aws

Guia do Desenvolvedor

AMBAcesse Bitcoin

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMBAcesse Bitcoin: Guia do Desenvolvedor

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon Managed Blockchain (AMB) Access Bitcoin? 1
Você é um usuário de Bitcoin AMB Access pela primeira vez? 2
Principais conceitos 3
Considerações e limitações 3
Configuração 6
Pré-requisitos e considerações 6
Inscreva-se para AWS 6
Crie um IAM usuário com as permissões apropriadas 7
Instale e configure o AWS Command Line Interface 7
Conceitos básicos 8
Crie uma IAM política 8
RPCExemplo de console 9
exemplo de ascurl RPC 10
RPCExemplo de Node.js 11
AMBAcesse Bitcoin por PrivateLink 15
Casos de uso de Bitcoin 16
Crie uma carteira Bitcoin (BTC) para enviar e receber BTC 16
Analise a atividade na blockchain Bitcoin 16
Verifique as mensagens assinadas usando um par de chaves Bitcoin 17
Inspecione o mempool Bitcoin 17
Bitcoin JSON-RPCs 19
JSON-RPCs compatíveis 20
Segurança 24
Proteção de dados 25
Criptografia de dados 26
Criptografia em trânsito 26
Gerenciamento de identidade e acesso 26
Público 27
Autenticando com identidades 27
Gerenciando acesso usando políticas 31
Como o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com IAM 34
Exemplos de políticas baseadas em identidade 41
Solução de problemas 45
CloudTrail troncos 48

AMB Acesse as informações do Bitcoin em CloudTrail 48
Compreendendo as entradas do arquivo de log Bitcoin do AMB Access 49
Usando CloudTrail para rastrear Bitcoin JSON-RPCs 50
..... lii

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-RPCs compatíveis 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 RPCs Bitcoin JSON 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.

- Supported Regions (Regiões compatíveis)

  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)	ÍCONE	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 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 JSON-RPCs individuais do Bitcoin.

- 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 seus 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 um 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 no AWS, seu Conta da AWS é automaticamente inscrito para todos Serviços da AWS, incluindo Amazon Managed Blockchain (AMB) Acesse Bitcoin. Você será cobrado apenas pelos serviços que usar.

Se você tem um Conta da AWS já, vá para a próxima etapa. Se você não tem um Conta da AWS, use o procedimento a seguir para criar um.

Para criar um 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 e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário root tem acesso a todos 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 IAM usuário com as permissões apropriadas

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

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

Para obter informações sobre como criar um IAM usuário, consulte Criação de um IAM usuário no seu AWS conta. Para obter mais informações sobre como anexar uma política de permissões a um usuário, consulte Alterando as permissões de um IAM usuário. 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 o mais recente AWS Interface de linha de comando (CLI) com a qual trabalhar AWS recursos de um terminal. Para obter mais informações, consulte Instalando ou atualizando a versão mais recente do AWS CLI.

> **Note**
>
> Para CLI acessar, você precisa de um ID de chave de acesso e 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 Usando credenciais temporárias com AWS recursos no Guia do IAM usuário.

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 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 IAM política para acessar o Bitcoin JSON - RPCs
- Faça solicitações de chamada de procedimento remoto (RPC) do Bitcoin no RPC editor do AMB Access usando o AWS Management Console
- Faça RPC solicitações de AMB acesso ao Bitcoin JSON em awscurl usando o AWS CLI
- Faça Bitcoin JSON - RPC solicitações em Node.js
- Use o AMB Access Bitcoin em AWS PrivateLink

Crie uma IAM política para acessar o Bitcoin JSON - RPCs

Para acessar os endpoints públicos da Bitcoin Mainnet e da Testnet para fazer JSON RPC chamadas, você deve ter credenciais de usuário (AWS_ACCESS_ KEY _ID e AWS_SECRET _ _) que tenham as permissões apropriadas para que o Amazon IAM Managed Blockchain (KEY) acesse o Bitcoin. ACCESS AMB Em um terminal com o AWS CLI instalado, execute o seguinte comando para criar uma IAM política 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 IAM usuário para que ela entre em vigor. No painel, AWS Management Console, navegue até o IAM serviço e anexe a política `AmazonManagedBlockchainBitcoinAccess` à função atribuída ao seu IAM usuário. Para obter mais informações, consulte Criação de uma função e atribuição a um IAM usuário.

