aws

Guida per gli sviluppatori

Accesso AMB a Bitcoin

Accesso AMB a Bitcoin: Guida per gli sviluppatori

Table of Contents

Cos'è Amazon Managed Blockchain (AMB) Access Bitcoin? 1
Sei un utente AMB Access Bitcoin per la prima volta? 1
Concetti chiave 3
Considerazioni e limitazioni 3
Configurazione 6
Prerequisiti e considerazioni 6
Iscriviti per AWS 6
Crea un utente IAM con le autorizzazioni appropriate 7
Installa e configura il AWS Command Line Interface 7
Nozioni di base 8
Creazione di una policy IAM 8
Esempio di RPC per console 9
esempio RPC awscurl 10
Esempio di RPC per Node.js 11
AMB Access Bitcoin su PrivateLink 15
Casi d'uso di Bitcoin 16
Crea un portafoglio Bitcoin (BTC) per inviare e ricevere BTC 16
Analizza l'attività sulla blockchain di Bitcoin 16
Verifica i messaggi firmati utilizzando una coppia di chiavi Bitcoin 17
Ispeziona il mempool di Bitcoin 17
Bitcoin JSON- RPCs 18
JSON supportato RPCs 19
Sicurezza 23
Protezione dei dati 24
Crittografia dei dati 25
Crittografia in transito 25
Gestione dell’identità e degli accessi 25
Destinatari 26
Autenticazione con identità 26
Gestione dell’accesso tramite policy 27
Come funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM 29
Esempi di policy basate su identità 35
Risoluzione dei problemi 39
CloudTrail registri 42

AMB Accedi alle informazioni su Bitcoin in CloudTrail 42
Comprensione delle voci dei file di registro di AMB Access Bitcoin 43
Utilizzo CloudTrail per tracciare Bitcoin JSON- RPCs 44
..... xlvi

Cos'è Amazon Managed Blockchain (AMB) Access Bitcoin?

Amazon Managed Blockchain (AMB) Access ti fornisce nodi blockchain pubblici per Ethereum e Bitcoin e puoi anche creare reti blockchain private con il framework Hyperledger Fabric. Scegli tra vari metodi per interagire con le blockchain pubbliche, tra cui operazioni API multi-tenant completamente gestite, single-tenant (dedicate) e multi-tenant senza server su nodi blockchain pubblici. Per i casi d'uso in cui i controlli degli accessi sono importanti, puoi scegliere tra reti blockchain private completamente gestite. Le operazioni API standardizzate offrono una scalabilità istantanea su un'infrastruttura resiliente e completamente gestita, in modo da poter creare applicazioni blockchain.

AMB Access offre due tipi distinti di servizi di infrastruttura blockchain: operazioni API di accesso alla rete blockchain multi-tenant e nodi e reti blockchain dedicati. Con un'infrastruttura blockchain dedicata, puoi creare e utilizzare nodi blockchain Ethereum pubblici e reti blockchain private Hyperledger Fabric per uso personale. Le offerte multi-tenant e basate su API, tuttavia, come AMB Access Bitcoin, sono composte da una flotta di nodi Bitcoin protetti da un livello API in cui l'infrastruttura sottostante dei nodi blockchain è condivisa tra i clienti.

Bitcoin è una rete blockchain decentralizzata che consente peer-to-peer transazioni sicure di valore denominate nella criptovaluta nativa della rete, Bitcoin (BTC). La rete Bitcoin è utilizzata da privati, istituzioni finanziarie, società fintech, governi e altro ancora. La rete Bitcoin è un mezzo di scambio, una materia prima per gli investimenti o un registro pubblicamente verificabile e immutabile per i dati registrati. Con Amazon Managed Blockchain (AMB) Access Bitcoin, puoi accedere a un pool di reti Bitcoin Mainnet e Testnet tramite endpoint regionali, attraverso i quali puoi scrivere transazioni, leggere dati dal registro e richiamare richieste JSON-RPC disponibili sul client Bitcoin Core node. Con gli endpoint Bitcoin serverless, puoi concentrarti sulla creazione delle tue applicazioni invece di investire in attività indifferenziate come il provisioning, la manutenzione e il bilanciamento del carico dei nodi Bitcoin. Che tu stia creando un portafoglio Bitcoin, creando uno scambio di criptovalute o analizzando i dati della blockchain di Bitcoin, paghi solo per le richieste che effettui tramite gli endpoint Bitcoin utilizzando AMB Access Bitcoin.

Sei un utente AMB Access Bitcoin per la prima volta?

Se sei un utente principiante di AMB Access Bitcoin, ti consigliamo di iniziare leggendo le seguenti sezioni:

- Concetti chiave: Amazon Managed Blockchain (AMB) Access Bitcoin
- Guida introduttiva ad Amazon Managed Blockchain (AMB) Access Bitcoin

- Casi d'uso di Bitcoin con Amazon Managed Blockchain (AMB) Access Bitcoin
- Bitcoin JSON supportato: RPCs con Amazon Managed Blockchain (AMB) Access Bitcoin

Concetti chiave: Amazon Managed Blockchain (AMB) Access Bitcoin

> **Note**
>
> Questa guida presuppone che tu abbia familiarità con i concetti essenziali di Bitcoin. Questi concetti includono decentralizzazione, nodi, transazioni, portafogli proof-of-work, chiavi pubbliche e private, halving e altri. Prima di utilizzare Amazon Managed Blockchain (AMB) Access Bitcoin, ti consigliamo di consultare la documentazione sullo sviluppo di Bitcoin e la masterizzazione di Bitcoin.

