aws

Entwicklerhandbuch

AMB Access Bitcoin

AMB Access Bitcoin: Entwicklerhandbuch

Table of Contents

Was ist Amazon Managed Blockchain (AMB) Access Bitcoin?

Amazon Managed Blockchain (AMB) Access bietet Ihnen öffentliche Blockchain-Knoten für Ethereum und Bitcoin, und Sie können mit dem Hyperledger Fabric-Framework auch private Blockchain-Netzwerke erstellen. Wählen Sie aus verschiedenen Methoden für die Interaktion mit öffentlichen Blockchains, darunter vollständig verwaltete Single-Tenant- (dedizierte) und serverlose Multi-Tenant-API-Operationen für öffentliche Blockchain-Knoten. Für Anwendungsfälle, in denen Zugriffskontrollen wichtig sind, können Sie aus vollständig verwalteten privaten Blockchain-Netzwerken wählen. Standardisierte API-Operationen bieten Ihnen sofortige Skalierbarkeit auf einer vollständig verwalteten, ausfallsicheren Infrastruktur, sodass Sie Blockchain-Anwendungen erstellen können.

AMB Access bietet Ihnen zwei verschiedene Arten von Blockchain-Infrastrukturdiensten: API-Operationen für den mehrinstanzenfähigen Blockchain-Netzwerkzugriff und dedizierte Blockchain-Knoten und -Netzwerke. Mit einer speziellen Blockchain-Infrastruktur können Sie öffentliche Ethereum-Blockchain-Knoten und private Hyperledger Fabric-Blockchainnetzwerke für Ihren eigenen Gebrauch erstellen und verwenden. API-basierte Mehrmandantenangebote wie AMB Access Bitcoin bestehen jedoch aus einer Flotte von Bitcoin-Knoten hinter einer API-Ebene, in der die zugrunde liegende Blockchain-Knoteninfrastruktur von den Kunden gemeinsam genutzt wird.

Bitcoin ist ein dezentrales Blockchain-Netzwerk, das sichere peer-to-peer Transaktionen im Wert von Bitcoin (BTC), der systemeigenen Kryptowährung des Netzwerks, ermöglicht. Das Bitcoin-Netzwerk wird von Einzelpersonen, Finanzinstituten, Fintech-Unternehmen, Regierungen und mehr genutzt. Das Bitcoin-Netzwerk ist ein Austauschmedium, eine Investitionsware oder ein öffentlich überprüfbares und unveränderliches Hauptbuch für eingeschriebene Daten. Mit Amazon Managed Blockchain (AMB) Access Bitcoin können Sie über regionale Endpunkte auf einen Pool von Bitcoin-Mainnet- und Testnet-Netzwerken zugreifen, über die Sie Transaktionen schreiben, Daten aus dem Ledger lesen und JSON-RPC-Anfragen aufrufen können, die auf dem Bitcoin Core-Node-Client verfügbar sind. Mit serverlosen Bitcoin-Endpunkten können Sie sich auf die Entwicklung Ihrer Anwendungen konzentrieren, anstatt in undifferenzierte Aufgaben wie die Bereitstellung, Wartung und Lastverteilung von Bitcoin-Knoten zu investieren. Ganz gleich, ob Sie eine Bitcoin-Wallet erstellen, eine Krypto-Börse aufbauen oder Bitcoin-Blockchaindaten analysieren — mit AMB Access Bitcoin zahlen Sie nur für die Anfragen, die Sie über die Bitcoin-Endpunkte stellen.

Sind Sie zum ersten Mal AMB Access Bitcoin-Nutzer?

Wenn Sie AMB Access Bitcoin zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Schlüsselkonzepte: Amazon Managed Blockchain (AMB) Access Bitcoin
- Erste Schritte mit Amazon Managed Blockchain (AMB) Access Bitcoin
- Bitcoin-Anwendungsfälle mit Amazon Managed Blockchain (AMB) Access Bitcoin
- Unterstütztes Bitcoin-JSON — RPCs mit Amazon Managed Blockchain (AMB) auf Bitcoin zugreifen

Schlüsselkonzepte: Amazon Managed Blockchain (AMB) Access Bitcoin

> **Note**
>
> In diesem Leitfaden wird davon ausgegangen, dass Sie mit den für Bitcoin wesentlichen Konzepten vertraut sind. Zu diesen Konzepten gehören Dezentralisierung, Knoten, Transaktionen proof-of-work, Wallets, öffentliche und private Schlüssel, Halbierungen und andere. Bevor Sie Amazon Managed Blockchain (AMB) Access Bitcoin verwenden, empfehlen wir Ihnen, die Bitcoin Development Documentation und Mastering Bitcoin zu lesen.

Amazon Managed Blockchain (AMB) Access Bitcoin bietet Ihnen serverlosen Zugriff auf die Bitcoin-Blockchain, ohne dass Sie eine Bitcoin-Infrastruktur, einschließlich Knoten, bereitstellen und verwalten müssen. Mit diesem verwalteten Service können Sie schnell und bei Bedarf auf die Bitcoin-Netzwerke zugreifen und so Ihre Gesamtbetriebskosten senken.

Der AMB Access Bitcoin bietet Ihnen Zugriff auf das Bitcoin-Netzwerk über vollständige Knoten, auf denen der Bitcoin Core-Client ausgeführt wird, wobei die Wallet-Funktionalität deaktiviert ist und mehrere JSON Remote Procedure (JSON-RPC) -Aufrufe unterstützt werden. Sie können Bitcoin JSON aufrufen, um mit Bitcoin-Knoten RPCs zu kommunizieren, die von Managed Blockchain verwaltet werden, um mit den Bitcoin-Netzwerken zu interagieren. Mit Bitcoin JSON- RPCs können Sie Daten lesen und Transaktionen schreiben, einschließlich der Abfrage von Daten und der Übermittlung von Transaktionen an die Bitcoin-Netzwerke mithilfe des Amazon Managed Blockchain Blockchain-Service.

> **Important**
>
> Sie sind für die Erstellung, Pflege, Verwendung und Verwaltung Ihrer Bitcoin-Adressen verantwortlich. Sie sind auch für den Inhalt Ihrer Bitcoin-Adressen verantwortlich. AWS ist nicht verantwortlich für Transaktionen, die über Bitcoin-Knoten auf Amazon Managed Blockchain bereitgestellt oder aufgerufen werden.

