인 설정

Amazon Managed Blockchain (AMB) 액세스 비트코인을 처음 사용하기 전에 이 섹션의 단계에 따라 AWS 계정을 생성하십시오. 다음 장에서는 AMB Access 비트코인 사용을 시작하는 방법을 설명합니다.

필수 조건 및 고려 사항

AWS 처음 사용하기 전에 반드시 가지고 있어야 합니다. AWS 계정

가입하기 AWS

AWS가입하면 Amazon Managed Blockchain (AMB) 액세스 비트코인을 AWS 서비스포함한 모든 항목에 자동으로 AWS 계정 가입됩니다. 사용한 서비스에 대해서만 청구됩니다.

AWS 계정 이미 가지고 있다면 다음 단계로 넘어가세요. AWS 계정이 없는 경우에는 다음 절차에 따라 계정을 만드세요.

AWS 계정을 만들려면

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

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 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 권한을 가진 AWS Identity and Access Management (IAM) 주체 (사용자 또는 그룹) 가 있어야 합니다.

IAM 주체만이 비트코인 JSON-RPC 호출을 할 수 있습니다. Amazon Managed Blockchain에서 비트코인 JSON-RPC를 호출할 때는 서명 버전 4 서명 프로세스를 사용하여 인증된 HTTPS 연결을 통해 호출

할 수 있습니다. 즉, 계정 내 승인된 IAM 주체만 비트코인 JSON-RPC 호출을 할 수 있습니다. AWS 이를 위해서는 호출과 함께 AWS 자격 증명 (액세스 키 ID 및 비밀 액세스 키) 을 제공해야 합니다.

IAM 사용자를 생성하는 방법에 대한 자세한 내용은 계정에 IAM 사용자 생성을 참조하십시오. AWS 권한 정책을 사용자에게 연결하는 방법에 대한 자세한 내용은 IAM 사용자의 권한 변경을 참조하십시오. AMB Access Bitcoin을 사용할 수 있는 권한을 사용자에게 부여하는 데 사용할 수 있는 권한 정책의 예는 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

AWS Command Line Interface설치 및 구성

아직 설치하지 않았다면 최신 AWS 명령줄 인터페이스 (CLI) 를 설치하여 터미널의 AWS 리소스로 작업하십시오. 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 인증을 사용합니다. 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 리소스와 함께 임시 자격 증명 사용을 참조하십시오.

아마존 매니지드 블록체인 (AMB) 액세스 비트코인 시작하기

이 섹션의 step-by-step 자습서를 통해 Amazon Managed Blockchain (AMB) Access Bitcoin을 사용하여 작업을 수행하는 방법을 알아보십시오. 이러한 예제를 사용하려면 몇 가지 사전 요구 사항을 완료해야 합니다. AMB Access Bitcoin을 처음 사용하는 경우 이 가이드의 설정 섹션을 검토하여 해당 사전 요구 사항을 완료했는지 확인하십시오. 자세한 정보는 아마존 매니지드 블록체인 (AMB) 액세스 비트코인 설정을 참조하세요.

주제

- 비트코인 JSON-RPC에 액세스하기 위한 IAM 정책을 생성하십시오.
- AMB Access RPC 편집기에서 다음을 사용하여 비트코인 원격 프로시저 호출 (RPC) 요청을 생성합니다. AWS Management Console
- 다음을 사용하여 awscurl에서 AMB 액세스 비트코인 JSON-RPC 요청을 생성하십시오. AWS CLI
- Node.js 에서 비트코인 JSON-RPC 요청을 하세요.
- AMB 액세스 비트코인 오버 사용 AWS PrivateLink

비트코인 JSON-RPC에 액세스하기 위한 IAM 정책을 생성하십시오.