Amazon Managed Blockchain (AMB) Access Bitcoin ti offre un accesso senza server alla blockchain di Bitcoin, senza richiedere il provisioning e la gestione di alcuna infrastruttura Bitcoin, inclusi i nodi. Puoi utilizzare questo servizio gestito per accedere alle reti Bitcoin in modo rapido e su richiesta, riducendo il costo complessivo di proprietà.

AMB Access Bitcoin ti fornisce l'accesso alla rete Bitcoin tramite nodi completi che eseguono il client Bitcoin Core, con la funzionalità del portafoglio disabilitata e il supporto di diverse chiamate JSON Remote Procedure (JSON-RPC). Puoi invocare Bitcoin JSON RPCs per comunicare con i nodi Bitcoin gestiti da Managed Blockchain per interagire con le reti Bitcoin. Con Bitcoin JSON-RPCs, puoi leggere dati e scrivere transazioni, inclusa l'interrogazione di dati e l'invio di transazioni alle reti Bitcoin utilizzando il servizio Amazon Managed Blockchain.

> **Important**
>
> Sei responsabile della creazione, del mantenimento, dell'utilizzo e della gestione dei tuoi indirizzi Bitcoin. Sei anche responsabile del contenuto dei tuoi indirizzi Bitcoin. AWS non è responsabile per le transazioni distribuite o richiamate utilizzando nodi Bitcoin su Amazon Managed Blockchain.

Considerazioni e limitazioni per l'utilizzo di Amazon Managed Blockchain (AMB) Access Bitcoin

- Reti Bitcoin supportate

AMB Access Bitcoin supporta le seguenti reti pubbliche:

- Mainnet: la blockchain pubblica di Bitcoin protetta dal proof-of-work consenso e sulla quale viene emessa e negoziata la criptovaluta Bitcoin (BTC). Le transazioni su Mainnet hanno un valore effettivo (ovvero comportano costi reali) e vengono registrate sulla blockchain pubblica.
- Testnet: la testnet è una blockchain Bitcoin alternativa utilizzata per i test. Le monete Testnet sono separate e distinte dal vero Bitcoin (BTC) e di solito non hanno alcun valore.

> **Note**
>
> Le reti private non sono supportate.

- Regioni supportate

  Le seguenti sono le regioni supportate per questo servizio:

Nome della Regione	Codice	Region
Stati Uniti orientali (Virginia settentrionale)	IAD	`us-east-1`
Asia Pacifico (Tokyo)	NRT	ap-northeast-1
Asia Pacifico (Seul)	ICN	ap-northeast-2
Asia Pacifico (Singapore)	SIN	ap-southeast-1
Europa (Irlanda)	DUB	eu-west-1
Europa (Londra)	LHR	eu-west-2

- Service endpoints (Endpoint del servizio)

  Di seguito sono riportati gli endpoint del servizio per AMB Access Bitcoin. Per connetterti al servizio, devi utilizzare un endpoint che includa una delle regioni supportate.

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

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

- Il mining non è supportato

AMB Access Bitcoin non supporta il mining di Bitcoin (BTC).

- Firma in versione 4 delle chiamate JSON-RPC di Bitcoin

  Quando effettui chiamate a Bitcoin JSON- RPCs su Amazon Managed Blockchain, puoi farlo tramite una connessione HTTPS autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono effettuare chiamate Bitcoin JSON-RPC. Per fare ciò, insieme alla chiamata devono essere AWS fornite delle credenziali (un ID della chiave di accesso e una chiave di accesso segreta).

  > **Important**
  >
  > - Non incorporate le credenziali del client nelle applicazioni rivolte agli utenti.
  > - Non puoi utilizzare le policy IAM per limitare l'accesso ai singoli Bitcoin JSON-. RPCs

- Sono supportati solo gli invii di transazioni non elaborate

  Usa `sendrawtransaction` JSON-RPC per inviare transazioni che aggiornano lo stato della blockchain di Bitcoin.

- AWS CloudTrail supporto per la registrazione

  Puoi configurare CloudTrail per registrare il tuo Bitcoin JSON-. RPCs Per ulteriori informazioni, consulta Registrazione degli eventi di Amazon Managed Blockchain (AMB) Access Bitcoin utilizzando AWS CloudTrail

Configurazione di Amazon Managed Blockchain (AMB) Access Bitcoin

Prima di utilizzare Amazon Managed Blockchain (AMB) Access Bitcoin per la prima volta, segui i passaggi in questa sezione per creare un AWS account. Il capitolo seguente illustra come iniziare a utilizzare AMB Access Bitcoin.

Prerequisiti e considerazioni

Prima di utilizzarlo AWS per la prima volta, è necessario disporre di un. Account AWS

Iscriviti per AWS

Quando ti iscrivi AWS, il tuo Account AWS viene automaticamente registrato per tutti Servizi AWS, incluso Amazon Managed Blockchain (AMB) Access Bitcoin. Ti vengono addebitati solo i servizi che utilizzi.

Se ne hai Account AWS già uno, vai al passaggio successivo. Se non disponi di un Account AWS, utilizza la seguente procedura per crearne uno.

Per creare un AWS account

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Crea un utente IAM con le autorizzazioni appropriate

Per creare e lavorare con AMB Access Bitcoin, devi disporre di un principale AWS Identity and Access Management (IAM) (utente o gruppo) con autorizzazioni che consentano le necessarie azioni gestite sulla blockchain.

