aws

Guida per gli sviluppatori

AMBAccedi a Bitcoin

AMBAccedi a Bitcoin: Guida per gli sviluppatori

Table of Contents

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

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 RPC per comunicare con i nodi Bitcoin gestiti da Managed Blockchain per interagire con le reti Bitcoin. Con Bitcoin JSON-RPC, 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 Regione	Codice	Regione
Stati Uniti orientali (Virginia settentrionale)	IAD	`us-east-1`
Asia Pacifico (Tokyo)	NRT	ap-northeast-1
Asia Pacifico (Seul)	ICONA	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-RPC 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 JSON-RPC Bitcoin.

- 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 i tuoi Bitcoin JSON-RPC. 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 conto. Il capitolo seguente illustra come iniziare a utilizzare AMB Access Bitcoin.

Prerequisiti e considerazioni

Prima di usare AWS per la prima volta, devi avere un Account AWS.

Iscriviti per AWS

Quando ti iscrivi a 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 hai un Account AWS già, vai al passaggio successivo. Se non hai un Account AWS, utilizza la procedura seguente 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, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, un Utente root dell'account AWSviene creato. L'utente root ha accesso a tutti Servizi AWS e le risorse presenti 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 IAM utente con le autorizzazioni appropriate

Per creare e lavorare con AMB Access Bitcoin, devi avere un AWS Identity and Access Management (IAM) principale (utente o gruppo) con autorizzazioni che consentono le azioni Managed Blockchain necessarie.

Solo IAM gli amministratori possono effettuare chiamate in BitcoinJSON. RPC Quando effettui chiamate verso Bitcoin JSON - RPCs su Amazon Managed Blockchain, puoi farlo tramite una HTTPS connessione autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i IAM destinatari autorizzati nel AWS l'account può effettuare RPC chiamate in BitcoinJSON. Per farlo: AWS le credenziali (un ID della chiave di accesso e una chiave di accesso segreta) devono essere fornite con la chiamata.

Per informazioni su come creare un IAM utente, vedi Creazione di un IAM utente in AWS conto. Per ulteriori informazioni su come allegare una politica di autorizzazioni a un utente, vedere Modifica delle autorizzazioni per un IAM utente. 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 () Access Bitcoin AMB

Installa e configura il AWS Command Line Interface

Se non l'hai ancora fatto, installa la versione più recente AWS Interfaccia a riga di comando (CLI) con cui lavorare AWS risorse da un terminale. Per ulteriori informazioni, vedere Installazione o aggiornamento della versione più recente di AWS CLI.

> **Note**
>
> Per CLI accedere, 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, vedere Utilizzo di credenziali temporanee con AWS risorse nella Guida per l'IAMutente.

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 IAM politica per accedere a Bitcoin JSON - RPCs

Per poter accedere agli endpoint pubblici su Bitcoin Mainnet e Testnet per effettuare JSON RPC chiamate, devi disporre di credenziali utente (AWS_ACCESS_ KEY _ID e AWS_SECRET _ _) con le autorizzazioni appropriate per IAM Amazon Managed Blockchain (KEY) Access Bitcoin. ACCESS AMB In un terminale con AWS CLI installato, esegui il seguente comando per creare una IAM politica 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 IAM dell'utente per renderla effettiva. Nel AWS Management Console, accedi al IAM servizio e allega la policy `AmazonManagedBlockchainBitcoinAccess` al ruolo assegnato al tuo IAM utente. Per ulteriori informazioni, consulta Creazione di un ruolo e assegnazione a un IAM utente.

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

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

Example

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

1. Apri la console Managed Blockchain all'indirizzo. https://console.aws.amazon.com/managedblockchain/
2. Scegli RPCl'editor.
3. Nella sezione Richiesta, scegli `BITCOIN_MAINNET` come rete Blockchain.
4. Scegli `getblock` come RPCmetodo.
5. Inserisci `00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09` come numero di blocco e scegli `0` come verbosità.
6. Quindi, scegli Submit (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 RPCssupportata da AMB Access Bitcoin

Make AMB Access BitcoinJSON: RPC richieste in awscurl utilizzando il AWS CLI

Example

Firma le richieste con le tue credenziali IAM utente utilizzando Signature Version 4 (SigV4) per effettuare RPC chiamate Bitcoin agli endpoint JSON Access Bitcoin. AMB Lo strumento da riga di comando awscurl può aiutarti a firmare le richieste a AWS servizi che utilizzano SigV4. Per ulteriori informazioni, consulta READMEawscurl .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 il AWS CLI, le credenziali IAM utente e la AWS regione predefinita sono impostate nel tuo ambiente e hanno accesso a awscurl. Utilizzando awscurl, invia una richiesta sia a Bitcoin Mainnet che a Testnet invocando il. `getblock` RPC 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 preferito e RPC AWS Regione supportata da Amazon Managed Blockchain (AMB) Access Bitcoin. Inoltre, puoi effettuare una richiesta sulla rete Testnet, anziché sulla rete Mainnet, sostituendola `mainnet` con `testnet` nel comando.