Überlegungen und Einschränkungen bei der Verwendung von Amazon Managed Blockchain (AMB) Access Bitcoin

- Unterstützte Bitcoin-Netzwerke

  AMB Access Bitcoin unterstützt die folgenden öffentlichen Netzwerke:

  - Mainnet — Die öffentliche Bitcoin-Blockchain, die durch proof-of-work Konsens gesichert ist und auf der die Bitcoin (BTC) -Kryptowährung ausgegeben und abgewickelt wird. Transaktionen im Mainnet haben einen tatsächlichen Wert (das heißt, sie verursachen reale Kosten) und werden in der öffentlichen Blockchain aufgezeichnet.
  - Testnet — Das Testnet ist eine alternative Bitcoin-Blockchain, die zum Testen verwendet wird. Testnet-Münzen sind getrennt und unterscheiden sich von den tatsächlichen Bitcoin (BTC) und haben normalerweise keinen Wert.

  > **Note**
  >
  > Private Netzwerke werden nicht unterstützt.

- Unterstützte Regionen

  Im Folgenden sind die unterstützten Regionen für diesen Dienst aufgeführt:

Name der Region	Code	Region
USA Ost (Nord-Virginia)	IAD	`us-east-1`
Asien-Pazifik (Tokio)	NRT	ap-northeast-1
Asien-Pazifik (Seoul)	ICON	ap-northeast-2
Asien-Pazifik (Singapur)	SIN	ap-southeast-1
Europa (Irland)	DUB	eu-west-1
Europa (London)	LHR	eu-west-2

- Service-Endpunkte

Im Folgenden sind die Service-Endpunkte für AMB Access Bitcoin aufgeführt. Um eine Verbindung mit dem Dienst herzustellen, müssen Sie einen Endpunkt verwenden, der eine der unterstützten Regionen umfasst.

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

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

- Mining wird nicht unterstützt

  AMB Access Bitcoin unterstützt kein Bitcoin (BTC) -Mining.

- Signatur Version 4: Signierung von Bitcoin-JSON-RPC-Aufrufen

  Wenn Sie Bitcoin JSON- RPCs auf Amazon Managed Blockchain aufrufen, können Sie dies über eine HTTPS-Verbindung tun, die mit dem Signature Version 4-Signaturprozess authentifiziert wurde. Das bedeutet, dass nur autorisierte IAM-Prinzipale im AWS Konto Bitcoin-JSON-RPC-Aufrufe tätigen können. Zu diesem Zweck müssen beim AWS Anruf Anmeldeinformationen (eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel) bereitgestellt werden.

  > **Important**
  >
  > - Betten Sie keine Client-Anmeldeinformationen in benutzerseitige Anwendungen ein.
  > - Sie können IAM-Richtlinien nicht verwenden, um den Zugriff auf einzelne Bitcoin-JSON-Dateien einzuschränken. RPCs

- Es werden nur Einreichungen von Rohtransaktionen unterstützt

  Verwenden Sie den `sendrawtransaction` JSON-RPC, um Transaktionen einzureichen, die den Status der Bitcoin-Blockchain aktualisieren.

- AWS CloudTrail Unterstützung für Protokollierung

  Sie können so konfigurieren CloudTrail , dass Ihr Bitcoin-JSON- protokolliert wirdRPCs. Weitere Informationen finden Sie unter Protokollierung von Bitcoin-Ereignissen mit Amazon Managed Blockchain (AMB) Access mithilfe von AWS CloudTrail.

Einrichtung von Amazon Managed Blockchain (AMB) Access Bitcoin

Bevor Sie Amazon Managed Blockchain (AMB) Access Bitcoin zum ersten Mal verwenden, folgen Sie den Schritten in diesem Abschnitt, um ein AWS Konto zu erstellen. Im folgenden Kapitel wird beschrieben, wie Sie mit der Nutzung von AMB Access Bitcoin beginnen können.

Voraussetzungen und Überlegungen

Bevor Sie es AWS zum ersten Mal verwenden, benötigen Sie eine AWS-Konto.

Melde dich an für AWS

Wenn Sie sich für Bitcoin anmelden AWS, werden Sie AWS-Konto automatisch für alle registriert AWS-Services, einschließlich Amazon Managed Blockchain (AMB) Access Bitcoin. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Wenn Sie AWS-Konto bereits eine haben, fahren Sie mit dem nächsten Schritt fort. Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos aus.

Um ein AWS Konto zu erstellen

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Erstellen Sie einen IAM-Benutzer mit den entsprechenden Berechtigungen

Um AMB Access Bitcoin zu erstellen und damit zu arbeiten, benötigen Sie einen AWS Identity and Access Management (IAM-) Principal (Benutzer oder Gruppe) mit Berechtigungen, die die erforderlichen Managed Blockchain-Aktionen ermöglichen.

Nur IAM-Prinzipale können Bitcoin-JSON-RPC-Aufrufe tätigen. Wenn Sie Bitcoin JSON- RPCs auf Amazon Managed Blockchain aufrufen, können Sie dies über eine HTTPS-Verbindung tun, die mit dem Signature Version 4-Signaturprozess authentifiziert wurde. Das bedeutet, dass nur autorisierte IAM-Prinzipale im AWS Konto Bitcoin-JSON-RPC-Aufrufe tätigen können. Zu diesem Zweck müssen beim AWS Anruf Anmeldeinformationen (eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel) bereitgestellt werden.

Informationen zum Erstellen eines IAM-Benutzers finden Sie unter Einen IAM-Benutzer in Ihrem AWS Konto erstellen. Weitere Informationen dazu, wie Sie einem Benutzer eine Berechtigungsrichtlinie zuordnen, finden Sie unter Berechtigungen für einen IAM-Benutzer ändern. Ein Beispiel für eine Berechtigungsrichtlinie, mit der Sie einem Benutzer die Erlaubnis erteilen können, mit AMB Access Bitcoin zu arbeiten, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

Installieren und konfigurieren Sie AWS Command Line Interface

Falls Sie dies noch nicht getan haben, installieren Sie die neueste AWS Befehlszeilenschnittstelle (CLI), um mit AWS Ressourcen von einem Terminal aus zu arbeiten. Weitere Informationen finden Sie unter Installieren oder Aktualisierung auf die neueste Version von AWS CLI.