Solo i principali IAM possono effettuare chiamate Bitcoin JSON-RPC. Quando effettui chiamate a Bitcoin JSON- RPCs su Amazon Managed Blockchain, puoi farlo tramite una connessione HTTPS autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono effettuare chiamate Bitcoin JSON-RPC. Per fare ciò, insieme alla chiamata devono essere AWS fornite delle credenziali (un ID della chiave di accesso e una chiave di accesso segreta).

Per informazioni su come creare un utente IAM, consulta Creazione di un utente IAM nel tuo AWS account. Per ulteriori informazioni su come allegare una politica di autorizzazioni a un utente, consulta Modifica delle autorizzazioni per un utente IAM. Per un esempio di politica di autorizzazioni che puoi utilizzare per concedere a un utente il permesso di lavorare con AMB Access Bitcoin, vedi. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

Installa e configura il AWS Command Line Interface

Se non l'hai già fatto, installa l'ultima versione dell'interfaccia a AWS riga di comando (CLI) per utilizzare AWS le risorse di un terminale. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.

> **Note**
>
> Per l'accesso alla CLI, sono necessari un ID chiave di accesso e una chiave di accesso segreta. Utilizza credenziali temporanee al posto delle chiavi di accesso a lungo termine quando possibile. Le credenziali temporanee includono un ID della chiave di accesso, una chiave di accesso segreta e un token di sicurezza che ne indica la scadenza. Per ulteriori informazioni, consulta Using temporary credenziali with AWS resources nella IAM User Guide.

Guida introduttiva ad Amazon Managed Blockchain (AMB) Access Bitcoin

Usa step-by-step i tutorial in questa sezione per imparare a eseguire attività utilizzando Amazon Managed Blockchain (AMB) Access Bitcoin. Questi esempi richiedono il completamento di alcuni prerequisiti. Se non conosci AMB Access Bitcoin, consulta la sezione Configurazione di questa guida per assicurarti di aver completato i prerequisiti. Per ulteriori informazioni, consulta Configurazione di Amazon Managed Blockchain (AMB) Access Bitcoin.

Argomenti

- Crea una policy IAM per accedere a Bitcoin JSON- RPCs
- Effettua richieste di chiamata di procedura remota (RPC) Bitcoin sull'editor RPC di AMB Access utilizzando il Console di gestione AWS
- Effettua richieste AMB Access Bitcoin JSON-RPC in awscurl utilizzando il AWS CLI
- Effettua richieste Bitcoin JSON-RPC in Node.js
- Usa AMB Access Bitcoin su AWS PrivateLink

Crea una policy IAM per accedere a Bitcoin JSON- RPCs

Per accedere agli endpoint pubblici di Bitcoin Mainnet e Testnet per effettuare chiamate JSON-RPC, devi disporre delle credenziali utente (AWS_ACCESS_KEY_ID e AWS_SECRET _ACCESS_KEY) con le autorizzazioni IAM appropriate per Amazon Managed Blockchain (AMB) Access Bitcoin. In un terminale su cui è AWS CLI installato, esegui il seguente comando per creare una policy IAM per accedere a entrambi gli endpoint 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**
>
> L'esempio precedente ti dà accesso sia a Bitcoin Mainnet che a Testnet. Per accedere a un endpoint specifico, usa il seguente comando: `Action`
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

Dopo aver creato la policy, associala al ruolo del tuo utente IAM affinché abbia effetto. Nella Console di gestione AWS, accedi al servizio IAM e collega la policy `AmazonManagedBlockchainBitcoinAccess` al ruolo assegnato al tuo utente IAM. Per ulteriori informazioni, consulta Creazione di un ruolo e assegnazione a un utente IAM.

Effettua richieste di chiamata di procedura remota (RPC) Bitcoin sull'editor RPC di AMB Access utilizzando il Console di gestione AWS

Puoi modificare e inviare chiamate di procedura remota (RPCs) Console di gestione AWS utilizzando AMB Access. Con questi RPCs, puoi leggere dati, scrivere e inviare transazioni sulla rete Bitcoin.

Example

L'esempio seguente mostra come ottenere informazioni su 00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 utilizzando *`blockhash`* RPC. `getBlock` Sostituisci le variabili evidenziate con i tuoi input o scegli uno degli altri metodi RPC elencati e inserisci gli input pertinenti richiesti.

1. Apri la console Managed Blockchain all'indirizzo. https://console.aws.amazon.com/managedblockchain/

2. Scegli l'editor RPC.
3. Nella sezione Richiesta, scegli *BITCOIN_MAINNET* come rete Blockchain.
4. Scegli *getblock* come metodo RPC.
5. Inserisci *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09* come numero di blocco e scegli *0* come verbosità.
6. Quindi, scegli Invia RPC.
7. Otterrai i risultati nella sezione Risposta di questa pagina. È quindi possibile copiare le transazioni non elaborate complete per ulteriori analisi o utilizzarle nella logica aziendale delle applicazioni.

Per ulteriori informazioni, consulta la pagina RPCs supportata da AMB Access Bitcoin

Effettua richieste AMB Access Bitcoin JSON-RPC in awscurl utilizzando il AWS CLI

Example

Firma le richieste con le tue credenziali utente IAM utilizzando Signature Version 4 (SigV4) per effettuare chiamate Bitcoin JSON-RPC agli endpoint Bitcoin di AMB Access. Lo strumento da riga di comando awscurl può aiutarti a firmare le richieste ai servizi che utilizzano SigV4. AWS Per ulteriori informazioni, vedere awscurl README.md.