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

Você pode editar e enviar chamadas de procedimento remoto (RPCs) no AWS Management Console usando o AMB Access. Com elesRPCs, 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`. `getBlock` RPC Substitua as variáveis destacadas por suas próprias entradas ou escolha um dos outros RPCmétodos listados e insira as entradas relevantes necessárias.

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. Escolha o RPCeditor.
3. Na seção Solicitação, escolha *BITCOIN_MAINNET* como Rede Blockchain.
4. Escolha *getblock* como RPCmétodo.
5. Insira *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09* como o número do bloco e escolha *0* como a verbosidade.
6. Escolha Submit (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 RPCssuporte do AMB Access Bitcoin

Faça RPC solicitações de AMB acesso ao Bitcoin JSON em awscurl usando o AWS CLI

Example

Assine solicitações com suas credenciais de IAM usuário usando o Signature Version 4 (SigV4) para fazer RPC chamadas Bitcoin para os JSON endpoints do AMB Access Bitcoin. A ferramenta de linha de comando awscurl pode ajudar você a assinar solicitações para AWS serviços usando SigV4. Para obter mais informações, consulte READMEawscurl .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 o AWS CLI, suas credenciais de IAM usuário e a AWS região padrão são definidas em seu ambiente e têm acesso ao awscurl. Usando awscurl, envie uma solicitação para a Bitcoin Mainnet e a Testnet invocando o. `getblock` RPC 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 pelo seu Bitcoin preferido JSON - RPC e AWS Região que é suportada pelo Amazon Managed Blockchain (AMB) Acesse 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 Bitcoin JSON - RPC solicitações em Node.js

