aws

Guia do desenvolvedor

AMB Acesse Bitcoin

AMB Acesse Bitcoin: Guia do desenvolvedor

Table of Contents

O que é o Amazon Managed Blockchain (AMB) Access Bitcoin?

O Amazon Managed Blockchain (AMB) Access fornece nós públicos de blockchain para Ethereum e Bitcoin, e você também pode criar redes privadas de blockchain com a estrutura Hyperledger Fabric. Escolha entre vários métodos para interagir com blockchains públicos, incluindo operações de API totalmente gerenciadas, de inquilino único (dedicado) e multilocatário sem servidor para nós públicos de blockchain. Para casos de uso em que os controles de acesso são importantes, você pode escolher entre redes de blockchain privadas totalmente gerenciadas. As operações de API padronizadas oferecem escalabilidade instantânea em uma infraestrutura resiliente e totalmente gerenciada, para que você possa criar aplicativos de blockchain.

O AMB Access oferece dois tipos distintos de serviços de infraestrutura de blockchain: operações de API de acesso à rede blockchain multilocatário e nós e redes de blockchain dedicados. Com uma infraestrutura de blockchain dedicada, você pode criar e usar nós públicos de blockchain Ethereum e redes privadas de blockchain Hyperledger Fabric para seu próprio uso. No entanto, as ofertas multilocatárias baseadas em API, como o AMB Access Bitcoin, são compostas por uma frota de nós Bitcoin por trás de uma camada de API, na qual a infraestrutura subjacente do nó blockchain é compartilhada entre os clientes.

Bitcoin é uma rede blockchain descentralizada que permite peer-to-peer transações seguras de valor denominadas na criptomoeda nativa da rede, Bitcoin (BTC). A rede Bitcoin é usada por indivíduos, instituições financeiras, empresas de fintech, governos e muito mais. A rede Bitcoin é um meio de troca, uma mercadoria para investimento ou um livro contábil publicamente verificável e imutável para dados inscritos. Com o Amazon Managed Blockchain (AMB) Access Bitcoin, você pode acessar um pool de redes Bitcoin Mainnet e Testnet por meio de endpoints regionais, por meio dos quais você pode gravar transações, ler dados do livro contábil e invocar solicitações JSON-RPC disponíveis no cliente do nó Bitcoin Core. Com endpoints Bitcoin sem servidor, você pode se concentrar na criação de seus aplicativos em vez de investir em trabalho indiferenciado, como provisionamento, manutenção e balanceamento de carga de nós Bitcoin. Se você está criando uma carteira de Bitcoin, criando uma bolsa de criptomoedas ou analisando dados de blockchain de Bitcoin, você paga apenas pelas solicitações feitas por meio dos endpoints de Bitcoin usando o AMB Access Bitcoin.

Você é um usuário de Bitcoin AMB Access pela primeira vez?

Se você é um usuário iniciante do AMB Access Bitcoin, recomendamos que comece lendo as seguintes seções:

- Conceitos principais: Amazon Managed Blockchain (AMB) Acesse Bitcoin
- Introdução ao Amazon Managed Blockchain (AMB) Acesse Bitcoin
- Casos de uso de Bitcoin com Amazon Managed Blockchain (AMB) Acesse Bitcoin
- Bitcoin JSON compatível - RPCs com Amazon Managed Blockchain (AMB) Acesse Bitcoin

Conceitos principais: Amazon Managed Blockchain (AMB) Acesse Bitcoin

> **Note**
>
> Este guia pressupõe que você esteja familiarizado com os conceitos essenciais para o Bitcoin. Esses conceitos incluem descentralização, nós, transações, carteiras proof-of-work, chaves públicas e privadas, metades e outros. Antes de usar o Amazon Managed Blockchain (AMB) Access Bitcoin, recomendamos que você revise a documentação de desenvolvimento do Bitcoin e o Mastering Bitcoin.

O Amazon Managed Blockchain (AMB) Access Bitcoin fornece acesso sem servidor ao blockchain Bitcoin, sem exigir que você provisione e gerencie qualquer infraestrutura Bitcoin, incluindo nós. Você pode usar esse serviço gerenciado para acessar as redes Bitcoin rapidamente e sob demanda, reduzindo seu custo geral de propriedade.

O AMB Access Bitcoin fornece acesso à rede Bitcoin por meio de nós completos executando o cliente Bitcoin Core, com a funcionalidade de carteira desativada e suportando várias chamadas de procedimento remoto JSON (JSON-RPC). Você pode invocar o Bitcoin JSON RPCs para se comunicar com os nós Bitcoin gerenciados pelo Managed Blockchain para interagir com as redes Bitcoin. Com o Bitcoin JSON-RPCs, você pode ler dados e gravar transações, incluindo consultar dados e enviar transações para as redes Bitcoin usando o serviço Amazon Managed Blockchain.

> **Important**
>
> Você é responsável por criar, manter, usar e gerenciar seus endereços Bitcoin. Você também é responsável pelo conteúdo dos seus endereços Bitcoin. AWS não é responsável por nenhuma transação implantada ou chamada usando nós Bitcoin no Amazon Managed Blockchain.