JSON-RPC 호출을 위해 비트코인 메인넷 및 테스트넷의 퍼블릭 엔드포인트에 액세스하려면 아마존 관리형 블록체인 (AMB) 액세스 비트코인에 대한 적절한 IAM 권한을 가진 사용자 자격 증명 (AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY) 이 있어야 합니다. 설치된 터미널에서 다음 명령을 실행하여 두 비트코인 엔드포인트에 모두 액세스할 수 있는 IAM 정책을 생성합니다. AWS CLI

```
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 예시에서는 비트코인 메인넷과 테스트넷 모두에 액세스할 수 있습니다. 특정 엔드포인트에 액세스하려면 다음 `Action` 명령을 사용하십시오.
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

정책을 생성한 후 해당 정책을 IAM 사용자의 역할에 연결하여 적용하십시오. 에서 AWS Management Console IAM 서비스로 `AmazonManagedBlockchainBitcoinAccess` 이동하여 정책을 IAM 사용자에게 할당된 역할에 연결합니다. 자세한 내용은 역할 생성 및 IAM 사용자에게 할당을 참조하십시오.

AMB Access RPC 편집기에서 다음을 사용하여 비트코인 원격 프로시저 호출 (RPC) 요청을 생성합니다. AWS Management Console

AMB Access를 사용하여 원격 프로시저 호출 (RPC) 을 편집하고 제출할 수 있습니다. AWS Management Console 이러한 RPC를 사용하여 비트코인 네트워크에서 데이터를 읽고, 쓰고, 트랜잭션을 제출할 수 있습니다.

Example

다음 예제는 RPC를 사용하여 *blockhash*00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09에 대한 정보를 얻는 방법을 보여줍니다. `getBlock` 강조 표시된 변수를 자체 입력으로 바꾸거나 나열된 다른 RPC 방법 중 하나를 선택하고 필요한 관련 입력을 입력합니다.

1. https://console.aws.amazon.com/managedblockchain/ 에서 매니지드 블록체인 콘솔을 엽니다.
2. RPC 에디터를 선택합니다.
3. 요청 섹션에서 블록체인 ***BITCOIN_MAINNET*** 네트워크로 선택합니다.
4. RPC ***getblock*** 방법으로 선택하세요.

5. 블록 번호로 입력하고 ***00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09*** 상세 ***0*** 정보로 선택합니다.
6. 그런 다음 [RPC 제출] 을 선택합니다.
7. 이 페이지의 응답 섹션에서 결과를 확인할 수 있습니다. 그런 다음 전체 원시 트랜잭션을 복사하여 추가 분석을 위해 또는 애플리케이션의 비즈니스 로직에 사용할 수 있습니다.

자세한 내용은 AMB Access 비트코인이 지원하는 RPC를 참조하십시오.

다음을 사용하여 awscurl에서 AMB 액세스 비트코인 JSON-RPC 요청을 생성하십시오. AWS CLI

Example

AMB 액세스 비트코인 엔드포인트로 비트코인 JSON-RPC를 호출하려면 서명 버전 4 (SigV4) 를 사용하여 IAM 사용자 자격 증명으로 요청에 서명하십시오. awscurl 명령줄 도구를 사용하면 SigV4를 사용하여 서비스에 대한 요청에 서명할 수 있습니다. AWS 자세한 내용은 awscurl README.md를 참조하십시오.

운영 체제에 적합한 방법을 사용하여 awscurl을 설치합니다. macOS에서는 HomeBrew 다음과 같은 응용 프로그램을 사용하는 것이 좋습니다.

```
brew install awscurl
```

AWS CLI를 이미 설치하고 구성한 경우 IAM 사용자 자격 증명과 기본 AWS 리전이 환경에 설정되며 awscurl에 액세스할 수 있습니다. awscurl을 사용하여 RPC를 호출하여 비트코인 메인넷과 테스트넷 모두에 요청을 제출하십시오. `getblock` 이 호출은 정보를 검색하려는 블록 해시에 해당하는 문자열 파라미터를 수락합니다.

다음 명령은 `params` 배열의 블록 해시를 사용하여 헤더를 검색할 특정 블록을 선택하여 비트코인 메인넷에서 블록 헤더 데이터를 검색합니다. 이 예시에서는 엔드포인트를 사용합니다. `us-east-1` 이를 선호하는 비트코인 JSON-RPC 및 아마존 관리형 블록체인 (AMB) 액세스 비트코인이 지원하는 AWS 지역으로 대체할 수 있습니다. 또한 명령에서 로 대체하여 메인넷 대신 테스트넷 네트워크를 대상으로 요청할 수 있습니다. `mainnet` `testnet`

```
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.js 에서 비트코인 JSON-RPC 요청을 하세요.

HTTPS를 사용하여 서명된 요청을 제출하여 비트코인 메인넷 및 테스트넷 엔드포인트에 액세스하고 Node.js 네이티브 https 모듈을 사용하여 JSON-RPC API 호출을 수행하거나 AXIOS와 같은 타사 라이브러리를 사용할 수 있습니다. 다음 예시는 AMB Access 비트코인 엔드포인트에 비트코인 JSON-RPC를 요청하는 방법을 보여줍니다.

Example

이 예제 Node.js 스크립트를 실행하려면 다음 사전 요구 사항을 적용하십시오.

1. 시스템에 노드 버전 관리자 (nvm) 와 Node.js 가 설치되어 있어야 합니다. 여기에서 해당 OS의 설치 지침을 찾을 수 있습니다.
2. `node --version`명령을 사용하여 Node 버전 14 이상을 사용하고 있는지 확인합니다. 필요한 경우 `nvm install 14` 명령과 명령을 차례로 사용하여 버전 14를 설치할 수 있습니다. `nvm use 14`
3. 환경 변수에는 `AWS_ACCESS_KEY_ID` 계정과 관련된 자격 증명이 `AWS_SECRET_ACCESS_KEY` 포함되어야 합니다. 환경 변수에는 AMB Access 비트코인 엔드포인트가 `AMB_HTTP_ENDPOINT` 포함되어야 합니다.