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

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 IAM usuário.

```
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 RPC solicitações ao endpoint Bitcoin e assina essas solicitações com os cabeçalhos apropriados do Signature Version 4 (SigV4) usando o código oficial AWS SDKferramentas v3. 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 RPC solicitações de AMB acesso ao Bitcoin JSON em awscurl usando o AWS CLI exemplo. Para fazer outras chamadas, modifique o `rpc` objeto no script com um Bitcoin diferente JSON -RPC. 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 seus VPC serviços de forma privada, como se estivessem no seu. VPC Você não precisa usar um gateway de internet, NAT dispositivo, endereço IP público, AWS Conexão Direct Connect ou AWS VPNConexão site a site para se comunicar com o serviço a partir de suas sub-redes privadas. Para obter mais informações sobre AWS PrivateLink ou para configurar AWS PrivateLink, veja O que é AWS PrivateLink?

Você pode enviar Bitcoin JSON - RPC solicitações para AMB acessar o 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 Access AWS serviços por meio de AWS PrivateLink.

Para o nome do serviço, procure Amazon Managed Blockchain na AWS coluna de serviço. Para ter mais informações, consulte AWS serviços que se integram com AWS PrivateLink. 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
- Analise a atividade na blockchain Bitcoin
- Verifique as mensagens assinadas usando um par de chaves Bitcoin
- Inspecione o mempool Bitcoin

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-RPCs de Bitcoin que o Amazon Managed Blockchain (AMB) Access Bitcoin suporta para transações de carteira BTC:

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

Para ter mais informações, consulte JSON-RPCs compatíveis.

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 ter mais informações, consulte JSON-RPCs compatíveis.

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 ter mais informações, consulte JSON-RPCs compatíveis.

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 RPCs JSON de Bitcoin como`getmempoolancestors`,`getmempoolentry`, e `getrawmempool` que suportam essa atividade. Esses Bitcoin JSON-RPCs ajudam os aplicativos a obter as informações de que precisam do mempool.

O Amazon Managed Blockchain (AMB) Access Bitcoin também oferece suporte ao `testmempoolaccept` Bitcoin JSON-RPCs, o 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 ter mais informações, consulte JSON-RPCs compatíveis.

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

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

Note

- Você pode autenticar 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 os 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-RPCs compatíveis

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

Categoria	JSON-RPC	Descrição
RPCs de blockchain	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
	pegue uma piscina crua	Retorna todos os IDs de transação no pool de memória como uma matriz JSON de IDs de transação 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.
RPCs de transações brutas	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 hexadecimal.
	obter transação bruta	Retorna os dados brutos da transação.
	transação de envio bruto	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
Até 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
- Gerenciamento de identidade e acesso para Amazon Managed Blockchain (AMB) Access Bitcoin

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

A ferramenta AWS modelo de responsabilidade compartilhada 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 todas as 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 do Serviços da AWS que você usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o AWS Modelo de responsabilidade compartilhada e postagem no GDPR blog sobre o AWS Blog de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS credenciais e configure usuários individuais com AWS IAM Identity Center 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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Trabalhando com CloudTrail trilhas no AWS CloudTrail Guia do usuário.
- Use AWS soluções de criptografia, junto com todos os controles de segurança padrão dentro 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 FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um FIPS endpoint. Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações 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 consoleAPI, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou 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 altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse 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 TLS conexãoHTTPS/para criptografar todos os dados transmitidos de um computador cliente que executa o AWS CLI para AWS endpoints de serviço.

Você não precisa fazer nada para habilitar o uso deHTTPS/TLS. Ele está sempre ativado, a menos que você o desative explicitamente para um indivíduo AWS CLI comando 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 um AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso ao AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AMB Access Bitcoin. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com IAM
- Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

- Solução de problemas do Amazon Managed Blockchain (AMB) Acesse a identidade e o acesso ao Bitcoin

Público

Como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AMB Access Bitcoin.

Usuário do serviço — Se você usa o serviço AMB Access Bitcoin para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do AMB Access Bitcoin para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no AMB Access Bitcoin, consulteSolução de problemas do Amazon Managed Blockchain (AMB) Acesse a identidade e o acesso ao Bitcoin.

Administrador de serviços — Se você é responsável pelos recursos do AMB Access Bitcoin em sua empresa, provavelmente tem acesso total ao AMB Access Bitcoin. É seu trabalho determinar quais recursos e recursos do AMB Access Bitcoin seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar IAM o AMB Access Bitcoin, consulteComo o Amazon Managed Blockchain (AMB) Access Bitcoin funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AMB Access Bitcoin. Para ver exemplos de políticas baseadas em identidade do AMB Access Bitcoin que você pode usarIAM, consulte. Exemplos de políticas baseadas em identidade para Amazon Managed Blockchain (AMB) Access Bitcoin

Autenticando com identidades

Autenticação é como você faz login em AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado em AWS) como o Usuário raiz da conta da AWS, como IAM usuário ou assumindo uma IAM função.

Você pode fazer login em AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu

administrador configurou previamente a federação de identidades usando IAM funções. Quando você acessa AWS ao usar a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou o AWS portal de acesso. Para obter mais informações sobre como fazer login no AWS, veja Como fazer login no seu Conta da AWS no Início de Sessão da AWS Guia do usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Assinatura AWS APIsolicitações no Guia do IAM usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no AWS IAM Identity Center Guia do usuário e uso da autenticação multifatorial (MFA) em AWS no IAM Guia do usuário.

Conta da AWS usuário raiz

Quando você cria um Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS e recursos na conta. Essa identidade é chamada de Conta da AWS usuário root e é acessado fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, um provedor de identidade da web, o AWS Directory Service, o diretório do Identity Center ou qualquer usuário que acesse Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, eles assumem funções, e as funções fornecem credenciais temporárias.

Para gerenciamento de acesso centralizado, recomendamos que você use AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no AWS IAM Identity Center Guia do usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro do seu Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Um IAMpapel é uma identidade dentro de você Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de papéis. Você pode assumir uma função chamando um AWS CLI ou AWS APIoperação ou usando um personalizadoURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa

identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no AWS IAM Identity Center Guia do usuário.

- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS use recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações no AWS, você é considerado diretor. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinado com a solicitação AWS service (Serviço da AWS) para fazer solicitações para serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou recursos para concluir. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS) no IAM Guia do usuário.
  - Função vinculada a serviços — Uma função vinculada a serviços é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de realizar