Considerações e limitações para usar o Amazon Managed Blockchain (AMB) Access Bitcoin

- Redes Bitcoin suportadas

O AMB Access Bitcoin suporta as seguintes redes públicas:

- Mainnet — A blockchain pública de Bitcoin garantida por proof-of-work consenso e na qual a criptomoeda Bitcoin (BTC) é emitida e transacionada. As transações na Mainnet têm valor real (ou seja, incorrem em custos reais) e são registradas na blockchain pública.
- Testnet — A testnet é uma blockchain alternativa de Bitcoin usada para testes. As moedas Testnet são separadas e distintas do Bitcoin (BTC) real e geralmente não têm nenhum valor.

> **Note**
>
> Não há suporte para redes privadas.

- Regiões aceitas

  A seguir estão as regiões com suporte para esse serviço:

Nome da região	Código	Região
Leste dos EUA (Norte da Virgínia)	IAD	`us-east-1`
Ásia-Pacífico (Tóquio)	NRT	ap-northeast-1
Ásia-Pacífico (Seul)	ICN	ap-northeast-2
Ásia-Pacífico (Singapura)	SIN	ap-southeast-1
Europa (Irlanda)	DUB	eu-west-1
Europa (Londres)	LHR	eu-west-2

- Service endpoints (Endpoints de serviço)

  A seguir estão os endpoints de serviço do AMB Access Bitcoin. Para se conectar ao serviço, você deve usar um endpoint que inclua uma das regiões suportadas.

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

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

- Mineração não suportada

O AMB Access Bitcoin não suporta a mineração de Bitcoin (BTC).

- Assinatura Versão 4: assinatura de chamadas Bitcoin JSON-RPC

  Ao fazer chamadas para o Bitcoin JSON- RPCs no Amazon Managed Blockchain, você pode fazer isso por meio de uma conexão HTTPS autenticada usando o processo de assinatura Signature Version 4. Isso significa que somente diretores autorizados do IAM na AWS conta podem fazer chamadas Bitcoin JSON-RPC. Para fazer isso, AWS as credenciais (uma ID da chave de acesso e uma chave de acesso secreta) devem ser fornecidas com a chamada.

  > **Important**
  >
  > - Não incorpore credenciais do cliente em aplicativos voltados para o usuário.
  > - Você não pode usar políticas do IAM para restringir o acesso a Bitcoin JSON- RPCs individuais.

- Somente envios de transações brutas são aceitos

  Use o `sendrawtransaction` JSON-RPC para enviar transações que atualizem o estado do blockchain do Bitcoin.

- AWS CloudTrail suporte de registro

  Você pode configurar CloudTrail para registrar seu Bitcoin JSON-. RPCs Para obter mais informações, consulte Registro em log do Amazon Managed Blockchain (AMB) Acesse eventos de Bitcoin usando AWS CloudTrail.

Configurando o Amazon Managed Blockchain (AMB) Acesse Bitcoin

Antes de usar o Amazon Managed Blockchain (AMB) Acesse Bitcoin pela primeira vez, siga as etapas nesta seção para criar uma AWS conta. O capítulo a seguir discute como começar a usar o AMB Access Bitcoin.

Pré-requisitos e considerações

Antes de usar AWS pela primeira vez, você deve ter um Conta da AWS.

Inscreva-se para AWS

Quando você se inscreve AWS, você Conta da AWS é automaticamente inscrito para todos Serviços da AWS, incluindo Amazon Managed Blockchain (AMB) Access Bitcoin. Você será cobrado apenas pelos serviços que usar.

Se você Conta da AWS já tem um, vá para a próxima etapa. Se você não tem uma Conta da AWS, siga o procedimento abaixo para criar uma.

Para criar uma AWS conta

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Crie um usuário do IAM com as permissões apropriadas

Para criar e trabalhar com o AMB Access Bitcoin, você deve ter um diretor AWS Identity and Access Management (IAM) (usuário ou grupo) com permissões que permitam as ações necessárias do Managed Blockchain.

Somente diretores do IAM podem fazer chamadas Bitcoin JSON-RPC. Ao fazer chamadas para o Bitcoin JSON- RPCs no Amazon Managed Blockchain, você pode fazer isso por meio de uma conexão HTTPS autenticada usando o processo de assinatura Signature Version 4. Isso significa que somente diretores autorizados do IAM na AWS conta podem fazer chamadas Bitcoin JSON-RPC. Para fazer isso, AWS as credenciais (uma ID da chave de acesso e uma chave de acesso secreta) devem ser fornecidas com a chamada.

Para obter informações sobre como criar um usuário do IAM, consulte Como criar um usuário do IAM em sua AWS conta. Para obter mais informações sobre como anexar uma política de permissões a um usuário, consulte Alteração de permissões para um usuário do IAM. Para obter um exemplo de uma política de permissões que você pode usar para dar permissão ao usuário para trabalhar com o AMB Access Bitcoin, consulteExemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin.