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

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

모든 사전 요구 사항을 완료한 후 편집기를 사용하여 다음 package.json 파일과 index.js 스크립트를 로컬 환경에 복사하십시오.

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 비트코인 엔드포인트에 RPC 요청을 보내고 공식 SDK v3 도구를 사용하여 적절한 서명 버전 4 (SigV4) 헤더를 사용하여 해당 요청에 서명합니다. AWS 코드를 실행하려면 파일과 동일한 디렉터리에서 터미널을 열고 다음을 실행하십시오.

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

생성되는 결과는 다음과 같습니다.

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
    confirmations":784126,"height":1000, "version":1,"versionHex":"00000001",
    "merkleroot":"fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33",
    "time":1232346882,
    "mediantime":1232344831,"nonce":2595206198,"bits":"1d00ffff","difficulty":1,
    "chainwork":"0000000000000000000000000000000000000000000000000003e903e903e9",
    "nTx":1,

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

> **Note**
>
> 이전 스크립트의 샘플 요청은 예제와 동일한 입력 매개 변수 블록 해시를 사용하여 `getblock` 호출합니다다음을 사용하여 awscurl에서 AMB 액세스 비트코인 JSON-RPC 요청을 생성하십시오. AWS CLI. 다른 호출을 하려면 스크립트의 `rpc` 객체를 다른 비트코인 JSON-RPC

로 수정하십시오. 호스트 속성 옵션을 비트코인으로 변경하여 해당 엔드포인트에서 호출을 `testnet` 할 수 있습니다.

AMB 액세스 비트코인 오버 사용 AWS PrivateLink

AWS PrivateLink VPC를 마치 VPC에 있는 것처럼 비공개로 서비스에 연결하는 데 사용할 수 있는 가용성과 확장성이 뛰어난 기술입니다. 사설 서브넷에서 서비스와 통신하기 위해 인터넷 게이트웨이, NAT 장치, 공용 IP 주소, AWS Direct Connect 연결 또는 AWS Site-to-Site VPN 연결을 사용할 필요가 없습니다. AWS PrivateLink AWS PrivateLink설정이나 설정에 대한 자세한 내용은 What is? 를 참조하십시오. AWS PrivateLink

VPC 엔드포인트를 AWS PrivateLink 사용하여 AMB 액세스 비트코인을 통해 비트코인 JSON-RPC 요청을 보낼 수 있습니다. 이 프라이빗 엔드포인트에 대한 요청은 개방형 인터넷을 통해 전달되지 않으므로 동일한 SiGV4 인증을 사용하여 비트코인 엔드포인트에 직접 요청을 보낼 수 있습니다. 자세한 내용은 액세스 AWS 서비스를 참조하십시오. AWS PrivateLink

서비스 이름을 보려면AWS 서비스 열에서 Amazon Managed Blockchain을 검색하십시오. 자세한 내용은 통합되는AWS 서비스를 참조하십시오 AWS PrivateLink. 엔드포인트의 서비스 이름은 다음 `com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`* 형식입니다.

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

아마존 관리형 블록체인 (AMB) 액세스 비트코인을 활용한 비트코인 사용 사례

이 주제에서는 AMB Access 비트코인 사용 사례 목록을 제공합니다.

주제

BTC를 보내고 받을 수 있는 비트코인 (BTC) 지갑을 구축하세요

비트코인 네트워크의 고유 암호화폐인 BTC는 네트워크 보안 모델의 필수 구성 요소 역할을 합니다. 또한 기관, 기업 및 개인이 널리 사용하는 상품 및 교환 매체 역할도 합니다. 따라서 많은 지갑 애플리케이션은 비트코인 노드를 사용하여 비트코인 블록체인과 상호작용합니다. 이러한 애플리케이션은 주어진 주소 집합에 대한 미사용 출력 잔고 (UTXO) 를 계산하고, 거래를 서명하여 비트코인 네트워크로 전송하고, 과거 거래에 대한 데이터를 검색합니다.

다음은 아마존 관리형 블록체인 (AMB) 액세스 비트코인이 BTC 지갑 거래를 위해 지원하는 비트코인 JSON-RPC 중 일부의 샘플입니다.

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

자세한 정보는 지원되는 JSON-RPC을 참조하세요.

비트코인 블록체인에서의 활동 분석

`getchaintxstats`JSON-RPC 방법을 사용하여 비트코인 블록체인의 거래 활동량을 분석할 수 있습니다. 이 JSON-RPC를 사용하면 초당 평균 거래율, 총 거래 수, 블록 수 등과 같은 지표에 액세스할 수

있습니다. 필요한 경우 블록 번호 창이나 블록 해시를 구분 기호로 정의하여 네트워크의 특정 블록 세트에 대한 통계를 계산할 수도 있습니다.