> **Note**
>
> Für CLI-Zugriff benötigen Sie eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Verwenden Sie möglichst temporäre Anmeldeinformationen anstelle langfristiger Zugriffsschlüssel. Temporäre Anmeldeinformationen bestehen aus einer Zugriffsschlüssel-ID, einem geheimen Zugriffsschlüssel und einem Sicherheits-Token, das angibt, wann die Anmeldeinformationen ablaufen. Weitere Informationen finden Sie unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Erste Schritte mit Amazon Managed Blockchain (AMB) Access Bitcoin

In den step-by-step Tutorials in diesem Abschnitt erfahren Sie, wie Sie Aufgaben mithilfe von Amazon Managed Blockchain (AMB) Access Bitcoin ausführen. Für diese Beispiele müssen Sie einige Voraussetzungen erfüllen. Wenn Sie mit AMB Access Bitcoin noch nicht vertraut sind, überprüfen Sie den Abschnitt Einrichtung dieses Handbuchs, um sicherzustellen, dass Sie diese Voraussetzungen erfüllt haben. Weitere Informationen finden Sie unter Einrichtung von Amazon Managed Blockchain (AMB) Access Bitcoin.

Themen

Erstellen Sie eine IAM-Richtlinie für den Zugriff auf Bitcoin JSON-RPCs

Um auf die öffentlichen Endpunkte für das Bitcoin-Mainnet und das Testnet zuzugreifen, um JSON-RPC-Aufrufe zu tätigen, benötigen Sie Benutzeranmeldedaten (AWS_ACCESS_KEY_ID und AWS_SECRET _ACCESS_KEY), die über die entsprechenden IAM-Berechtigungen für Amazon Managed Blockchain (AMB) Access Bitcoin verfügen. Führen Sie in einem Terminal, auf dem das AWS CLI installiert ist, den folgenden Befehl aus, um eine IAM-Richtlinie für den Zugriff auf beide Bitcoin-Endpunkte zu erstellen:

```
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**
>
> Im vorherigen Beispiel haben Sie Zugriff auf das Bitcoin-Mainnet und das Testnet. Verwenden Sie den folgenden `Action` Befehl, um Zugriff auf einen bestimmten Endpunkt zu erhalten:
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

Nachdem Sie die Richtlinie erstellt haben, fügen Sie diese Richtlinie der Rolle Ihres IAM-Benutzers hinzu, damit sie wirksam wird. Navigieren Sie im AWS-Managementkonsole zum IAM-Dienst und fügen Sie die Richtlinie der Rolle `AmazonManagedBlockchainBitcoinAccess` hinzu, die Ihrem IAM-Benutzer zugewiesen ist. Weitere Informationen finden Sie unter Rolle erstellen und sie einem IAM-Benutzer zuweisen.

Stellen Sie Bitcoin-RPC-Anfragen (Remote Procedure Call) im AMB Access RPC-Editor mit dem AWS-Managementkonsole

Sie können Remote-Prozeduraufrufe (RPCs) AWS-Managementkonsole mithilfe von AMB Access bearbeiten und einreichen. Mit diesen RPCs können Sie Daten lesen, Transaktionen im Bitcoin-Netzwerk schreiben und einreichen.

Example

Das folgende Beispiel zeigt, wie Sie mithilfe von RPC Informationen über *`blockhash`*00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 abrufen

können. `getBlock` Ersetzen Sie die hervorgehobenen Variablen durch Ihre eigenen Eingaben oder wählen Sie eine der anderen aufgeführten RPC-Methoden und geben Sie die entsprechenden erforderlichen Eingaben ein.

1. Öffnen Sie die Managed Blockchain-Konsole unter https://console.aws.amazon.com/managedblockchain/.
2. Wählen Sie den RPC-Editor.
3. Wählen Sie *`BITCOIN_MAINNET`* im Bereich Anfrage das Blockchain-Netzwerk aus.
4. Wählen Sie *`getblock`* als RPC-Methode.
5. Geben Sie *`00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09`* die Blocknummer ein und wählen Sie *`0`* die Ausführlichkeit.
6. Wählen Sie dann Submit RPC.
7. Die Ergebnisse werden im Antwortbereich dieser Seite angezeigt. Anschließend können Sie die vollständigen Rohtransaktionen zur weiteren Analyse oder zur Verwendung in der Geschäftslogik für Ihre Anwendungen kopieren.

Weitere Informationen finden Sie im von AMB Access RPCs unterstützten Bitcoin

Stellen Sie AMB Access Bitcoin JSON-RPC-Anfragen in awscurl, indem Sie den AWS CLI

Example

Signieren Sie Anfragen mit Ihren IAM-Benutzeranmeldedaten, indem Sie Signature Version 4 (Sigv4) verwenden, um Bitcoin-JSON-RPC-Aufrufe an die AMB Access Bitcoin-Endpunkte zu tätigen. Das awscurl-Befehlszeilentool kann Ihnen helfen, Anfragen an Dienste zu signieren, die Sigv4 verwenden. AWS Weitere Informationen finden Sie in der Datei awscurl README.md.

Installieren Sie awscurl mit der für Ihr Betriebssystem geeigneten Methode. Unter macOS HomeBrew ist die empfohlene Anwendung:

```
brew install awscurl
```

Wenn Sie die AWS CLI bereits installiert und konfiguriert haben, sind Ihre IAM-Benutzeranmeldedaten und die AWS-Standardregion in Ihrer Umgebung festgelegt und Sie

haben Zugriff auf awscurl. Senden Sie mit awscurl eine Anfrage sowohl an das Bitcoin-Mainnet als auch an das Testnet, indem Sie den RPC aufrufen. `getblock` Dieser Aufruf akzeptiert einen Zeichenkettenparameter, der dem Block-Hash entspricht, für den Sie Informationen abrufen möchten.

Der folgende Befehl ruft die Block-Header-Daten aus dem Bitcoin-Mainnet ab, indem er den Block-Hash im `params` Array verwendet, um den spezifischen Block auszuwählen, für den die Header abgerufen werden sollen. In diesem Beispiel wird der Endpunkt verwendet. `us-east-1` Sie können dies durch Ihr bevorzugtes Bitcoin-JSON-RPC und Ihre bevorzugte AWS Region ersetzen, die von Amazon Managed Blockchain (AMB) Access Bitcoin unterstützt werden. Darüber hinaus können Sie eine Anfrage an das Testnet-Netzwerk und nicht an das Mainnet richten, indem Sie im Befehl durch ersetzen. `mainnet` `testnet`