Instale e configure o AWS Command Line Interface

Se você ainda não tiver feito isso, instale a interface de AWS linha de comando (CLI) mais recente para trabalhar com AWS recursos de um terminal. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.

> **Note**
>
> Para acesso à CLI, é necessário ter um ID de chave de acesso e de uma chave de acesso secreta. Use credenciais temporárias em vez de chaves de acesso de longo prazo quando possível. As credenciais temporárias incluem um ID de acesso, uma chave de acesso secreta e um token de segurança que indica quando as credenciais expiram. Para obter mais informações, consulte Uso de credenciais temporárias com AWS recursos no Guia do usuário do IAM.

Introdução ao Amazon Managed Blockchain (AMB) Acesse Bitcoin

Use os step-by-step tutoriais desta seção para aprender a realizar tarefas usando o Amazon Managed Blockchain (AMB) Access Bitcoin. Esses exemplos exigem que você preencha alguns pré-requisitos. Se você é novo no AMB Access Bitcoin, revise a seção de configuração deste guia para verificar se você cumpriu esses pré-requisitos. Para obter mais informações, consulte Configurando o Amazon Managed Blockchain (AMB) Acesse Bitcoin.

Tópicos

Crie uma política do IAM para acessar Bitcoin JSON- RPCs

Para acessar os endpoints públicos da Bitcoin Mainnet e da Testnet para fazer chamadas JSON-RPC, você deve ter credenciais de usuário (AWS_ACCESS_KEY_ID e AWS_SECRET _ACCESS_KEY) que tenham as permissões apropriadas do IAM para o Amazon Managed Blockchain (AMB) acessar o Bitcoin. Em um terminal com o AWS CLI instalado, execute o seguinte comando para criar uma política do IAM para acessar os dois endpoints Bitcoin:

```
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**
>
> O exemplo anterior fornece acesso ao Bitcoin Mainnet e ao Testnet. Para obter acesso a um endpoint específico, use o seguinte `Action` comando:
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

Depois de criar a política, anexe essa política à função do usuário do IAM para que ela entre em vigor. No Console de gerenciamento da AWS, navegue até o serviço do IAM e anexe a política `AmazonManagedBlockchainBitcoinAccess` à função atribuída ao seu usuário do IAM. Para obter mais informações, consulte Como criar uma função e atribuir a um usuário do IAM.

Faça solicitações de chamada de procedimento remoto (RPC) do Bitcoin no editor RPC do AMB Access usando o Console de gerenciamento da AWS

Você pode editar e enviar chamadas de procedimento remoto (RPCs) Console de gerenciamento da AWS usando o AMB Access. Com eles RPCs, você pode ler dados, gravar e enviar transações na rede Bitcoin.

Example

O exemplo a seguir mostra como obter informações sobre o 00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 usando *`blockhash`* RPC. `getBlock` Substitua as variáveis destacadas por suas próprias entradas ou escolha um dos outros métodos RPC listados e insira as entradas relevantes necessárias.

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. Escolha o editor RPC.
3. Na seção Solicitação, escolha `BITCOIN_MAINNET` como Rede Blockchain.
4. Escolha `getblock` como método RPC.
5. Insira `00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09` como o número do bloco e escolha `0` como a verbosidade.
6. Em seguida, escolha Enviar RPC.
7. Você obterá resultados na seção Resposta desta página. Em seguida, você pode copiar todas as transações brutas para análise posterior ou para usar na lógica de negócios de seus aplicativos.

Para obter mais informações, consulte o RPCs suporte do AMB Access Bitcoin

Faça solicitações AMB Access Bitcoin JSON-RPC em awscurl usando o AWS CLI

Example

Assine solicitações com suas credenciais de usuário do IAM usando o Signature Version 4 (SigV4) para fazer chamadas Bitcoin JSON-RPC para os endpoints Bitcoin do AMB Access. A ferramenta de linha de comando awscurl pode ajudá-lo a assinar solicitações de AWS serviços usando o SigV4. Para obter mais informações, consulte o awscurl README.md.

Instale o awscurl usando o método apropriado ao seu sistema operacional. No macOS, HomeBrew é o aplicativo recomendado:

```
brew install awscurl
```

Se você já instalou e configurou a AWS CLI, suas credenciais de usuário do IAM e a região padrão da AWS estão definidas em seu ambiente e têm acesso ao awscurl. Usando awscurl, envie uma solicitação para a rede principal do Bitcoin e para a Testnet invocando a RPC. `getblock` Essa chamada aceita um parâmetro de string correspondente ao hash do bloco para o qual você deseja recuperar informações.

O comando a seguir recupera os dados do cabeçalho do bloco da rede principal do Bitcoin usando o hash do bloco na `params` matriz para selecionar o bloco específico para o qual recuperar os cabeçalhos. Este exemplo usa o `us-east-1` endpoint. Você pode substituí-lo por seu Bitcoin JSON-RPC e sua AWS região preferidos, que são suportados pelo Amazon Managed Blockchain (AMB) Access Bitcoin. Além disso, você pode fazer uma solicitação na rede Testnet, em vez da Mainnet, `mainnet` substituindo por `testnet` no comando.