자세한 정보는 지원되는 JSON-RPC을 참조하세요.

비트코인 키 페어를 사용하여 서명된 메시지 확인

비트코인 지갑에는 키 쌍을 구성하는 개인 키와 공개 키가 있습니다. 이러한 키는 거래에 서명하는 데 사용되며 블록체인에서 사용자의 신원 역할을 합니다. 공개 키는 표준화된 영숫자 식별자 (27~34자 길이) 인 주소를 생성하는 데 사용됩니다. 이 주소는 BTC 출력을 수신하고 트랜잭션 또는 메시지를 처리하는 데 사용됩니다.

또한 사용자는 비트코인 지갑을 사용하여 메시지에 암호로 서명하고 확인할 수 있습니다. 이 프로세스는 종종 특정 지갑 주소 및 이와 관련된 BTC의 소유권을 증명하는 데 사용됩니다. `verifymessage`비트코인 JSON-RPC를 사용하면 다른 지갑에서 서명한 메시지의 진위 여부와 유효성을 확인할 수 있습니다. 특히 비트코인 노드를 사용하여 서명된 메시지 내에서 제공된 공개 키 파생 주소에 해당하는 개인 키를 사용하여 메시지가 서명되었는지 확인할 수 있습니다.

자세한 정보는 지원되는 JSON-RPC을 참조하세요.

비트코인 멤풀을 살펴보세요.

많은 애플리케이션은 보류 중인 트랜잭션을 추적하거나, 모든 보류 중인 트랜잭션의 목록을 가져오거나, 트랜잭션의 출처를 찾기 위해 멤풀에 액세스해야 합니다. 이를 위해, 와 같은 비트코인 JSON-RPC가 있으며 `getrawmempool` 이러한 `getmempoolancestors` 활동을 `getmempoolentry` 지원합니다. 이러한 비트코인 JSON-RPC는 애플리케이션이 멤풀에서 필요한 정보를 얻을 수 있도록 도와줍니다.

Amazon Managed Blockchain (AMB) 액세스 비트코인은 `testmempoolaccept` 비트코인 JSON-RPC도 지원합니다. 이를 통해 트랜잭션이 프로토콜 규칙을 준수하고 제출하기 전에 노드가 이를 수락하는지 확인할 수 있습니다. 지갑, 거래소 및 비트코인 블록체인에 직접 거래를 제출하는 기타 주체는 이러한 비트코인 JSON-RPC를 활용합니다.

자세한 내용은 지원되는 JSON-RPC을(를) 참조하세요.

아마존 관리형 블록체인 (AMB) 액세스 비트코인을 지원하는 비트코인 JSON-RPC

이 주제에서는 관리형 블록체인이 지원하는 비트코인 JSON-RPC의 목록과 이에 대한 참조를 제공합니다. 지원되는 각 JSON-RPC에는 용도에 대한 간략한 설명이 있습니다.

> **Note**
>
> - 서명 버전 4 (SigV4) 서명 프로세스를 사용하여 관리형 블록체인에서 비트코인 JSON-RPC를 인증할 수 있습니다. 즉, 계정 내 승인된 IAM 주체만 비트코인 JSON-RPC를 사용하여 해당 AWS 계정과 상호작용할 수 있습니다. 호출 시 AWS 자격 증명 (액세스 키 ID 및 비밀 액세스 키) 을 제공하십시오.
> - HTTP 응답이 10MB보다 크면 오류가 발생합니다. 이 문제를 해결하려면 압축 헤더를 로 설정해야 합니다. `Accept-Encoding:gzip` 그러면 클라이언트가 받는 압축된 응답에는 다음 헤더가 포함됩니다. 및. `Content-Type: application/json` `Content-Encoding: gzip`
> - 아마존 관리형 블록체인 (AMB) 액세스 비트코인은 잘못된 형식의 JSON-RPC 요청에 대해 400 오류를 생성합니다.
> - `sendrawtransaction`JSON-RPC를 사용하여 비트코인 블록체인 상태를 업데이트하는 트랜잭션을 제출하십시오.
> - AMB Access 비트코인의 기본 요청 한도는 지역별 초당 100개 요청 (RPS) 입니다. `NETWORK_TYPE` AWS
>
> 할당량을 늘리려면 지원팀에AWS 문의해야 합니다. AWS 지원팀에 문의하려면 AWS 지원 센터 콘솔에 로그인하십시오. 사례 생성을 선택합니다. [기술] 을 선택합니다. 관리형 블록체인을 서비스로 선택하세요. 카테고리로 Access:Bitcoin을 선택하고 심각도로는 일반 지침을 선택하십시오. 제목 및 설명 입력란에 RPC 할당량을 입력하고 지역별 비트코인 네트워크당 RPS로 요구 사항에 적용할 수 있는 할당량 한도를 나열하십시오. 사례를 제출하세요.