```
awscurl -X POST -d '{ "jsonrpc": "1.0", "id": "getblockheader-curltest", "method":
 "getblockheader", "params":
 ["000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0"] }' --service
 managedblockchain https://mainnet.bitcoin.managedblockchain.us-east-1.amazonaws.com
 --region us-east-1 -k
```

Die Ergebnisse enthalten Details aus den Block-Headern und eine Liste der Transaktions-Hashes, die im angeforderten Block enthalten sind. Sehen Sie sich das folgende Beispiel an:

```
{"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"}
```

Stellen Sie Bitcoin-JSON-RPC-Anfragen in Node.js

Sie können signierte Anfragen über HTTPS einreichen, um auf die Bitcoin Mainnet - und Testnet-Endpunkte zuzugreifen und JSON-RPC-API-Aufrufe zu tätigen, indem Sie das native https-Modul in Node.js verwenden, oder Sie können eine Drittanbieterbibliothek wie AXIOS verwenden. Das

folgende Beispiel zeigt Ihnen, wie Sie eine Bitcoin-JSON-RPC-Anfrage an die AMB Access Bitcoin-Endpunkte stellen.

Example

Um dieses Beispielskript Node.js auszuführen, müssen die folgenden Voraussetzungen erfüllt sein:

1. Sie müssen Node Version Manager (nvm) und Node.js auf Ihrem Computer installiert haben. Installationsanweisungen für Ihr Betriebssystem finden Sie hier.
2. Verwenden Sie den `node --version` Befehl und bestätigen Sie, dass Sie Node Version 14 oder höher verwenden. Bei Bedarf können Sie den `nvm install 14` Befehl gefolgt vom `nvm use 14` Befehl verwenden, um Version 14 zu installieren.
3. Die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` müssen die Anmeldeinformationen enthalten, die mit Ihrem Konto verknüpft sind. Die Umgebungsvariablen `AMB_HTTP_ENDPOINT` müssen Ihre AMB Access Bitcoin-Endpunkte enthalten.

   Exportieren Sie diese Variablen mithilfe der folgenden Befehle als Zeichenketten auf Ihrem Client. Ersetzen Sie die hervorgehobenen Werte in den folgenden Zeichenfolgen durch entsprechende Werte aus Ihrem IAM-Benutzerkonto.

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

Nachdem Sie alle Voraussetzungen erfüllt haben, kopieren Sie die folgende `package.json` Datei und `index.js` das folgende Skript mit Ihrem Editor in Ihre lokale Umgebung:

package.json

```
{
  "name": "bitcoin-rpc",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "@aws-crypto/sha256-js": "^4.0.0",
```

```
    "@aws-sdk/credential-provider-node": "^3.360.0",
    "@aws-sdk/protocol-http": "^3.357.0",
    "@aws-sdk/signature-v4": "^3.357.0",
    "axios": "^1.4.0"
  }
}
```

index.js

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

// define a signer object with AWS service name, credentials, and region
const signer = new SignatureV4({
  credentials: defaultProvider(),
  service: 'managedblockchain',
  region: 'us-east-1',
  sha256: SHA256,
});


const rpcRequest = async () => {

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

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

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

  // create an HTTP Request object
```

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


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

  try {
    //make the request using axios
    const response = await axios({...signedRequest, url: bitcoinURL, data: req.body})

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


}

rpcRequest();
```

Der vorherige Beispielcode verwendet Axios, um RPC-Anfragen an den Bitcoin-Endpunkt zu stellen, und signiert diese Anfragen mithilfe der offiziellen AWS SDK v3-Tools mit den entsprechenden Signature Version 4-Headern (Sigv4). Um den Code auszuführen, öffnen Sie ein Terminal im selben Verzeichnis wie Ihre Dateien und führen Sie Folgendes aus:

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

Das generierte Ergebnis sieht wie folgt aus:

```
{"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**
>
> Die Beispielanforderung im vorherigen Skript führt den `getblock` Aufruf mit demselben Block-Hash für den Eingabeparameter durch wie im Stellen Sie AMB Access Bitcoin JSON-RPC-Anfragen in awscurl, indem Sie den AWS CLI Beispiel. Um weitere Aufrufe zu tätigen, ändern Sie das `rpc` Objekt im Skript mit einem anderen Bitcoin-JSON-RPC. Sie können die Host-Eigenschaftsoption auf Bitcoin ändern, um Aufrufe an `testnet` diesem Endpunkt zu tätigen.

Verwenden Sie AMB Access Bitcoin über AWS PrivateLink

AWS PrivateLink ist eine hochverfügbare, skalierbare Technologie, mit der Sie Ihre VPC privat mit Diensten verbinden können, als ob sie sich in Ihrer VPC befinden würden. Sie müssen kein Internet-Gateway, kein NAT-Gerät, keine öffentliche IP-Adresse, keine AWS Direct Connect-Verbindung oder eine AWS Site-to-Site-VPN-Verbindung verwenden, um von Ihren privaten Subnetzen aus mit dem Dienst zu kommunizieren. Weitere Informationen zu AWS PrivateLink oder zur Einrichtung finden Sie unter Was ist AWS PrivateLink? AWS PrivateLink

Sie können Bitcoin-JSON-RPC-Anfragen über AWS PrivateLink einen VPC-Endpunkt an AMB Access Bitcoin senden. Anfragen an diesen privaten Endpunkt werden nicht über das offene Internet weitergeleitet, sodass Sie Anfragen mit derselben SigV4-Authentifizierung direkt an die Bitcoin-Endpunkte senden können. Weitere Informationen finden Sie unter Zugriff auf AWS Dienste über. AWS PrivateLink

Suchen Sie nach dem Servicenamen in der Spalte AWS Service nach Amazon Managed Blockchain. Weitere Informationen finden Sie unter AWS Dienste, die sich in integrieren lassen AWS PrivateLink. Der Dienstname für den Endpunkt wird das folgende Format haben:`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