Installa awscurl utilizzando il metodo appropriato al tuo sistema operativo. Su macOS, HomeBrew è l'applicazione consigliata:

```
brew install awscurl
```

Se hai già installato e configurato la AWS CLI, le credenziali utente IAM e la regione AWS predefinita sono impostate nel tuo ambiente e hanno accesso a awscurl. Utilizzando awscurl, invia una richiesta sia a Bitcoin Mainnet che a Testnet invocando l'RPC. `getblock` Questa chiamata accetta un parametro di stringa corrispondente all'hash del blocco per il quale si desidera recuperare le informazioni.

Il comando seguente recupera i dati dell'intestazione del blocco dalla rete principale di Bitcoin utilizzando l'hash del blocco nell'`params`array per selezionare il blocco specifico per il quale

recuperare le intestazioni. Questo esempio utilizza l'endpoint. `us-east-1` Puoi sostituirlo con il tuo Bitcoin JSON-RPC e la tua AWS regione preferiti supportati da Amazon Managed Blockchain (AMB) Access Bitcoin. Inoltre, puoi inviare una richiesta alla rete Testnet, anziché alla rete Mainnet, sostituendola con nel comando. `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
```

I risultati includono i dettagli delle intestazioni dei blocchi e un elenco di hash delle transazioni inclusi nel blocco richiesto. Fai riferimento al file di esempio seguente:

```
{"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"}
```

Effettua richieste Bitcoin JSON-RPC in Node.js

Puoi inviare richieste firmate utilizzando HTTPS per accedere agli endpoint Bitcoin Mainnet e Testnet e per effettuare chiamate API JSON-RPC utilizzando il modulo https nativo in Node.js, oppure puoi utilizzare una libreria di terze parti come AXIOS. L'esempio seguente mostra come effettuare una richiesta Bitcoin JSON-RPC agli endpoint Bitcoin di AMB Access.

Example

Per eseguire questo script Node.js di esempio, applica i seguenti prerequisiti:

1. È necessario che nel computer siano installati node version manager (nvm) e Node.js. Puoi trovare le istruzioni di installazione per il tuo sistema operativo qui.

2. Usa il `node --version` comando e conferma che stai usando la versione 14 o successiva di Node. Se necessario, è possibile utilizzare il `nvm install 14` comando, seguito dal `nvm use 14` comando, per installare la versione 14.
3. Le variabili `AWS_ACCESS_KEY_ID` di ambiente `AWS_SECRET_ACCESS_KEY` devono contenere le credenziali associate all'account. Le variabili di ambiente `AMB_HTTP_ENDPOINT` devono contenere gli endpoint Bitcoin AMB Access.

   Esporta queste variabili come stringhe sul tuo client utilizzando i seguenti comandi. Sostituisci i valori evidenziati nelle seguenti stringhe con i valori appropriati del tuo account utente IAM.

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

Dopo aver completato tutti i prerequisiti, copia il `package.json` file e `index.js` lo script seguenti nell'ambiente locale utilizzando l'editor:

pacchetto.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();
```

Il codice di esempio precedente utilizza Axios per effettuare richieste RPC all'endpoint Bitcoin e firma tali richieste con le intestazioni Signature Version 4 (SigV4) appropriate utilizzando gli strumenti SDK v3 ufficiali. AWS Per eseguire il codice, apri un terminale nella stessa directory dei file ed esegui quanto segue:

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

Il risultato generato sarà simile al seguente:

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
    confirmations":784126,"height":1000, "version":1,"versionHex":"00000001",
    "merkleroot":"fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33",
    "time":1232346882,
    "mediantime":1232344831,"nonce":2595206198,"bits":"1d00ffff","difficulty":1,
    "chainwork":"0000000000000000000000000000000000000000000000003e903e903e9",
    "nTx":1,

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

```
    "error":null,"id":"1001"}
```

> **Note**
>
> La richiesta di esempio nello script precedente effettua la `getblock` chiamata con lo stesso hash di blocco del parametro di input dell'Effettua richieste AMB Access Bitcoin JSON-RPC in awscurl utilizzando il AWS CLIesempio. Per effettuare altre chiamate, modifica l'`rpc`oggetto nello script con un Bitcoin JSON-RPC diverso. Puoi modificare l'opzione della proprietà host in Bitcoin per `testnet` effettuare chiamate su quell'endpoint.

Usa AMB Access Bitcoin su AWS PrivateLink

AWS PrivateLink è una tecnologia scalabile e altamente disponibile che puoi utilizzare per connettere il tuo VPC ai servizi in modo privato come se fossero nel tuo VPC. Non è necessario utilizzare un gateway Internet, un dispositivo NAT, un indirizzo IP pubblico, una connessione AWS Direct Connect o una connessione VPN da AWS sito a sito per comunicare con il servizio dalle sottoreti private. Per ulteriori informazioni AWS PrivateLink o per la configurazione, consulta Cos'è? AWS PrivateLinkAWS PrivateLink

Puoi inviare richieste Bitcoin JSON-RPC a AMB Access Bitcoin AWS PrivateLink tramite un endpoint VPC. Le richieste a questo endpoint privato non vengono trasmesse su Internet aperto, quindi puoi inviare le richieste direttamente agli endpoint Bitcoin utilizzando la stessa autenticazione SigV4. Per ulteriori informazioni, consulta Access services through. AWSAWS PrivateLink