지원되는 JSON-RPC

AMB 액세스 비트코인은 다음과 같은 비트코인 JSON-RPC를 지원합니다. 지원되는 각 호출에는 사용에 대한 간략한 설명이 있습니다.

범주	JSON-RPC	설명
블록체인 RPC	최고의 블록 해시를 얻으세요	가장 많이 작동하고 완전히 검증된 체인에서 가장 좋은 (팁) 블록의 해시를 반환합니다.
	getblock	verbosity가 0인 경우 블록 'hash'에 대해 직렬화된 16진수 인코딩 데이터인 문자열을 반환합니다. verbosity가 1인 경우, 블록 'hash'에 대한 정보가 포함된 Object를 반환합니다. verbosity가 2인 경우 블록 '해시'에 대한 정보와 각 트랜잭션에 대한 정보가 포함된 Object를 반환합니다. verbosity가 3인 경우 블록 '해시'에 대한 정보와 각 트랜잭션에 대한 정보 (입력 정보 포함) 가 포함된 Object를 반환합니다. `prevout`
	get/블록체인/정보	블록체인 처리와 관련된 다양한 상태 정보가 들어 있는 객체를 반환합니다.
	get/블록/카운트	가장 많이 작동하고 완전히 검증된 체인의 높이를 반환합니다. 제네시스 블록의 높이는 0입니다.
	겟블록 필터	블록 해시를 사용하여 특정 블록의 BIP 157 콘텐츠 필터를 검색합니다.
	get/블록/해시	블록의 best-block-chain 해시를 제공된 높이로 반환합니다.
	get/블록 헤더	verbose가 false인 경우 블록 헤더 'hash'에 대해 직렬화된 16진수 인코딩 데이터인 문자열을 반환합니다. verbose가 true인 경우 블록 헤더 '해시'에 대한 정보가 포함된 Object를 반환합니다.
	getblockstats	주어진 윈도우의 블록당 통계를 계산합니다. 모든 금액은 사토시 단위입니다. 일부 높이에서는 가지치기를 하면 효과가 없을 거예요.

범주	JSON-RPC	설명
	체인 팁을 구하세요	메인 체인과 분리된 브랜치를 포함하여 블록 트리에 있는 알려진 모든 팁에 대한 정보를 반환합니다.
	getchaintxstats	체인의 총 트랜잭션 수와 비율에 대한 통계를 계산합니다.
	난이도 증가	난이도를 최소 proof-of-work 난이도의 배수로 반환합니다.
	Getmempool 조상	txid가 멤풀에 있는 경우 모든 멤풀 내 조상을 반환합니다.
	멤풀 자손을 가져오세요.	txid가 멤풀에 있는 경우 모든 멤풀 내 하위 항목을 반환합니다.
	메모리 풀 엔트리 가져오기	주어진 트랜잭션의 멤풀 데이터를 반환합니다.
	getmempool info	TX 메모리 풀의 활성 상태에 대한 세부 정보를 반환합니다.
	getrawmempool	메모리 풀의 모든 트랜잭션 ID를 문자열 트랜잭션 ID로 구성된 JSON 배열로 반환합니다. **Note** `verbose = true`는 지원되지 않습니다.
	gettxout	사용하지 않은 트랜잭션 출력에 대한 세부 정보를 반환합니다.
	gettxoutproof	블록에 “txid”가 포함되었다는 16진수로 인코딩된 증명을 반환합니다.
원시 트랜잭션 RPC	원시 트랜잭션 생성	주어진 입력값을 사용하고 새 출력을 생성하는 트랜잭션을 생성합니다.

범주	JSON-RPC	설명
	디코더 원시 트랜잭션	직렬화된 16진수로 인코딩된 트랜잭션을 나타내는 JSON 객체를 반환합니다.
	디코스크립트	16진수로 인코딩된 스크립트를 디코딩합니다.
	원시 트랜잭션 가져오기	원시 트랜잭션 데이터를 반환합니다.
	미가공 트랜잭션 전송	원시 트랜잭션 (직렬화, 16진수 인코딩) 을 로컬 노드와 네트워크에 제출합니다.
	테스트, 메모, 수락	mempool에서 원시 트랜잭션 (직렬화, 16진수 인코딩) 을 수락할지 여부를 나타내는 mempool 승인 테스트 결과를 반환합니다. 이는 트랜잭션이 합의 또는 정책 규칙을 위반하는지 확인합니다.
RPC를 활용하십시오.	멀티서명 생성	내 키의 서명이 필요 없는 다중 서명 주소를 생성합니다.
	스마트 요금 추정	가능한 경우 conf_target 블록 내에서 트랜잭션이 확인을 시작하는 데 필요한 킬로바이트당 대략적인 수수료를 추정하고 추정치가 유효한 블록 수를 반환합니다. BIP 141에 정의된 가상 트랜잭션 크기를 사용합니다 (감시 데이터는 할인).
	주소 확인	주어진 비트코인 주소에 대한 정보를 반환합니다.
	인증/메시지	서명된 메시지를 확인합니다.