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

Bitcoin-Anwendungsfälle mit Amazon Managed Blockchain (AMB) Access Bitcoin

Dieses Thema enthält eine Liste der Anwendungsfälle von AMB Access Bitcoin

Themen

Erstellen Sie eine Bitcoin (BTC) -Brieftasche zum Senden und Empfangen von BTC

BTC, die native Kryptowährung im Bitcoin-Netzwerk, ist ein wesentlicher Bestandteil des Sicherheitsmodells des Netzwerks. Es fungiert auch als Ware und Austauschmedium und wird häufig von Institutionen, Unternehmen und Einzelpersonen genutzt. Folglich verlassen sich viele Wallet-Anwendungen auf Bitcoin-Knoten, um mit der Bitcoin-Blockchain zu interagieren. Diese Anwendungen berechnen den Saldo der nicht ausgegebenen Ausgaben (UTXOs) für einen bestimmten Satz von Adressen, signieren und senden Transaktionen an das Bitcoin-Netzwerk und rufen Daten über historische Transaktionen ab.

Im Folgenden finden Sie ein Beispiel für einige Bitcoin-JSON-DateienRPCs , die Amazon Managed Blockchain (AMB) Access Bitcoin für BTC-Wallet-Transaktionen unterstützt:

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

Weitere Informationen finden Sie unter Unterstütztes JSON- RPCs.

Analysieren Sie die Aktivitäten auf der Bitcoin-Blockchain

Sie können das Volumen der Transaktionsaktivitäten in der Bitcoin-Blockchain mithilfe der `getchaintxstats` JSON-RPC-Methode analysieren. Mit diesem JSON-RPC können Sie auf Kennzahlen wie durchschnittliche Transaktionsraten pro Sekunde, Gesamtzahl der Transaktionen, Blockanzahl und mehr zugreifen. Sie können bei Bedarf auch ein Fenster mit Blocknummern oder einen Block-Hash als Trennzeichen definieren, um diese Statistiken für eine bestimmte Gruppe von Blöcken im Netzwerk zu berechnen.

Weitere Informationen finden Sie unter Unterstütztes JSON- RPCs.

Verifizieren Sie Nachrichten, die mit einem Bitcoin-Schlüsselpaar signiert wurden

Bitcoin-Wallets haben einen privaten Schlüssel und einen öffentlichen Schlüssel, die ein key pair bilden. Diese Schlüssel werden verwendet, um Transaktionen zu signieren und dienen als Identität des Benutzers in der Blockchain. Der öffentliche Schlüssel wird verwendet, um Adressen zu erstellen. Dabei handelt es sich um standardisierte alphanumerische Identifikatoren (27 bis 34 Zeichen lang). Diese Adressen werden verwendet, um BTC-Ausgaben zu empfangen und Transaktionen oder Nachrichten abzuwickeln.

Mit einer Bitcoin-Brieftasche können Benutzer Nachrichten auch kryptografisch signieren und verifizieren. Dieser Prozess wird häufig verwendet, um den Besitz einer bestimmten Wallet-Adresse und der damit verbundenen BTC nachzuweisen. Mithilfe des `verifymessage` Bitcoin JSON-RPC können Sie die Echtheit und Gültigkeit einer von einer anderen Wallet signierten Nachricht überprüfen. Insbesondere kann ein Bitcoin-Knoten verwendet werden, um zu überprüfen, ob eine Nachricht mit dem privaten Schlüssel signiert wurde, der der angegebenen abgeleiteten Adresse aus dem öffentlichen Schlüssel in der signierten Nachricht selbst entspricht.

Weitere Informationen finden Sie unter Unterstütztes JSON- RPCs.

Untersuchen Sie den Bitcoin-Mempool

Viele Anwendungen müssen auf den Mempool zugreifen, um den Überblick über ausstehende Transaktionen zu behalten, eine Liste aller ausstehenden Transaktionen abzurufen oder herauszufinden, woher eine Transaktion stammt. Zu diesem Zweck gibt es RPCs Bitcoin-JSON-ähnliche `getmempoolancestorsgetmempoolentry`, und `getrawmempool` die diese Aktivität

unterstützen. Diese Bitcoin-JSON-Anwendungen RPCs helfen dabei, die benötigten Informationen aus dem Mempool zu erhalten.

Amazon Managed Blockchain (AMB) Access Bitcoin unterstützt auch `testmempoolaccept` Bitcoin JSON-RPCs, mit dem Sie vor dem Absenden überprüfen können, ob eine Transaktion den Protokollregeln entspricht und von einem Knoten akzeptiert würde. Wallets, Börsen und alle anderen Entitäten, die Transaktionen direkt an die Bitcoin-Blockchain übermitteln, verwenden diese Bitcoin-JSON-Daten. RPCs

Weitere Informationen finden Sie unter Unterstütztes JSON- RPCs.

Unterstütztes Bitcoin-JSON — RPCs mit Amazon Managed Blockchain (AMB) auf Bitcoin zugreifen

Dieses Thema enthält eine Liste der Bitcoin-JSON-Dateien, die von Managed Blockchain unterstützt werden, und Verweise RPCs darauf. Zu jedem unterstützten JSON-RPC gibt es eine kurze Beschreibung seiner Verwendung.

Note

- Sie können Bitcoin JSON- RPCs auf Managed Blockchain authentifizieren, indem Sie den Signaturprozess Signature Version 4 (Sigv4) verwenden. Das bedeutet, dass nur autorisierte IAM-Prinzipale im AWS Konto mithilfe des Bitcoin-JSON-Codes mit dem Konto interagieren können. RPCs Geben Sie AWS beim Anruf Anmeldeinformationen (eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel) an.
- Wenn Ihre HTTP-Antwort größer als 10 MB ist, erhalten Sie eine Fehlermeldung. Um dies zu korrigieren, müssen Sie die Komprimierungsheader auf `Accept-Encoding:gzip` setzen. Die komprimierte Antwort, die Ihr Client dann erhält, enthält die folgenden Header: `Content-Type: application/json` und. `Content-Encoding: gzip`
- Amazon Managed Blockchain (AMB) Access Bitcoin generiert einen 400-Fehler für falsch formatierte JSON-RPC-Anfragen.
- Verwenden Sie den `sendrawtransaction` JSON-RPC, um Transaktionen einzureichen, die den Status der Bitcoin-Blockchain aktualisieren.
- AMB Access Bitcoin hat ein Standard-Anforderungslimit von 100 Anfragen pro Sekunde (RPS) pro Region. `NETWORK_TYPE` AWS

  Um Ihr Kontingent zu erhöhen, müssen Sie sich an den Support wenden AWS . Um den AWS Support zu kontaktieren, melden Sie sich AWS bei der Support Center-Konsole an. Wählen Sie Create case (Fall erstellen) aus. Wählen Sie Technisch. Wählen Sie Managed Blockchain als Ihren Service. Wählen Sie Access:Bitcoin als Kategorie und General Guidance als Schweregrad. Geben Sie RPC Quota als Betreff und in das Textfeld Beschreibung ein und listen Sie die für Ihre Bedürfnisse geltenden Kontingentlimits in RPS pro Bitcoin-Netzwerk pro Region auf. Reichen Sie Ihren Fall ein.