```
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
```

Os resultados incluem detalhes dos cabeçalhos dos blocos e uma lista de hashes de transação incluídos no bloco solicitado. Veja o exemplo a seguir:

```
{"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"}
```

Faça solicitações Bitcoin JSON-RPC em Node.js

Você pode enviar solicitações assinadas usando HTTPS para acessar os endpoints Bitcoin Mainnet e Testnet e fazer chamadas de API JSON-RPC usando o módulo https nativo em Node.js, ou você pode usar uma biblioteca de terceiros, como a AXIOS. O exemplo a seguir mostra como fazer uma solicitação Bitcoin JSON-RPC para os endpoints Bitcoin do AMB Access.

Example

Para executar esse exemplo de script Node.js, aplique os seguintes pré-requisitos:

1. Você deve ter o node version manager (nvm) e o Node.js instalados em sua máquina. Você pode encontrar instruções de instalação para seu sistema operacional aqui.
2. Use o `node --version` comando e confirme se você está usando a versão 14 ou superior do Node. Se necessário, você pode usar o `nvm install 14` comando, seguido pelo `nvm use 14` comando, para instalar a versão 14.
3. As variáveis `AWS_ACCESS_KEY_ID` de ambiente `AWS_SECRET_ACCESS_KEY` devem conter as credenciais associadas à sua conta. As variáveis de ambiente `AMB_HTTP_ENDPOINT` devem conter seus endpoints AMB Access Bitcoin.

   Exporte essas variáveis como cadeias de caracteres em seu cliente usando os comandos a seguir. Substitua os valores destacados nas sequências de caracteres a seguir pelos valores apropriados da sua conta de usuário do IAM.

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

Depois de concluir todos os pré-requisitos, copie o `package.json` arquivo e o `index.js` script a seguir em seu ambiente local usando seu editor:

pacote.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();
```

O código de exemplo anterior usa o Axios para fazer solicitações RPC ao endpoint Bitcoin e assina essas solicitações com os cabeçalhos apropriados do Signature Version 4 (SigV4) usando as ferramentas oficiais do SDK v3. AWS Para executar o código, abra um terminal no mesmo diretório dos seus arquivos e execute o seguinte:

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

O resultado gerado será semelhante ao seguinte:

```
{"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**
>
> A solicitação de amostra no script anterior faz a `getblock` chamada com o mesmo hash de bloco de parâmetros de entrada do Faça solicitações AMB Access Bitcoin JSON-RPC em awscurl usando o AWS CLI exemplo. Para fazer outras chamadas, modifique o `rpc` objeto no script com um Bitcoin JSON-RPC diferente. Você pode alterar a opção de propriedade do host para Bitcoin `testnet` para fazer chamadas nesse endpoint.

Use o AMB Access Bitcoin em AWS PrivateLink

AWS PrivateLink é uma tecnologia altamente disponível e escalável que você pode usar para conectar sua VPC a serviços de forma privada, como se eles estivessem em sua VPC. Você não precisa usar um gateway de internet, dispositivo NAT, endereço IP público, conexão AWS Direct Connect ou conexão VPN AWS Site-to-Site para se comunicar com o serviço a partir de suas sub-redes privadas. Para obter mais informações sobre AWS PrivateLink ou configurar AWS PrivateLink, consulte O que é AWS PrivateLink?

Você pode enviar solicitações Bitcoin JSON-RPC para o AMB Access Bitcoin AWS PrivateLink usando um VPC endpoint. As solicitações para esse endpoint privado não são passadas pela Internet aberta, então você pode enviar solicitações diretamente para os endpoints Bitcoin usando a mesma autenticação SigV4. Para obter mais informações, consulte Acessar AWS serviços por meio de AWS PrivateLink.

Para o nome do serviço, procure Amazon Managed Blockchain na coluna AWS de serviço. Para obter mais informações, consulte AWS serviços que se integram com AWS PrivateLink o. O nome do serviço para o endpoint estará no seguinte formato:`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

Por exemplo: `com.amazonaws.`*`us-east-1`*`.managedblockchain.bitcoin.`*`testnet`*.

Casos de uso de Bitcoin com Amazon Managed Blockchain (AMB) Acesse Bitcoin

Este tópico fornece uma lista de casos de uso do AMB Access Bitcoin

Tópicos

Crie uma carteira Bitcoin (BTC) para enviar e receber BTC

O BTC, a criptomoeda nativa da rede Bitcoin, serve como um componente essencial do modelo de segurança da rede. Também atua como mercadoria e meio de troca, amplamente utilizado por instituições, empresas e indivíduos. Consequentemente, muitos aplicativos de carteira dependem dos nós do Bitcoin para interagir com o blockchain do Bitcoin. Esses aplicativos calculam o saldo de saídas não gastas (UTXOs) para um determinado conjunto de endereços, assinam e enviam transações para a rede Bitcoin e recuperam dados sobre transações históricas.

A seguir está uma amostra de alguns dos JSON de Bitcoin RPCs que o Amazon Managed Blockchain (AMB) Access Bitcoin suporta para transações de carteira BTC:

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

Para obter mais informações, consulte JSON- compatível RPCs.

Analise a atividade na blockchain Bitcoin

Você pode analisar o volume da atividade de transação no blockchain Bitcoin usando o método `getchaintxstats` JSON-RPC. Esse JSON-RPC permite acessar métricas como taxas médias

de transação por segundo, contagem total de transações, contagem de blocos e muito mais. Você também pode definir uma janela de números de blocos ou um hash de bloco como delimitador para calcular essas estatísticas para um conjunto específico de blocos na rede, se desejar.

Para obter mais informações, consulte JSON- compatível RPCs.

Verifique as mensagens assinadas usando um par de chaves Bitcoin

As carteiras Bitcoin têm uma chave privada e uma chave pública que formam um par de chaves. Essas chaves são usadas para assinar transações e servir como identidade do usuário no blockchain. A chave pública é usada para criar endereços, que são identificadores alfanuméricos padronizados (27 a 34 caracteres). Esses endereços são usados para receber saídas BTC e lidar com transações ou mensagens.

Com uma carteira Bitcoin, os usuários também podem assinar e verificar mensagens criptograficamente. Esse processo geralmente é usado para provar a propriedade de um endereço de carteira específico e do BTC associado a ele. Ao usar o `verifymessage` Bitcoin JSON-RPC, você pode verificar a autenticidade e a validade de uma mensagem assinada por outra carteira. Especificamente, um nó Bitcoin pode ser usado para verificar se uma mensagem foi assinada usando a chave privada correspondente ao endereço derivado da chave pública fornecida na própria mensagem assinada.

Para obter mais informações, consulte JSON- compatível RPCs.

Inspecione o mempool Bitcoin

Muitos aplicativos precisam acessar o mempool para acompanhar as transações pendentes, obter uma lista de todas as transações pendentes ou descobrir de onde veio uma transação. Para fazer isso, existem Bitcoin, do RPCs tipo JSON `getmempoolancestorsgetmempoolentry`, e `getrawmempool` que suportam essa atividade. Esses aplicativos Bitcoin JSON RPCs ajudam a obter as informações de que precisam do mempool.

O Amazon Managed Blockchain (AMB) Access Bitcoin também suporta o `testmempoolaccept` Bitcoin JSON-RPCs, que permite verificar se uma transação atende às regras do protocolo e se seria aceita por um nó antes do envio. Carteiras, bolsas e quaisquer outras entidades que enviam transações diretamente para o blockchain Bitcoin utilizam esses Bitcoin JSON-. RPCs

Para obter mais informações, consulte JSON- compatível RPCs.

Bitcoin JSON compatível - RPCs com Amazon Managed Blockchain (AMB) Acesse Bitcoin

Este tópico fornece uma lista e referências ao Bitcoin JSON RPCs que o Managed Blockchain suporta. Cada JSON-RPC compatível tem uma breve descrição de seu uso.

Note

- Você pode autenticar o Bitcoin JSON- RPCs no Managed Blockchain usando o processo de assinatura Signature Version 4 (SigV4). Isso significa que somente os diretores autorizados do IAM na AWS conta podem interagir com ela usando o Bitcoin JSON-. RPCs Forneça AWS credenciais (um ID da chave de acesso e uma chave de acesso secreta) com a chamada.
- Se sua resposta HTTP for maior que 10 MB, você receberá um erro. Para corrigir isso, você deve definir os cabeçalhos de compressão como`Accept-Encoding:gzip`. A resposta comprimida que seu cliente recebe contém os seguintes cabeçalhos: e. `Content-Type: application/json` `Content-Encoding: gzip`
- O Amazon Managed Blockchain (AMB) Access Bitcoin gera um erro 400 para solicitações JSON-RPC malformadas.
- Use o `sendrawtransaction` JSON-RPC para enviar transações que atualizem o estado do blockchain do Bitcoin.
- O AMB Access Bitcoin tem um limite de solicitação padrão de 100 solicitações por segundo (RPS)`NETWORK_TYPE`, por AWS região.

  Para aumentar sua cota, você deve entrar em contato com o AWS suporte. Para entrar em contato com o AWS suporte, faça login no console do AWS Support Center. Escolha Criar caso. Escolha Técnico. Escolha o Managed Blockchain como seu serviço. Escolha Access:Bitcoin como sua categoria e Orientação geral como sua gravidade. Insira a Cota RPC como Assunto e na caixa de texto Descrição e liste os limites de cota aplicáveis às suas necessidades em RPS por rede Bitcoin por região. Envie seu caso.

JSON- compatível RPCs

O AMB Access Bitcoin suporta o seguinte Bitcoin JSON-. RPCs Cada chamada suportada tem uma breve descrição de seu uso.

Categoria	JSON-RPC	Descrição
Blockchain RPCs	obtenha o melhor hash de bloco	Retorna o hash do melhor bloco (dica) na cadeia mais trabalhosa e totalmente validada.