아마존 매니지드 블록체인 (AMB) 액세스 비트코인의 보안

클라우드 AWS 보안은 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 귀사 간의 공동 책임입니다. AWS 공동 책임 모델은 이를 클라우드의 보안과 클라우드에서의 보안 모두로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 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 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오.
- 클라우드에서의 보안 — 귀하의 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 관리형 블록체인에서 실행되는 오픈 소스 프레임워크의 특징과 AWS 특징을 사용합니다.

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

주제

아마존 매니지드 블록체인 (AMB) 액세스 비트코인의 데이터 보호

AWS 공동 책임 모델 공동 모델은 아마존 관리형 블록체인 (AMB) Access 비트코인의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로, AWS 는 모든 것을 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 클라우드이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 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 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API 또는 SDK를 AWS 서비스 사용하여 AMB Access 비트코인 또는 기타 장치로 작업하는 경우가 포함됩니다. AWS CLI AWS 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 보안 인증를 URL에 포함시켜서는 안 됩니다.

데이터 암호화

데이터 암호화는 승인되지 않은 사용자가 블록체인 네트워크 및 관련 데이터 스토리지 시스템에서 데이터를 읽는 것을 방지하는 데 도움이 됩니다. 여기에는 네트워크를 이동할 때 가로챌 수 있는 데이터(전송 중인 데이터) 가 포함됩니다.

전송 중 암호화

기본적으로 Managed Blockchain은 HTTPS/TLS 연결을 사용하여 서비스 엔드포인트를 실행하는 클라이언트 컴퓨터에서 전송되는 모든 데이터를 암호화합니다. AWS CLI AWS

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

아마존 매니지드 블록체인 (AMB) 액세스 비트코인을 위한 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. AWS IAM 관리자는 AMB Access 비트코인 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 관리합니다. IAM은 추가 비용 AWS 서비스 없이 사용할 수 있습니다.

주제

고객

AMB Access 비트코인에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 — AMB Access Bitcoin 서비스를 사용하여 업무를 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. AMB Access Bitcoin 기능을 더 많이 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AMB Access 비트코인의 기능에 액세스할 수 없는 경우 을 참조하십시오. 아마존 관리형 블록체인 (AMB) 액세스 비트코인 ID 및 액세스 문제 해결

서비스 관리자 — 회사에서 AMB Access 비트코인 리소스를 담당하고 있다면 AMB Access 비트코인에 완전히 액세스할 수 있을 것입니다. 서비스 사용자가 액세스해야 하는 AMB Access 비트코인 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사에서 AMB Access Bitcoin과 함께 IAM을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인이 IAM과 연동되는 방식

IAM 관리자 — IAM 관리자라면 AMB Access Bitcoin에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AMB Access 비트코인 ID 기반 정책

의 예를 보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 연합형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 연합을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 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 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

연동 보안 인증

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

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

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 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 참조하십시오.

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 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증 정보만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다:

- 연합 사용자 액세스 - 연합 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연합 아이덴티티가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 집합을 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 통제하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 상관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 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 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 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 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 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 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인

스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증 정보를 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책의 권한이 요청 허용 또는 거부 여부를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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, 사용자와 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`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

보안 인증 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 보안 인증에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 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 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 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 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 특성을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.

- 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 정책의 교집합과 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 참조하십시오.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

아마존 매니지드 블록체인 (AMB) 액세스 비트코인이 IAM과 연동되는 방식

IAM을 사용하여 AMB 액세스 비트코인에 대한 액세스를 관리하기 전에 AMB 액세스 비트코인과 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

아마존 관리형 블록체인 (AMB) 액세스 비트코인과 함께 사용할 수 있는 IAM 기능

IAM 특성	AMB 액세스 비트코인 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
보안 주체 권한	아니요

IAM 특성	AMB 액세스 비트코인 지원
서비스 역할	아니요
서비스 연결 역할	아니요

AMB Access Bitcoin 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서에서 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

AMB 액세스 비트코인에 대한 ID 기반 정책

ID 기반 정책 지원	예

자격 증명기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 태스크와 리소스 뿐만 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

AMB 액세스 비트코인에 대한 ID 기반 정책 예제

AMB Access 비트코인 ID 기반 정책의 예를 보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

AMB 액세스 비트코인 내의 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 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, 페더레이션 사용자 등이 포함될 수 있습니다. AWS 서비스

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

AMB 액세스 비트코인에 대한 정책 조치

정책 작업 지원	예

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.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

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

AMB Access 비트코인 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Managed Blockchain (AMB) Access Bitcoin에서 정의한 작업을 참조하십시오.