Per il nome del servizio, cerca Amazon Managed Blockchain nella colonna del AWS servizio.
Per ulteriori informazioni, consulta AWS i servizi che si integrano con AWS PrivateLink.
Il nome del servizio per l'endpoint sarà nel seguente formato:`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

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

Casi d'uso di Bitcoin con Amazon Managed Blockchain (AMB) Access Bitcoin

Questo argomento fornisce un elenco dei casi d'uso di AMB Access Bitcoin

Argomenti

- Crea un portafoglio Bitcoin (BTC) per inviare e ricevere BTC
- Analizza l'attività sulla blockchain di Bitcoin
- Verifica i messaggi firmati utilizzando una coppia di chiavi Bitcoin
- Ispeziona il mempool di Bitcoin

Crea un portafoglio Bitcoin (BTC) per inviare e ricevere BTC

BTC, la criptovaluta nativa della rete Bitcoin, funge da componente essenziale del modello di sicurezza della rete. Funziona anche come merce e mezzo di scambio, ampiamente utilizzato da istituzioni, aziende e privati. Di conseguenza, molte applicazioni di portafoglio si affidano ai nodi Bitcoin per interagire con la blockchain Bitcoin. Queste applicazioni calcolano il saldo degli output non spesi (UTXOs) per un determinato insieme di indirizzi, firmano e inviano transazioni alla rete Bitcoin e recuperano i dati sulle transazioni storiche.

Di seguito è riportato un esempio di alcuni dei Bitcoin JSON supportati da Amazon Managed Blockchain (AMB) Access Bitcoin per le transazioni con portafogli BTC: RPCs

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

Per ulteriori informazioni, consulta JSON supportato RPCs.

Analizza l'attività sulla blockchain di Bitcoin

Puoi analizzare il volume dell'attività delle transazioni sulla blockchain di Bitcoin utilizzando il metodo `getchaintxstats` JSON-RPC. Questo JSON-RPC ti consente di accedere a metriche come i

tassi medi di transazione al secondo, il numero totale di transazioni, il numero di blocchi e altro ancora. Puoi anche definire una finestra di numeri di blocco o un hash di blocco come delimitatore per calcolare queste statistiche per un insieme specifico di blocchi nella rete, se lo desideri.

Per ulteriori informazioni, consulta JSON supportato RPCs.

Verifica i messaggi firmati utilizzando una coppia di chiavi Bitcoin

I portafogli Bitcoin hanno una chiave privata e una chiave pubblica che costituiscono una coppia di chiavi. Queste chiavi vengono utilizzate per firmare le transazioni e fungono da identità dell'utente sulla blockchain. La chiave pubblica viene utilizzata per creare indirizzi, che sono identificatori alfanumerici standardizzati (da 27 a 34 caratteri). Questi indirizzi vengono utilizzati per ricevere output BTC e gestire transazioni o messaggi.

Con un portafoglio Bitcoin, gli utenti possono anche firmare e verificare i messaggi in modo crittografico. Questo processo viene spesso utilizzato per dimostrare la proprietà di uno specifico indirizzo di portafoglio e del BTC ad esso associato. Utilizzando `verifymessage` Bitcoin JSON-RPC, puoi verificare l'autenticità e la validità di un messaggio firmato da un altro portafoglio. In particolare, un nodo Bitcoin può essere utilizzato per verificare se un messaggio è stato firmato utilizzando la chiave privata corrispondente all'indirizzo derivato dalla chiave pubblica fornita all'interno del messaggio firmato stesso.

Per ulteriori informazioni, consulta JSON supportato RPCs.

Ispeziona il mempool di Bitcoin

Molte applicazioni devono accedere al mempool per tenere traccia delle transazioni in sospeso, ottenere un elenco di tutte le transazioni in sospeso o scoprire da dove proviene una transazione. Per fare ciò, ci sono Bitcoin RPCs simili a JSON e `getrawmempool` che `getmempoolancestors` supportano `getmempoolentry` questa attività. Questi Bitcoin JSON RPCs aiutano le applicazioni a ottenere le informazioni di cui hanno bisogno dal mempool.

Amazon Managed Blockchain (AMB) Access Bitcoin supporta anche `testmempoolaccept` Bitcoin JSON-RPCs, che consente di verificare se una transazione soddisfa le regole del protocollo e verrebbe accettata da un nodo prima dell'invio. I portafogli, gli exchange e qualsiasi altra entità che invia direttamente transazioni alla blockchain di Bitcoin utilizzano questi Bitcoin JSON-. RPCs

Per ulteriori informazioni, consulta JSON supportato RPCs.

Bitcoin JSON supportato: RPCs con Amazon Managed Blockchain (AMB) Access Bitcoin

Questo argomento fornisce un elenco e riferimenti al codice JSON di Bitcoin supportato da Managed Blockchain. RPCs Ogni JSON-RPC supportato ha una breve descrizione del suo utilizzo.