uma ação em seu nome. As funções vinculadas ao serviço aparecem em seu Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI ou AWS APIsolicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir um AWS Ao atribuir a uma EC2 instância e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância que é anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso em AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto em AWS que, quando associados a uma identidade ou recurso, definem suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada em AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

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

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console, o AWS CLI, ou o AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas gerenciadas incluem AWS políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

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

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

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF, e a Amazon VPC são exemplos de serviços que oferecem suporteACLs. Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades em contas de membros, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no AWS Organizations Guia do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

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 determina se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

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

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

IAMrecursos que você pode usar com o Amazon Managed Blockchain (AMB) Acesse Bitcoin

IAMrecurso	AMBAcesse o suporte do Bitcoin
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Não
Chaves de condição de políticas	Não
ACLs	Não
ABAC(tags nas políticas)	Não
Credenciais temporárias	Não
Permissões de entidade principal	Não
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para obter uma visão de alto nível de como AMB acessar Bitcoin e outros AWS os serviços funcionam com a maioria dos IAM recursos, consulte AWS serviços que funcionam com IAM o Guia IAM do Usuário.

Políticas baseadas em identidade para Access Bitcoin AMB

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 Criação de IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para Access Bitcoin AMB

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 no Access Bitcoin AMB

Suporte a políticas baseadas em recursos: não

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

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso estão em condições diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder

acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para AMB Access Bitcoin

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que as associadas AWS APIoperação. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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) Acesse 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 suporte a recursos políticos: Não

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

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, 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 seusARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Acesse Bitcoin na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo Amazon Managed Blockchain (AMB) Acesse Bitcoin. ARN

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

Suporta chaves de condição de política específicas do serviço: Não

Os administradores podem usar AWS JSONpolíticas 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários `Condition` elementos em uma instrução ou várias chaves em um único `Condition` elemento, AWS os avalia usando uma `AND` operação lógica. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver tudo AWS chaves de condição globais, consulte AWS chaves de contexto de condição global no Guia IAM do usuário.

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

ACLsem AMB Access Bitcoin

SuportesACLs: Não

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

ABACcom AMB Access Bitcoin

Suportes ABAC (tags nas políticas): Não

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitas AWS recursos. Marcar entidades e

recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o AMB Access Bitcoin

Suporta credenciais temporárias: Não

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS trabalhar com credenciais temporárias, consulte Serviços da AWS que funcionam com IAM o Guia IAM do Usuário.

Você está usando credenciais temporárias se fizer login no AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Você pode então usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões principais entre serviços para AMB Access Bitcoin

Suporta sessões de acesso direto (FAS): Não

Quando você usa um IAM usuário ou uma função para realizar ações no AWS, você é considerado diretor. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinado com a solicitação AWS service (Serviço da AWS) para fazer solicitações para serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou recursos para concluir. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço do AMB Access Bitcoin

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS) no IAM Guia do usuário.

> **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 Access Bitcoin AMB

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 a função de realizar uma ação em seu nome. As funções vinculadas ao serviço aparecem em seu Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre a criação ou o gerenciamento de funções vinculadas ao serviço, consulte AWS serviços que funcionam com IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada 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 do AMB Access Bitcoin. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI), ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

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

Tópicos

- Melhores práticas de política
- Usando o console AMB Access Bitcoin
- Permitir que usuários visualizem suas próprias permissões
- Acessando redes Bitcoin

Melhores práticas 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 o seu Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS políticas gerenciadas e migrar para permissões com privilégios mínimos — Para começar a conceder permissões para seus usuários e cargas de trabalho, use o AWS políticas gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis em seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo AWS políticas gerenciadas pelo cliente que são específicas para seus casos de uso. Para ter mais informações, consulte AWS políticas gerenciadas ou AWS políticas gerenciadas para funções de trabalho no Guia IAM do usuário.

- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de um determinado AWS service (Serviço da AWS), por exemplo, AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root em seu Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

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. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas, o console não funcionará conforme planejado para entidades (usuários ou funções) com essa política.

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

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

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou AWS API.

```
{
    "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 JSON RPC chamadas, você precisará de credenciais de usuário (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) que tenham as IAM permissões apropriadas para o AMB Access Bitcoin.

Example IAMPolítica para acessar todas as redes Bitcoin

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

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

Example IAMPolítica para acessar a rede Bitcoin Testnet

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

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

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

Solução de problemas do Amazon Managed Blockchain (AMB) Acesse a identidade e o acesso ao Bitcoin

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. 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 Conta da AWS para acessar meus recursos do AMB Access Bitcoin

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, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictíciasmanagedblockchain::*`GetWidget`*.

```
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 IAM usuário 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 Conta da AWS para acessar meus recursos do AMB Access Bitcoin

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode 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 IAM.
- Para saber como fornecer acesso aos seus recursos em Contas da AWS que você possui, consulte Fornecendo acesso a um IAM usuário em outro Conta da AWS que você possui no Guia do IAM Usuário.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecendo acesso a Contas da AWS propriedade de terceiros no Guia do IAM Usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

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 AWS Management Console, 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 mais informações, 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:

- 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 o elemento CloudTrail userIdentity.

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 AWS Management Console, 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.