AMB Access 비트코인의 정책 조치는 조치 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(이)라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

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

AMB Access 비트코인 ID 기반 정책의 예를 보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

AMB 액세스 비트코인에 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. 보고서에는 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 이 작업을 수행할 수 있습니다.

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

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

AMB 액세스 비트코인 리소스 유형 및 해당 ARN 목록을 보려면 서비스 인증 참조의 Amazon Managed Blockchain (AMB) 액세스 비트코인에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 Amazon Managed Blockchain (AMB) Access Bitcoin에서 정의한 작업을 참조하십시오.

AMB Access 비트코인 ID 기반 정책의 예를 보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

AMB 액세스 비트코인의 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 적음 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`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명령문의 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 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

AMB 액세스 비트코인 조건 키 목록을 보려면 서비스 인증 참조의 Amazon Managed Blockchain (AMB) 액세스 비트코인의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon Managed Blockchain (AMB) Access Bitcoin에서 정의한 작업을 참조하십시오.

AMB Access 비트코인 ID 기반 정책의 예를 보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

AMB 액세스 비트코인의 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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC (AMB 액세스 포함) 비트코인

ABAC 지원(정책의 태그)	아니요

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 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/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 부분입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

AMB Access 비트코인에 임시 자격 증명 사용

임시 보안 인증 정보 지원	아니요

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증 정보를 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자

격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

AMB Access 비트코인에 대한 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	아니요

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AMB 액세스 비트코인의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하십시오.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 AMB Access 비트코인 기능이 작동하지 않을 수 있습니다. AMB Access 비트코인이 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

AMB 액세스 비트코인의 서비스 연결 역할

서비스 연결 역할 지원	아니요

서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되

며 해당 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 서비스 섹션을 참조하세요. Service-linked role(서비스 연결 역할) 열에서 Yes이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

아마존 매니지드 블록체인 (AMB) 액세스 비트코인에 대한 ID 기반 정책 예제

기본적으로 사용자와 역할은 AMB Access 비트코인 리소스를 생성하거나 수정할 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 ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 ARN 형식을 비롯하여 AMB Access Bitcoin에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조의 Amazon Managed Blockchain (AMB) Access Bitcoin용 작업, 리소스 및 조건 키를 참조하십시오.

주제

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

정책 모범 사례

ID 기반 정책은 누군가가 계정에서 AMB Access 비트코인 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하십시오. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습

니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 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 설명서의 IAM의 정책 및 권한을 참조하세요.
- Use conditions in IAM policies to further restrict access(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 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

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

AMB 액세스 비트코인 콘솔 사용

Amazon Managed Blockchain (AMB) 액세스 비트코인 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AMB Access 비트코인 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. AWS 계정최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 AMB Access 비트코인 콘솔을 계속 사용할 수 있도록 하려면 AMB Access 비트코인 *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

비트코인 네트워크 액세스

> **Note**
>
> 비트코인의 퍼블릭 엔드포인트에 `mainnet` 액세스하고 `testnet` JSON-RPC를 호출하려면 AMB Access 비트코인에 대한 적절한 IAM 권한을 가진 사용자 자격 증명(`AWS_ACCESS_KEY_ID`및`AWS_SECRET_ACCESS_KEY`) 이 필요합니다.

Example 모든 비트코인 네트워크에 접근하기 위한 IAM 정책

이 예시는 IAM 사용자에게 모든 비트코인 네트워크에 AWS 계정 대한 액세스 권한을 부여합니다.

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

Example 비트코인 테스트넷 네트워크 액세스를 위한 IAM 정책

이 예시는 IAM 사용자에게 비트코인 네트워크 AWS 계정 액세스 권한을 부여합니다. `testnet`

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

```
        }
    ]
}
```

아마존 관리형 블록체인 (AMB) 액세스 비트코인 ID 및 액세스 문제 해결

다음 정보를 사용하면 AMB Access 비트코인 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 AMB Access 비트코인으로 작업을 수행할 권한이 없습니다.
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 제 외부 사람들이 제 AMB Access 비트코인 AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

저는 AMB Access 비트코인으로 작업을 수행할 권한이 없습니다.

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

다음 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 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류가 발생하는 경우 AMB Access Bitcoin에 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. `iam:PassRole`

일부 AWS 서비스 서비스에서는 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 이라는 IAM 사용자가 AMB Access Bitcoin에서 콘솔을 사용하여 작업을 `marymajor` 수행하려고 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 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

제 외부 사람들이 제 AMB Access 비트코인 AWS 계정 리소스에 액세스할 수 있도록 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 참조하십시오.

- AMB Access 비트코인이 이러한 기능을 지원하는지 여부를 알아보려면 을 참조하십시오. 아마존 매니지드 블록체인 (AMB) 액세스 비트코인이 IAM과 연동되는 방식
- 소유하고 AWS 계정 있는 리소스에 대한 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 자격 증명 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하십시오.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

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

> **Note**
>
> 아마존 관리형 블록체인 (AMB) 액세스 비트코인은 관리 이벤트를 지원하지 않습니다.