Note

- Puoi autenticare Bitcoin JSON- RPCs su Managed Blockchain utilizzando il processo di firma Signature Version 4 (SigV4). Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono interagire con l'account utilizzando Bitcoin JSON-. RPCs Fornisci AWS le credenziali (un ID della chiave di accesso e una chiave di accesso segreta) con la chiamata.
- Se la risposta HTTP è superiore a 10 MB, verrà visualizzato un errore. Per correggere questo problema, è necessario impostare le intestazioni di compressione su`Accept-Encoding:gzip`. La risposta compressa che il client riceve contiene le seguenti intestazioni: e. `Content-Type: application/json` `Content-Encoding: gzip`
- Amazon Managed Blockchain (AMB) Access Bitcoin genera un errore 400 per richieste JSON-RPC non corrette.
- Usa `sendrawtransaction` JSON-RPC per inviare transazioni che aggiornano lo stato della blockchain di Bitcoin.
- AMB Access Bitcoin ha un limite di richieste predefinito di 100 richieste al secondo (RPS), per regione. `NETWORK_TYPE` AWS

  Per aumentare la tua quota, devi contattare AWS l'assistenza. Per contattare l' AWS assistenza, accedi alla console del AWS Support Center. Scegli Crea caso. Scegli Tecnico. Scegli Managed Blockchain come servizio. Scegli Access:Bitcoin come categoria e Guida generale come severità. Inserisci la quota RPC come oggetto e nella casella di testo Descrizione ed elenca i limiti di quota applicabili alle tue esigenze in RPS per rete Bitcoin per regione. Invia il tuo caso.

JSON supportato RPCs

AMB Access Bitcoin supporta i seguenti Bitcoin JSON-. RPCs Ogni chiamata supportata ha una breve descrizione del suo utilizzo.

Categoria	JSON-RPC	Descrizione
Blockchain RPCs	ottieni il miglior blockhash	Restituisce l'hash del blocco best (tip) nella catena più utilizzata e completamente convalidata.
	getblock	Se la verbosità è 0, restituisce una stringa composta da dati serializzati con codifica esadecimale per il blocco 'hash'. Se la verbosità è 1, restituisce un oggetto con informazioni sul blocco 'hash'. Se la verbosità è 2, restituisce un oggetto con informazioni sull'hash del blocco e informazioni su ogni transazione. Se la verbosità è 3, restituisce un oggetto con informazioni sull'hash del blocco e informazioni su ogni transazione, incluse le informazioni per gli input. `prevout`
	getblockchaininfo	Restituisce un oggetto contenente varie informazioni sullo stato relative all'elaborazione della blockchain.
	getblockcount	Restituisce l'altezza della catena più elaborata e completamente convalidata. Il blocco genesis ha altezza 0.
	getblock filter	Recupera un filtro di contenuto BIP 157 per un particolare blocco utilizzando l'hash del blocco.
	getblockhash	Restituisce l'hash del blocco all'altezza fornita. best-block-chain

Categoria	JSON-RPC	Descrizione
	getblockheader	Se verbose è false, restituisce una stringa composta da dati serializzati con codifica esadecimale per il blockheader 'hash'. Se verbose è vero, restituisce un oggetto con informazioni sul blockheader 'hash'.
	getblockstats	Calcola le statistiche per blocco per una determinata finestra. Tutti gli importi sono espressi in satoshi. Non funzionerà per alcune altezze con la potatura.
	ottieni consigli sulla catena	Restituisce informazioni su tutti i suggerime nti conosciuti nell'albero dei blocchi, inclusa la catena principale e i rami orfani.
	getchaintxstats	Calcola statistiche sul numero totale e sulla velocità delle transazioni nella catena.
	avere difficoltà	Restituisce la proof-of-work difficoltà come multiplo della difficoltà minima.
	getmempoolancestors	Se txid è nel mempool, restituisce tutti gli antenati in mempool.
	getmempool descendants	Se txid è nel mempool, restituisce tutti i discendenti in mempool.
	getmempool entry	Restituisce i dati mempool per una determinata transazione.
	getmempoolinfo	Restituisce dettagli sullo stato attivo del pool di memoria TX.

Categoria	JSON-RPC	Descrizione
	getrawmempool	Restituisce tutte le transazioni IDs nel pool di memoria come matrice JSON di transazioni di stringhe. IDs **Note** `verbose = true` non è supportato.
	gettxout	Restituisce i dettagli sull'output di una transazione non spesa.
	gettxoutproof	Restituisce una prova con codifica esadecimale che «txid» è stato incluso in un blocco.
Transazioni grezze RPCs	crea una transazione non elaborata	Crea una transazione spendendo gli input dati e creando nuovi output.
	decodifica una transazione grezza	Restituisce un oggetto JSON che rappresenta la transazione serializzata con codifica esadecimale.
	decodescript	Decodifica uno script con codifica esadecimale.
	ottieni una transazione grezza	Restituisce i dati grezzi della transazione.
	invia una transazione non elaborata	Invia una transazione non elaborata (serializzata, con codifica esadecimale) al nodo e alla rete locali.
	testmempoolaccept	Restituisce il risultato dei test di accettazione di mempool che indicano se la transazione non elaborata (serializzata, con codifica esadecimale) sarebbe stata accettata da mempool. Questo verifica se la transazione viola il consenso o le regole politiche.

Categoria	JSON-RPC	Descrizione
Util RPCs	crea multisig	Crea un indirizzo con più firme senza che sia richiesta la firma delle mie chiavi.
	stima la tariffa intelligente	Stima la commissione approssimativa per kilobyte richiesta per la conferma di una transazione all'interno dei blocchi conf_target, se possibile, e restituisce il numero di blocchi per i quali la stima è valida. Utilizza la dimensione della transazione virtuale, come definita nel BIP 141 (i dati di riferimento sono scontati).
	convalida l'indirizzo	Restituisce informazioni sull'indirizzo bitcoin specificato.
	messaggio di verifica	Verifica un messaggio firmato.