Unterstütztes JSON- RPCs

AMB Access Bitcoin unterstützt die folgenden Bitcoin-JSON-. RPCs Jeder unterstützte Anruf enthält eine kurze Beschreibung seiner Verwendung.

Kategorie	JSON-RPC	Beschreibung
Blockkette RPCs	Holen Sie sich den besten Block-Hash	Gibt den Hash des besten (Tipp-) Blocks in der am meisten funktionierenden, vollständig validierten Kette zurück.
	getblock	Wenn die Ausführlichkeit 0 ist, wird eine Zeichenfolge zurückgegeben, bei der es sich um serialisierte, hexadezimale Daten für den Block 'Hash' handelt. Wenn die Ausführli chkeit 1 ist, wird ein Objekt mit Informationen über den Block „Hash“ zurückgegeben. Wenn die Ausführlichkeit 2 ist, wird ein Objekt mit Informationen über den Block „Hash“ und Informationen zu jeder Transaktion zurückgeg eben. Wenn die Ausführlichkeit den Wert 3 hat, wird ein Objekt mit Informationen über den Block-Hash und Informationen zu jeder Transaktion zurückgegeben, einschließlich der `prevout` Informationen für Eingaben.
	getblockchaininfo	Gibt ein Objekt zurück, das verschiedene Statusinformationen zur Blockchain-Verarbe itung enthält.
	getblockcount	Gibt die Höhe der Kette zurück, die am meisten gearbeitet und vollständig validiert wurde. Der Genesis-Block hat die Höhe 0.
	getblockfilter	Ruft mithilfe des Block-Hashes einen BIP 157-Inhaltsfilter für einen bestimmten Block ab.

Kategorie	JSON-RPC	Beschreibung
	getblockhash	Gibt den Hash des Blocks in der angegebenen best-block-chain Höhe zurück.
	getblockheader	Wenn verbose den Wert false hat, wird eine Zeichenfolge zurückgegeben, die aus serialisierten, hexadezimalen Daten für den Blockheader 'hash' besteht. Wenn verbose den Wert true hat, wird ein Objekt mit Informationen über den Blockheader 'Hash' zurückgegeben.
	getblockstats	Berechnet Statistiken pro Block für ein bestimmtes Fenster. Alle Beträge sind in Satoshis angegeben. In einigen Höhen funktioniert es beim Beschneiden nicht.
	Hol dir Kettenspitzen	Gibt Informationen über alle bekannten Tipps im Blockbaum zurück, einschließlich der Hauptkette und verwaister Zweige.
	getchaintxstats	Berechnet Statistiken über die Gesamtzahl und Rate der Transaktionen in der Kette.
	Schwierigkeiten bekommen	Gibt die proof-of-work Schwierigkeit als Vielfaches der Mindestschwierigkeit zurück.
	getmempoolancestors	Wenn sich txid im Mempool befindet, werden alle Vorfahren im Mempool zurückgegeben.
	Ermittelt die Nachkommen von Mempool	Wenn txid im Mempool enthalten ist, werden alle von Mempool abgeleiteten Objekte zurückgegeben.
	getmempool-Eintrag	Gibt Mempool-Daten für die angegebene Transaktion zurück.
	getmempoolinfo	Gibt Details zum aktiven Status des TX-Speicherpools zurück.

Kategorie	JSON-RPC	Beschreibung
	getrawmempool	Gibt alle Transaktionen IDs im Speicherpool als JSON-Array mit String-Transaktionen zurück. IDs **Note** `verbose = true` wird nicht unterstützt.
	gettxout	Gibt Details zu einer noch nicht ausgegebenen Transaktionsausgabe zurück.
	gettxoutproof	Gibt einen hexadezimalen Nachweis zurück, dass „txid“ in einem Block enthalten war.
Rohtransaktionen RPCs	Rohtransaktion erstellen	Erstellt eine Transaktion, die die angegebenen Eingaben ausgibt und neue Ausgaben erzeugt.
	dekodiert eine Rohtransaktion	Gibt ein JSON-Objekt zurück, das die serialisierte, hex-kodierte Transaktion darstellt.
	dekodeskriptiv	Dekodiert ein hexadezimales Skript.
	getraw-Transaktion	Gibt die unformatierten Transaktionsdaten zurück.
	sendet eine Transaktion	Sendet eine Rohtransaktion (serialisiert, hex-kodiert) an den lokalen Knoten und das Netzwerk.
	testmempoolaccept	Gibt das Ergebnis von Mempool-Akzeptanztests zurück, die angeben, ob die Rohtransaktion (serialisiert, hex-codiert) von Mempool akzeptiert würde. Dadurch wird geprüft, ob die Transaktion gegen die Konsens- oder Richtlinienregeln verstößt.

Kategorie	JSON-RPC	Beschreibung
Bis RPCs	Multisig erstellen	Erstellt eine Adresse mit mehreren Signature n, für die keine Signatur meiner Schlüssel erforderlich ist.
	geschätzte Smartfee	Schätzt die ungefähre Gebühr pro Kilobyte, die erforderlich ist, damit eine Transaktion mit der Bestätigung innerhalb von conf_target-Blöcken beginnt, sofern möglich, und gibt die Anzahl der Blöcke zurück, für die die Schätzung gültig ist. Verwendet die virtuelle Transaktionsgröße, wie in BIP 141 definiert (Zeugendaten werden nicht berücksichtigt).
	Adresse validieren	Gibt Informationen über die angegebene Bitcoin-Adresse zurück.
	Nachricht verifizieren	Überprüft eine signierte Nachricht.