Amazon Managed Blockchain은 관리형 블록체인에서 사용자, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스인 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail 관리형 블록체인의 AMB Access 비트코인 엔드포인트를 데이터 플레인 이벤트로 호출한 사람을 캡처합니다.

원하는 데이터 플레인 이벤트를 수신하도록 구독된 적절하게 구성된 트레일을 생성하면 Amazon S3 버킷으로 AMB Access Bitcoin 관련 CloudTrail 이벤트를 지속적으로 전송할 수 있습니다. 에서 수집한 정보를 사용하여 AMB Access Bitcoin 엔드포인트 중 하나에 요청이 이루어졌는지 CloudTrail, 요청을 보낸 IP 주소, 요청한 사람, 요청 시기 및 기타 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AMB Access 비트코인 정보는 CloudTrail

AWS CloudTrail 를 생성할 때 기본적으로 활성화됩니다. AWS 계정하지만 AMB Access Bitcoin 엔드포인트를 호출한 사람을 확인하려면 데이터 플레인 이벤트를 CloudTrail 기록하도록 구성해야 합니다.

AMB Access Bitcoin의 데이터 플레인 이벤트를 포함하여 귀하의 AWS 계정이벤트를 지속적으로 기록하려면 트레일을 생성해야 합니다. 트레일을 통해 CloudTrail Amazon S3 버킷으로 로그 파일을 전송합니다. 기본적으로 에서 트레일을 생성하면 트레일이 모두에 적용됩니다 AWS 리전. AWS Management Console트레일은 AWS 파티션에 있는 모든 지원 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 이 데이터를 더 자세히 분석하고 CloudTrail 로그에 수집된 이벤트 데이터에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 비트코인 JSON-RPC를 CloudTrail 추적하는 데 사용
- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail

- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

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

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

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

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

AMB Access 비트코인 로그 파일 항목의 이해

데이터 플레인 이벤트의 경우 트레일은 이벤트를 지정된 S3 버킷에 로그 파일로 전달할 수 있는 구성입니다. 각 CloudTrail 로그 파일에는 모든 소스의 단일 요청을 나타내는 하나 이상의 로그 항목이 포함되어 있습니다. 이러한 항목은 작업 날짜 및 시간, 관련 요청 매개 변수를 포함하여 요청된 작업에 대한 세부 정보를 제공합니다.

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

비트코인 JSON-RPC를 CloudTrail 추적하는 데 사용

CloudTrail 이를 사용하여 계정에서 AMB Access 비트코인 엔드포인트를 호출한 사람이 누구인지, 어떤 JSON-RPC가 데이터 이벤트로 호출되었는지 추적할 수 있습니다. 기본적으로 트레일을 생성할 때 데이터 이벤트는 로깅되지 않습니다. AMB Access Bitcoin 엔드포인트를 CloudTrail 데이터 이벤트로 호출한 사람을 기록하려면 활동을 수집하려는 지원되는 리소스 또는 리소스 유형을 트레일에 명시적으로 추가해야 합니다. Amazon Managed Blockchain은 AWS Management Console, AWS SDK 및 AWS CLI를 사용하여 데이터 이벤트를 추가할 수 있도록 지원합니다. 자세한 내용은 사용 AWS CloudTrail 설명서의 고급 선택기를 사용한 이벤트 로깅을 참조하십시오.

트레일에 데이터 이벤트를 로깅하려면 트레일을 만든 후 put-event-selectors작업을 사용하십시오. AMB Access Bitcoin 엔드포인트를 호출한 사람을 확인하기 위해 데이터 이벤트 로깅을 시작하려면 이 `--advanced-event-selectors` 옵션을 사용하여 `AWS::ManagedBlockchain::Network` 리소스 유형을 지정합니다.

Example 모든 계정의 AMB Access 비트코인 엔드포인트 요청의 데이터 이벤트 로그 입력

다음 예시는 `put-event-selectors` 작업을 사용하여 해당 지역의 트레일에 `my-bitcoin-trail` 대한 모든 계정의 AMB Access Bitcoin 엔드포인트 요청을 기록하는 방법을 보여줍니다. `us-east-1`

```
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 후에는 이전 예제에서 지정한 트레일에 연결된 S3 버킷의 사용량을 추적할 수 있습니다.

다음 결과는 에서 수집한 정보의 CloudTrail 데이터 이벤트 로그 항목을 보여줍니다 CloudTrail. AMB Access 비트코인 엔드포인트 중 하나에 비트코인 JSON-RPC 요청이 이루어졌는지, 요청을 보낸 IP 주소, 요청한 사람, 요청 시기 및 기타 추가 세부 정보를 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.