Sicurezza in Amazon Managed Blockchain (AMB) Access Bitcoin

La sicurezza del cloud ha AWS la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa lo descrive sia come sicurezza del cloud che come sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per maggiori informazioni sui programmi di conformità che si applicano ad Amazon Managed Blockchain (AMB) Access Bitcoin, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Per fornire protezione dei dati, autenticazione e controllo degli accessi, Amazon Managed Blockchain utilizza AWS le caratteristiche e le caratteristiche del framework open source in esecuzione in Managed Blockchain.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AMB Access Bitcoin. I seguenti argomenti mostrano come configurare AMB Access Bitcoin per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse AMB Access Bitcoin.

Argomenti

- Protezione dei dati in Amazon Managed Blockchain (AMB) Access Bitcoin
- Gestione delle identità e degli accessi per Amazon Managed Blockchain (AMB) Access Bitcoin

Protezione dei dati in Amazon Managed Blockchain (AMB) Access Bitcoin

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon Managed Blockchain (AMB) Access Bitcoin. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AMB Access Bitcoin o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un

server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

La crittografia dei dati aiuta a impedire agli utenti non autorizzati di leggere i dati da una rete blockchain e dai sistemi di archiviazione dati associati. Ciò include i dati che potrebbero essere intercettati mentre viaggiano nella rete, noti come dati in transito.

Crittografia in transito

Per impostazione predefinita, Managed Blockchain utilizza una connessione HTTPS/TLS per crittografare tutti i dati trasmessi da un computer client che esegue gli endpoint dei due servizi. AWS CLI AWS

Non devi fare nulla per abilitare l'uso di HTTPS/TLS. È sempre abilitato a meno che non lo disabiliti esplicitamente per un singolo AWS CLI comando utilizzando il comando. `--no-verify-ssl`

Gestione delle identità e degli accessi per Amazon Managed Blockchain (AMB) Access Bitcoin

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse AMB Access Bitcoin. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell’accesso tramite policy
- Come funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM
- Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Bitcoin

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Bitcoin)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM

Prima di utilizzare IAM per gestire l'accesso a AMB Access Bitcoin, scopri quali funzionalità IAM sono disponibili per l'uso con AMB Access Bitcoin.

Funzionalità IAM che puoi utilizzare con Amazon Managed Blockchain (AMB) Access Bitcoin

Funzionalità IAM	Supporto per AMB Access Bitcoin
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	No
ACLs	No

Funzionalità IAM	Supporto per AMB Access Bitcoin
ABAC (tag nelle policy)	No
Credenziali temporanee	No
Autorizzazioni del principale	No
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come AMB Access Bitcoin e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AMB Access Bitcoin

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per AMB Access Bitcoin

Per visualizzare esempi di politiche basate sull'identità di AMB Access Bitcoin, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

Politiche basate sulle risorse all'interno di AMB Access Bitcoin

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per AMB Access Bitcoin

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni Bitcoin di AMB Access, consulta Azioni definite da Amazon Managed Blockchain (AMB) Access Bitcoin nel Service Authorization Reference.

Le azioni politiche in AMB Access Bitcoin utilizzano il seguente prefisso prima dell'azione:

```
managedblockchain:
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `InvokeRpcBitcoin`, includi la seguente azione:

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

Per visualizzare esempi di politiche basate sull'identità di AMB Access Bitcoin, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

Risorse politiche per AMB Access Bitcoin

Supporta le risorse di policy: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse Bitcoin di AMB Access e relativi ARNs, consulta Resources Defined by Amazon Managed Blockchain (AMB) Access Bitcoin nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Actions Defined by Amazon Managed Blockchain (AMB) Access Bitcoin.

Per visualizzare esempi di politiche basate sull'identità di AMB Access Bitcoin, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

Chiavi delle condizioni politiche per AMB Access Bitcoin

Supporta le chiavi di condizione delle policy specifiche del servizio: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per

visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di AMB Access Bitcoin, consulta Condition Keys for Amazon Managed Blockchain (AMB) Access Bitcoin nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Actions Defined by Amazon Managed Blockchain (AMB) Access Bitcoin.

Per visualizzare esempi di politiche basate sull'identità di AMB Access Bitcoin, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

ACLs in AMB Access Bitcoin

Supporti ACLs: No

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AMB Access Bitcoin

Supporta ABAC (tag nelle policy): No

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AMB Access Bitcoin

Supporta credenziali temporanee: No

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per AMB Access Bitcoin

Supporta l'inoltro delle sessioni di accesso (FAS): no

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AMB Access Bitcoin

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di AMB Access Bitcoin. Modifica i ruoli di servizio solo quando AMB Access Bitcoin fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per AMB Access Bitcoin

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono

visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Bitcoin

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse AMB Access Bitcoin. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da AMB Access Bitcoin, incluso il formato di ARNs per ogni tipo di risorsa, consulta Actions, Resources and Condition Keys for Amazon Managed Blockchain (AMB) Access Bitcoin nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console AMB Access Bitcoin
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accesso alle reti Bitcoin

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Bitcoin di AMB Access nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono

le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console AMB Access Bitcoin

Per accedere alla console Amazon Managed Blockchain (AMB) Access Bitcoin, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Bitcoin di AMB Access presenti nel tuo. Account AWS Se crei una policy basata

sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Bitcoin di AMB Access, allega anche la policy AMB Access Bitcoin *`ConsoleAccess`* o *`ReadOnly`* AWS gestita alle entità. Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. 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": "*"
        }
    ]
}
```

Accesso alle reti Bitcoin

> **Note**
>
> Per accedere agli endpoint pubblici del Bitcoin `mainnet` ed `testnet` effettuare chiamate JSON-RPC, avrai bisogno di credenziali utente (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) che dispongano delle autorizzazioni IAM appropriate per AMB Access Bitcoin.