Sicherheit im Amazon Managed Blockchain (AMB) Access Bitcoin

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die so konzipiert sind, dass sie die Anforderungen der sicherheitssensibelsten Unternehmen erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der gemeinsamen Verantwortung beschreibt dies sowohl als Sicherheit in der Cloud als auch als Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon Managed Blockchain (AMB) Access Bitcoin gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Um Datenschutz, Authentifizierung und Zugriffskontrolle zu gewährleisten, verwendet Amazon Managed Blockchain AWS Funktionen und Funktionen des Open-Source-Frameworks, das in Managed Blockchain ausgeführt wird.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von AMB Access Bitcoin anwenden können. Die folgenden Themen zeigen Ihnen, wie Sie AMB Access Bitcoin konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer AMB Access Bitcoin-Ressourcen helfen.

Topics

Datenschutz in Amazon Managed Blockchain (AMB) Access Bitcoin

Das AWS Modell der mit gilt für den Datenschutz in Amazon Managed Blockchain (AMB) Access Bitcoin. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der AWS Cloud alle Systeme laufen. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AMB Access Bitcoin oder anderen Geräten AWS-Services über die Konsole, API oder arbeiten. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL

für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

Datenverschlüsselung verhindert, dass unbefugte Benutzer Daten aus einem Blockchain-Netzwerk und den zugehörigen Datenspeichersystemen lesen. Dazu gehören Daten, die bei der Übertragung durch das Netzwerk möglicherweise abgefangen werden, sogenannte Daten bei der Übertragung.

Verschlüsselung während der Übertragung

Standardmäßig verwendet Managed Blockchain eine HTTPS/TLS-Verbindung, um alle Daten zu verschlüsseln, die von einem Client-Computer übertragen werden, auf dem die beiden Dienstendpunkte ausgeführt werden. AWS CLI AWS

Sie müssen nichts tun, um die Verwendung von HTTPS/TLS zu aktivieren. Sie ist immer aktiviert, es sei denn, Sie deaktivieren sie explizit für einen einzelnen AWS CLI Befehl, indem Sie den Befehl verwenden. `--no-verify-ssl`

Identitäts- und Zugriffsmanagement für Amazon Managed Blockchain (AMB) Access Bitcoin

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AMB Access Bitcoin-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Amazon Managed Blockchain (AMB) Access Bitcoin-Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Amazon Managed Blockchain (AMB) Access Bitcoin mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Amazon Managed Blockchain (AMB) Access Bitcoin mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AMB Access Bitcoin zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit AMB Access Bitcoin verfügbar sind.

IAM-Funktionen, die Sie mit Amazon Managed Blockchain (AMB) Access Bitcoin verwenden können

IAM-Feature	AMB Access Bitcoin-Unterstützung
Identitätsbasierte Richtlinien	Ja

IAM-Feature	AMB Access Bitcoin-Unterstützung
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Nein
Hauptberechtigungen	Nein
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AMB Access Bitcoin und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AMB Access Bitcoin

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie

in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AMB Access Bitcoin

Beispiele für identitätsbasierte Richtlinien von AMB Access Bitcoin finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

Ressourcenbasierte Richtlinien innerhalb von AMB Access Bitcoin

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AMB Access Bitcoin

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AMB Access Bitcoin-Aktionen finden Sie unter Von Amazon Managed Blockchain (AMB) Access Bitcoin definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in AMB Access Bitcoin verwenden vor der Aktion das folgende Präfix:

```
managedblockchain:
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `InvokeRpcBitcoin` beginnen, einschließlich der folgenden Aktion:

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

Beispiele für identitätsbasierte Richtlinien von AMB Access Bitcoin finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

Richtlinienressourcen für AMB Access Bitcoin

Unterstützt Richtlinienressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AMB Access Bitcoin-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon Managed Blockchain (AMB) Access Bitcoin definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource

angeben können, finden Sie unter Von Amazon Managed Blockchain (AMB) Access Bitcoin definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AMB Access Bitcoin finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

Schlüssel zur Richtlinienbedingung für AMB Access Bitcoin

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AMB Access Bitcoin-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Managed Blockchain (AMB) Access Bitcoin in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Managed Blockchain (AMB) Access Bitcoin definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AMB Access Bitcoin finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

ACLs in AMB Access Bitcoin

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AMB Access Bitcoin

Unterstützt ABAC (Tags in Richtlinien): Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, um Operationen zu ermöglichen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AMB Access Bitcoin

Unterstützt temporäre Anmeldeinformationen: Nein

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für AMB Access Bitcoin

Unterstützt Forward Access Sessions (FAS): Nein

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AMB Access Bitcoin

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern

und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> ⚠ Warning
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von AMB Access Bitcoin beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AMB Access Bitcoin Sie dazu anleitet.

Dienstbezogene Rollen für AMB Access Bitcoin

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon Managed Blockchain (AMB) Access Bitcoin

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AMB Access Bitcoin-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AMB Access Bitcoin definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Blockchain (AMB) Access Bitcoin in der Service Authorization Reference.

Themen

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AMB Access Bitcoin-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden Sie die AMB Access Bitcoin-Konsole

Um auf die Bitcoin-Konsole Amazon Managed Blockchain (AMB) Access zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, die AMB Access Bitcoin-Ressourcen in Ihrem aufzulisten und einzusehen. AWS-Konto Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AMB Access Bitcoin-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AMB Access Bitcoin `ConsoleAccess` - oder `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

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

Zugriff auf Bitcoin-Netzwerke

> **Note**
>
> Um auf die öffentlichen Endpunkte für den Bitcoin zuzugreifen `mainnet` und JSON-RPC-Aufrufe `testnet` zu tätigen, benötigen Sie Benutzeranmeldedaten

(`AWS_ACCESS_KEY_IDundAWS_SECRET_ACCESS_KEY`), die über die entsprechenden IAM-Berechtigungen für AMB Access Bitcoin verfügen.

Example IAM-Richtlinie für den Zugriff auf alle Bitcoin-Netzwerke

Dieses Beispiel gewährt einem IAM-Benutzer AWS-Konto Zugriff auf alle Bitcoin-Netzwerke.

JSON

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

Example IAM-Richtlinie für den Zugriff auf das Bitcoin Testnet-Netzwerk

Dieses Beispiel gewährt einem IAM-Benutzer AWS-Konto Zugriff auf das Bitcoin-Netzwerk. `testnet`

JSON

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