	obter bloqueio	Se a verbosidade for 0, retornará uma string serializada com dados codificados em hexadecimal para o bloco 'hash'. Se a verbosidade for 1, retornará um objeto com informações sobre o bloco 'hash'. Se a verbosidade for 2, retornará um objeto com informações sobre o 'hash' do bloco e informações sobre cada transação. Se a verbosidade for 3, retornará um objeto com informações sobre o 'hash' do bloco e informações sobre cada transação, incluindo as `prevout` informações das entradas.
	obtenha informações sobre blockchain	Retorna um objeto contendo várias informaçõ es de estado relacionadas ao processamento de blockchain.
	obter contagem de blocos	Retorna a altura da cadeia mais trabalhosa e totalmente validada. O bloco de gênese tem altura 0.
	obter filtro de blocos	Recupera um filtro de conteúdo BIP 157 para um bloco específico usando o hash do bloco.
	obtenha o hash do bloco	Retorna o hash do bloco best-block-chain na altura fornecida.

Categoria	JSON-RPC	Descrição
	obter cabeçalho de bloco	Se verbose for falso, retornará uma string serializada com dados codificados em hexadecimal para o cabeçalho de bloco 'hash'. Se verbose for verdadeiro, retornará um objeto com informações sobre o cabeçalho de bloco 'hash'.
	obtenha estatísticas de blocos	Calcula estatísticas por bloco para uma determinada janela. Todos os valores estão em satoshis. Não funcionará em algumas alturas com a poda.
	receba dicas de cadeias	Retorna informações sobre todas as pontas conhecidas na árvore de blocos, incluindo a cadeia principal e os galhos órfãos.
	estatísticas de getchaintx	Calcula estatísticas sobre o número total e a taxa de transações na cadeia.
	ter dificuldade	Retorna a proof-of-work dificuldade como um múltiplo da dificuldade mínima.
	obtenha ancestrais de mempool	Se txid estiver no mempool, retornará todos os ancestrais no mempool.
	obtenha descendentes de mempool	Se txid estiver no mempool, retornará todos os descendentes no mempool.
	obter entrada do mempool	Retorna dados do mempool para determinada transação.
	obtenha informações do mempool	Retorna detalhes sobre o estado ativo do pool de memória TX.

Categoria	JSON-RPC	Descrição
	obtenha uma piscina de cânhamo crua	Retorna todas as transações IDs no pool de memória como uma matriz JSON de transação IDs de string. **Note** Não há suporte ao `verbose = true`.
	tire o txout	Retorna detalhes sobre a saída de uma transação não gasta.
	gettxoutproof	Retorna uma prova codificada em hexadecimal de que “txid” foi incluído em um bloco.
Transações brutas RPCs	criar transação bruta	Cria uma transação gastando as entradas fornecidas e criando novas saídas.
	decodificar transação bruta	Retorna um objeto JSON representando a transação serializada e codificada em hexadecimal.
	decodificação	Decodifica um script codificado em hexadecim al.
	obter transação bruta	Retorna os dados brutos da transação.
	transação de envio de sorteio	Envia uma transação bruta (serializada, codificada em hexadecimal) para o nó e a rede locais.
	testmempool aceita	Retorna o resultado dos testes de aceitação do mempool indicando se a transação bruta (serializada, codificada em hexadecimal) seria aceita pelo mempool. Isso verifica se a transação viola as regras de consenso ou de política.

Categoria	JSON-RPC	Descrição
Util RPCs	criar multisig	Cria um endereço com várias assinaturas sem a necessidade de assinar minhas chaves.
	estimar a taxa inteligente	Estima a taxa aproximada por quilobyte necessária para que uma transação comece a ser confirmada dentro dos blocos conf_target, se possível, e retorna o número de blocos para os quais a estimativa é válida. Usa o tamanho da transação virtual, conforme definido no BIP 141 (os dados da testemunha são descontad os).
	validar endereço	Retorna informações sobre o endereço bitcoin fornecido.
	verificar mensagem	Verifica uma mensagem assinada.

Segurança no Amazon Managed Blockchain (AMB) Acesse Bitcoin

A segurança na nuvem AWS é da mais alta prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança na nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Managed Blockchain (AMB) Access Bitcoin, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Para fornecer proteção de dados, autenticação e controle de acesso, o Amazon Managed Blockchain usa AWS recursos e os recursos da estrutura de código aberto executada no Managed Blockchain.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AMB Access Bitcoin. Os tópicos a seguir mostram como configurar o AMB Access Bitcoin para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de Bitcoin do AMB Access.

Tópicos

Proteção de dados no Amazon Managed Blockchain (AMB) Acesse Bitcoin

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no Amazon Managed Blockchain (AMB) Access Bitcoin. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome.

Isso inclui quando você trabalha com o AMB Access Bitcoin ou outro Serviços da AWS usando o console AWS CLI, API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia de dados

A criptografia de dados ajuda a impedir que usuários não autorizados leiam dados de uma rede blockchain e dos sistemas de armazenamento de dados associados. Isso inclui dados que podem ser interceptados enquanto viajam pela rede, conhecidos como dados em trânsito.

Criptografia em trânsito

Por padrão, o Managed Blockchain usa uma conexão HTTPS/TLS para criptografar todos os dados transmitidos de um computador cliente que executa os AWS CLI dois endpoints de serviço. AWS

Você não precisa fazer nada para ativar o uso do HTTPS/TLS. Ele está sempre ativado, a menos que você o desative explicitamente para um AWS CLI comando individual usando o `--no-verify-ssl` comando.

Gerenciamento de identidade e acesso para Amazon Managed Blockchain (AMB) Access Bitcoin

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos Bitcoin do AMB Access. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin
- Solução de problemas de identidade e acesso ao Bitcoin no Amazon Managed Blockchain (AMB)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso ao Bitcoin no Amazon Managed Blockchain (AMB)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas

políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AMB Access Bitcoin, saiba quais recursos do IAM estão disponíveis para uso com o AMB Access Bitcoin.

Recursos do IAM que você pode usar com o Amazon Managed Blockchain (AMB) Access Bitcoin

Recurso do IAM	Suporte AMB Access Bitcoin
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Não

Recurso do IAM	Suporte AMB Access Bitcoin
Chaves de condição de políticas	Não
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Não
Permissões de entidade principal	Não
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para ter uma visão de alto nível de como o AMB Access Bitcoin e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AMB Access Bitcoin

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para AMB Access Bitcoin

Para ver exemplos de políticas baseadas em identidade do AMB Access Bitcoin, consulte. Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

Políticas baseadas em recursos dentro do AMB Access Bitcoin

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AMB Access Bitcoin

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AMB Access Bitcoin, consulte Ações definidas pelo Amazon Managed Blockchain (AMB) Access Bitcoin na Referência de Autorização de Serviço.

As ações de política no AMB Access Bitcoin usam o seguinte prefixo antes da ação:

```
managedblockchain:
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

```
      "managedblockchain::action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `InvokeRpcBitcoin`, inclua a seguinte ação:

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

Para ver exemplos de políticas baseadas em identidade do AMB Access Bitcoin, consulte. Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

Recursos de política para AMB Access Bitcoin

Oferece compatibilidade com recursos de políticas: não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do AMB Access Bitcoin e seus ARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Acesse Bitcoin na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon Managed Blockchain (AMB) Acesse Bitcoin.

Para ver exemplos de políticas baseadas em identidade do AMB Access Bitcoin, consulte. Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

Chaves de condição de política para AMB Access Bitcoin

Compatível com chaves de condição de política específicas de serviço: não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AMB Access Bitcoin, consulte Chaves de condição para o Amazon Managed Blockchain (AMB) Access Bitcoin na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon Managed Blockchain (AMB) Acesse Bitcoin.

Para ver exemplos de políticas baseadas em identidade do AMB Access Bitcoin, consulte. Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

ACLs em AMB Access Bitcoin

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AMB Access Bitcoin

Oferece compatibilidade com ABAC (tags em políticas): não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com o AMB Access Bitcoin

Compatível com credenciais temporárias: não

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões principais entre serviços para AMB Access Bitcoin

Compatível com o recurso de encaminhamento de sessões de acesso (FAS): Não

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço do AMB Access Bitcoin

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AMB Access Bitcoin. Edite as funções de serviço somente quando o AMB Access Bitcoin fornecer orientação para fazer isso.

Funções vinculadas a serviços para AMB Access Bitcoin

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos Bitcoin do AMB Access. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AMB Access Bitcoin, incluindo o formato de cada um dos ARNs tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Managed Blockchain (AMB) Acesse Bitcoin na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usando o console AMB Access Bitcoin
- Permitir que os usuários visualizem suas próprias permissões
- Acessando redes Bitcoin

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do AMB Access Bitcoin em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o console AMB Access Bitcoin

Para acessar o console Bitcoin do Amazon Managed Blockchain (AMB), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AMB Access Bitcoin em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console AMB Access Bitcoin, anexe também o AMB Access Bitcoin *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

Acessando redes Bitcoin

> **Note**
>
> Para acessar os endpoints públicos do Bitcoin `mainnet` e `testnet` fazer chamadas JSON-RPC, você precisará de credenciais de usuário (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) que tenham as permissões apropriadas do IAM para o AMB Access Bitcoin.

Example Política do IAM para acessar todas as redes Bitcoin

Este exemplo concede a um usuário do IAM seu Conta da AWS acesso a todas as redes Bitcoin.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AccessAllBitcoinNetworks",
            "Effect": "Allow",
```

```
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
```