Example Policy IAM per accedere a tutte le reti Bitcoin

Questo esempio garantisce a un utente IAM l' Account AWS accesso a tutte le reti Bitcoin.

JSON

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

Example Policy IAM per accedere alla rete Bitcoin Testnet

Questo esempio concede a un utente IAM l' Account AWS accesso alla rete Bitcoin`testnet`.

JSON

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

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Bitcoin

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AMB Access Bitcoin e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione su AMB Access Bitcoin
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AMB Access Bitcoin

Non sono autorizzato a eseguire un'azione su AMB Access Bitcoin

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `managedblockchain::`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `managedblockchain::`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AMB Access Bitcoin.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AMB Access Bitcoin. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AMB Access Bitcoin

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AMB Access Bitcoin supporta queste funzionalità, consulta. Come funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM
- Per scoprire come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà nella IAM User Guide. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Registrazione degli eventi di Amazon Managed Blockchain (AMB) Access Bitcoin utilizzando AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin non supporta gli eventi di gestione.

Amazon Managed Blockchain è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Managed Blockchain. CloudTrail rileva chi ha richiamato gli endpoint Bitcoin di AMB Access per Managed Blockchain come eventi del piano dati.

Se crei un percorso correttamente configurato e sottoscritto per ricevere gli eventi del piano dati desiderati, puoi ricevere la distribuzione continua di eventi relativi a AMB Access Bitcoin a CloudTrail un bucket Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare se è stata effettuata una richiesta a uno degli endpoint Bitcoin di AMB Access, l'indirizzo IP da cui proviene la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli aggiuntivi.

Per saperne di più CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

AMB Accedi alle informazioni su Bitcoin in CloudTrail

AWS CloudTrail è abilitato per impostazione predefinita quando crei il tuo Account AWS. Tuttavia, per vedere chi ha richiamato gli endpoint Bitcoin di AMB Access, devi configurarli CloudTrail per registrare gli eventi del piano dati.

Per tenere un registro continuo degli eventi nel tuo computer Account AWS, inclusi gli eventi del piano dati per AMB Access Bitcoin, devi creare una traccia. Un trail consente di CloudTrail consegnare i file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso in Console di gestione AWS, il percorso si applica a tutti. Regioni AWS Il trail registra gli eventi di tutte le regioni supportate nella AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente questi dati e agire in base ai dati degli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Utilizzo CloudTrail per tracciare Bitcoin JSON- RPCs

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Analizzando gli eventi CloudTrail relativi ai dati, puoi monitorare chi ha richiamato gli endpoint Bitcoin di AMB Access.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di registro di AMB Access Bitcoin

Per gli eventi del piano dati, un trail è una configurazione che consente la consegna di eventi come file di registro a un bucket S3 specificato. Ogni file di CloudTrail registro contiene una o più voci di registro che rappresentano una singola richiesta proveniente da qualsiasi fonte. Queste voci forniscono dettagli sull'azione richiesta, tra cui la data e l'ora dell'azione e gli eventuali parametri di richiesta associati.

> **Note**
>
> CloudTrail gli eventi di dati nei file di registro non sono una traccia dello stack ordinata delle chiamate API Bitcoin di AMB Access, quindi non appaiono in un ordine specifico.

Utilizzo CloudTrail per tracciare Bitcoin JSON- RPCs

Puoi utilizzarlo CloudTrail per tracciare chi nel tuo account ha richiamato gli endpoint Bitcoin di AMB Access e quali dati JSON-RPC sono stati richiamati come eventi relativi ai dati. Per impostazione predefinita, quando crei un trail, gli eventi relativi ai dati non vengono registrati. Per registrare chi ha richiamato gli endpoint Bitcoin di AMB Access come eventi CloudTrail relativi ai dati, devi aggiungere esplicitamente le risorse o i tipi di risorse supportati per i quali desideri raccogliere attività in un percorso. Amazon Managed Blockchain supporta l'aggiunta di eventi relativi ai dati utilizzando l' Console di gestione AWS AWS SDK e AWS CLI. Per ulteriori informazioni, consulta Registra gli eventi utilizzando selettori avanzati nella Guida per l'AWS CloudTrail utente.

Per registrare gli eventi relativi ai dati in un percorso, utilizzate l'put-event-selectorsoperazione dopo aver creato il percorso. Utilizza l'`--advanced-event-selectors`opzione per specificare i tipi di `AWS::ManagedBlockchain::Network` risorse per iniziare a registrare gli eventi relativi ai dati per determinare chi ha richiamato gli endpoint Bitcoin di AMB Access.

Example Inserimento nel registro degli eventi dati di tutte le richieste relative agli endpoint Bitcoin AMB Access del tuo account

L'esempio seguente mostra come utilizzare l'`put-event-selectors`operazione per registrare tutte le richieste degli endpoint Bitcoin AMB Access del vostro account per il trail nella regione. `my-bitcoin-trail` `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"] } ]}]'
```

Dopo la sottoscrizione, puoi tenere traccia dell'utilizzo nel bucket S3 collegato al trail specificato nell'esempio precedente.

Il risultato seguente mostra una voce del registro degli eventi di CloudTrail dati con le informazioni raccolte da. CloudTrail È possibile determinare se è stata effettuata una richiesta Bitcoin JSON-RPC a uno degli endpoint Bitcoin di AMB Access, l'indirizzo IP da cui proviene la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli aggiuntivi.

```
{
        "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"
}
```

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.