```
        }
    ]
}
```

Fehlerbehebung bei Amazon Managed Blockchain (AMB) Access Bitcoin-Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AMB Access Bitcoin und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in AMB Access Bitcoin durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AMB Access Bitcoin-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in AMB Access Bitcoin durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `managedblockchain::`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `managedblockchain::`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AMB Access Bitcoin übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AMB Access Bitcoin auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AMB Access Bitcoin-Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AMB Access Bitcoin diese Funktionen unterstützt, finden Sie unter. So funktioniert Amazon Managed Blockchain (AMB) Access Bitcoin mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Protokollierung von Bitcoin-Ereignissen mit Amazon Managed Blockchain (AMB) Access mithilfe von AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin unterstützt keine Verwaltungsereignisse.

Amazon Managed Blockchain ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Managed Blockchain bereitstellt. CloudTrail erfasst, wer die AMB Access Bitcoin-Endpunkte für Managed Blockchain als Ereignisse auf der Datenebene aufgerufen hat.

Wenn Sie einen ordnungsgemäß konfigurierten Trail erstellen, der für den Empfang der gewünschten Ereignisse auf der Datenebene abonniert ist, können Sie fortlaufend CloudTrail Ereignisse im Zusammenhang mit AMB Access Bitcoin an einen Amazon S3-Bucket senden lassen. Anhand der von gesammelten Informationen können Sie feststellen CloudTrail, ob eine Anfrage an einen der AMB Access Bitcoin-Endpunkte gestellt wurde, von welcher IP-Adresse die Anfrage kam, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere zusätzliche Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

AMB Access Bitcoin-Informationen finden Sie unter CloudTrail

AWS CloudTrail ist standardmäßig aktiviert, wenn Sie Ihre AWS-Konto erstellen. Um jedoch zu sehen, wer die AMB Access Bitcoin-Endpunkte aufgerufen hat, müssen Sie die Konfiguration so konfigurieren, dass Ereignisse auf der CloudTrail Datenebene protokolliert werden.

Um die Ereignisse in Ihrem System fortlaufend aufzuzeichnen AWS-Konto, einschließlich der Ereignisse auf der Datenebene für AMB Access Bitcoin, müssen Sie einen Trail erstellen. Ein Trail ermöglicht die CloudTrail Übertragung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der erstellen AWS-Managementkonsole, gilt der Trail standardmäßig für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen unterstützten Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber

hinaus können Sie andere AWS Dienste konfigurieren, um diese Daten weiter zu analysieren und auf die in den CloudTrail Protokollen gesammelten Ereignisdaten zu reagieren. Weitere Informationen finden Sie hier:

- Wird verwendet CloudTrail , um Bitcoin JSON zu verfolgen- RPCs
- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Durch die Analyse der CloudTrail Datenereignisse können Sie überwachen, wer die AMB Access Bitcoin-Endpunkte aufgerufen hat.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer ausgeführt wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in der Bitcoin-Protokolldatei von AMB Access

Bei Ereignissen auf der Datenebene ist ein Trail eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen bestimmten S3-Bucket ermöglicht. Jede CloudTrail Protokolldatei enthält einen oder mehrere Protokolleinträge, die eine einzelne Anfrage aus einer beliebigen Quelle darstellen. Diese Einträge enthalten Details zur angeforderten Aktion, einschließlich Datum und Uhrzeit der Aktion sowie aller zugehörigen Anforderungsparameter.

> **Note**
>
> CloudTrail Datenereignisse in den Protokolldateien sind kein geordneter Stack-Trace der Bitcoin-API-Aufrufe von AMB Access, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Wird verwendet CloudTrail , um Bitcoin JSON zu verfolgen- RPCs

Sie können CloudTrail damit verfolgen, wer in Ihrem Konto die AMB Access Bitcoin-Endpunkte aufgerufen hat und welcher JSON-RPC als Datenereignisse aufgerufen wurde. Wenn Sie einen Trail erstellen, werden Datenereignisse standardmäßig nicht protokolliert. Um aufzuzeichnen, wer die AMB Access Bitcoin-Endpunkte als CloudTrail Datenereignisse aufgerufen hat, müssen Sie die unterstützten Ressourcen oder Ressourcentypen, für die Sie Aktivitäten sammeln möchten, explizit zu einem Trail hinzufügen. Amazon Managed Blockchain unterstützt das Hinzufügen von Datenereignissen mithilfe des AWS SDK AWS-Managementkonsole, und AWS CLI. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mithilfe erweiterter Selektoren protokollieren.

Um Datenereignisse in einem Trail zu protokollieren, verwenden Sie den put-event-selectorsVorgang, nachdem Sie den Trail erstellt haben. Verwenden Sie die `--advanced-event-selectors` Option, um die `AWS::ManagedBlockchain::Network` Ressourcentypen anzugeben, um mit der Protokollierung von Datenereignissen zu beginnen und festzustellen, wer die AMB Access Bitcoin-Endpunkte aufgerufen hat.

Example Eintrag aller AMB Access-Bitcoin-Endpunktanfragen Ihres Kontos im Datenereignisprotokoll

Das folgende Beispiel zeigt, wie Sie mit diesem `put-event-selectors` Vorgang alle AMB Access-Bitcoin-Endpunktanfragen Ihres Kontos für den Trail `my-bitcoin-trail` in der Region protokollieren können. `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"] } ]}]'
```

Nachdem Sie das Abonnement abgeschlossen haben, können Sie die Nutzung in dem S3-Bucket verfolgen, der mit dem im vorherigen Beispiel angegebenen Trail verbunden ist.

Das folgende Ergebnis zeigt einen Eintrag im CloudTrail Datenereignisprotokoll der Informationen, die von gesammelt wurden CloudTrail. Sie können feststellen, dass eine Bitcoin-JSON-RPC-Anfrage an einen der AMB Access Bitcoin-Endpunkte gestellt wurde, die IP-Adresse, von der die Anfrage kam, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere zusätzliche Informationen.


```
{
        "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"
}
```

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.