Example Política do IAM para acessar a rede Bitcoin Testnet

Este exemplo concede a um usuário do IAM seu Conta da AWS acesso à `testnet` rede Bitcoin.

JSON

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

Solução de problemas de identidade e acesso ao Bitcoin no Amazon Managed Blockchain (AMB)

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AMB Access Bitcoin e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no AMB Access Bitcoin

- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Bitcoin do AMB Access

Não estou autorizado a realizar uma ação no AMB Access Bitcoin

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `managedblockchain::`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `managedblockchain::`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AMB Access Bitcoin.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AMB Access Bitcoin. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Bitcoin do AMB Access

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AMB Access Bitcoin suporta esses recursos, consulteComo o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Registro em log do Amazon Managed Blockchain (AMB) Acesse eventos de Bitcoin usando AWS CloudTrail

> **Note**
>
> O Amazon Managed Blockchain (AMB) Access Bitcoin não oferece suporte a eventos de gerenciamento.

O Amazon Managed Blockchain está integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Managed Blockchain. CloudTrail captura quem invocou os endpoints AMB Access Bitcoin para o Managed Blockchain como eventos do plano de dados.

Se você criar uma trilha devidamente configurada que esteja inscrita para receber os eventos do plano de dados desejados, poderá receber a entrega contínua de eventos relacionados ao AMB Access Bitcoin em CloudTrail um bucket do Amazon S3. Usando as informações coletadas por CloudTrail, você pode determinar se uma solicitação foi feita para um dos endpoints Bitcoin da AMB Access, o endereço IP de onde veio a solicitação, quem fez a solicitação, quando ela foi feita e outros detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AMB Acesse as informações do Bitcoin em CloudTrail

AWS CloudTrail é ativado por padrão quando você cria seu Conta da AWS. No entanto, para ver quem invocou os endpoints Bitcoin do AMB Access, você deve configurar CloudTrail para registrar eventos do plano de dados.

Para manter um registro contínuo dos eventos em seu Conta da AWS, incluindo os eventos do plano de dados do AMB Access Bitcoin, você deve criar uma trilha. Uma trilha faz a CloudTrail entrega dos arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no Console de gerenciamento da AWS, a trilha se aplica a todos Regiões da AWS. A trilha registra eventos de todas as regiões suportadas na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar mais detalhadamente esses dados e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Usando CloudTrail para rastrear Bitcoin JSON- RPCs
- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Ao analisar os eventos CloudTrail de dados, você pode monitorar quem invocou os endpoints Bitcoin do AMB Access.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Compreendendo as entradas do arquivo de log Bitcoin do AMB Access

Para eventos do plano de dados, uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket S3 especificado. Cada arquivo de CloudTrail log contém uma ou mais entradas de log que representam uma única solicitação de qualquer fonte. Essas entradas fornecem detalhes sobre a ação solicitada, incluindo a data e a hora da ação e quaisquer parâmetros de solicitação associados.

> **Note**
>
> CloudTrail os eventos de dados nos arquivos de log não são um rastreamento de pilha ordenado das chamadas da API AMB Access Bitcoin, portanto, eles não aparecem em nenhuma ordem específica.

Usando CloudTrail para rastrear Bitcoin JSON- RPCs

Você pode usar CloudTrail para rastrear quem em sua conta invocou os endpoints Bitcoin do AMB Access e qual JSON-RPC foi invocado como eventos de dados. Por padrão, quando você cria uma trilha, os eventos de dados não são registrados. Para registrar quem invocou os endpoints Bitcoin do AMB Access como eventos de CloudTrail dados, você deve adicionar explicitamente os recursos suportados ou os tipos de recursos para os quais deseja coletar atividades em uma trilha. O Amazon Managed Blockchain suporta a adição de eventos de dados usando o Console de gerenciamento da AWS, AWS SDK e. AWS CLI Para obter mais informações, consulte Registrar eventos usando seletores avançados no Guia do AWS CloudTrail usuário.

Para registrar eventos de dados em uma trilha, use a put-event-selectorsoperação depois de criar a trilha. Use a `--advanced-event-selectors` opção para especificar os tipos de `AWS::ManagedBlockchain::Network` recursos para começar a registrar eventos de dados para determinar quem invocou os endpoints Bitcoin do AMB Access.

Example Entrada do registro de eventos de dados de todas as solicitações de endpoints AMB Access Bitcoin da sua conta

O exemplo a seguir demonstra como usar a `put-event-selectors` operação para registrar todas as solicitações de endpoint AMB Access Bitcoin da sua conta para a trilha `my-bitcoin-trail` na região. `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"] } ]}]'
```

Depois de se inscrever, você pode monitorar o uso no bucket do S3 que está conectado à trilha especificada no exemplo anterior.

O resultado a seguir mostra uma entrada no registro de eventos de CloudTrail dados das informações coletadas pelo CloudTrail. Você pode determinar se uma solicitação Bitcoin JSON-RPC foi feita para um dos endpoints Bitcoin do AMB Access, o endereço IP de onde veio a solicitação, quem fez a solicitação, quando ela foi feita e outros detalhes adicionais.

```
{
        "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"
}
```

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.