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

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 RPC richieste in Bitcoin JSON in Node.js

Puoi inviare richieste firmate utilizzando HTTPS per accedere agli endpoint Bitcoin Mainnet e Testnet ed effettuare JSON RPC API chiamate 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 RPC richiesta Bitcoin agli JSON endpoint AMB Access Bitcoin.

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 AMB Access Bitcoin.

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

```
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 RPC richieste all'endpoint Bitcoin e firma tali richieste con le intestazioni Signature Version 4 (SigV4) appropriate utilizzando il codice ufficiale AWS SDKstrumenti v3. 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'Make AMB Access BitcoinJSON: RPC richieste in awscurl utilizzando il AWS CLIesempio. Per effettuare altre chiamate, modifica l'`rpc`oggetto nello script con un altro Bitcoin JSON -RPC. Puoi modificare l'opzione della proprietà host in Bitcoin `testnet` per 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 connetterti VPC ai servizi in modo privato come se fossero presenti nel tuo. VPC Non è necessario utilizzare un gateway Internet, un NAT dispositivo, un indirizzo IP pubblico, AWS Connessione Direct Connect, oppure AWS VPNConnessione da sito a sito per comunicare con il servizio dalle sottoreti private. Per ulteriori informazioni sull' AWS PrivateLink o per configurare AWS PrivateLink, vedi Cos'è AWS PrivateLink?

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

Per il nome del servizio, cerca Amazon Managed Blockchain nel AWS colonna di servizio. Per ulteriori informazioni, consulta AWS 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

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 (UTXO) per un determinato insieme di indirizzi, firmano e inviano transazioni alla rete Bitcoin e recuperano dati sulle transazioni storiche.

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

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

Per ulteriori informazioni, consulta JSON-RPC supportati.

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-RPC supportati.

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-RPC supportati.

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 JSON-RPC come`getmempoolancestors`, `getmempoolentry` e che supportano questa attività. `getrawmempool` Questi Bitcoin JSON-RPC aiutano le applicazioni a ottenere le informazioni di cui hanno bisogno dal mempool.

Amazon Managed Blockchain (AMB) Access Bitcoin supporta anche `testmempoolaccept` Bitcoin JSON-RPC, che consente di verificare se una transazione soddisfa le regole del protocollo e se 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 JSON-RPC di Bitcoin.

Per ulteriori informazioni, consulta JSON-RPC supportati.

Bitcoin JSON-RPC supportati con Amazon Managed Blockchain (AMB) Access Bitcoin

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

Note

- Puoi autenticare Bitcoin JSON-RPC 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-RPC. 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-RPC supportati

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

Categoria	JSON-RPC	Descrizione
RPC blockchain	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 tutti gli ID delle transazioni nel pool di memoria come matrice JSON di ID di transazione di stringa. **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 (RPC)	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 RPC	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

Il AWS modello di responsabilità 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 tutte le Cloud AWS. L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta la AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura singoli utenti con AWS IAM Identity Center oppure 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:

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi di acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di 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 sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente 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 consoleAPI, AWS CLI, oppure 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. Se fornisci un URL a un

server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel 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 TLS connessioneHTTPS/per crittografare tutti i dati trasmessi da un computer client che esegue il AWS CLI in AWS endpoint di servizio.

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

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

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

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in AMB Access Bitcoin.

Utente del servizio: se utilizzi il servizio AMB Access Bitcoin per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni di cui hai bisogno. Man mano che utilizzi più funzionalità di AMB Access Bitcoin per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AMB Access Bitcoin, vediRisoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Bitcoin.

Amministratore del servizio: se sei responsabile delle risorse di AMB Access Bitcoin presso la tua azienda, probabilmente hai pieno accesso ad AMB Access Bitcoin. È tuo compito determinare a quali funzionalità e risorse di AMB Access Bitcoin devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per saperne di più su come la tua azienda può utilizzare IAM AMB Access Bitcoin, consultaCome funziona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso ad AMB Access Bitcoin. Per visualizzare esempi di politiche basate sull'identità di AMB Access Bitcoin che puoi utilizzare inIAM, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain () Access Bitcoin AMB

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta AWS Signature Version 4 per API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Autenticazione a AWS più fattori IAM nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per

informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per IAM gli utenti nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. Per assumere temporaneamente un IAM ruolo in AWS Management Console, puoi passare da un utente a un IAM ruolo (console). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Metodi per assumere un ruolo nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni

sui ruoli per la federazione, consulta Creare un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Cross Account Resource Access IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FASIe richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: 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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per

informazioni su come creare una politica basata sull'identità, consulta Definire le IAM autorizzazioni personalizzate con le politiche gestite dal cliente nella Guida per l'utente. IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scegliere tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità

(utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

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

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

IAMfunzionalità che puoi usare con Amazon Managed Blockchain (AMB) Access Bitcoin

IAMfunzionalità	AMBAccedi al supporto Bitcoin
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	No
ACLs	No
ABAC(tag nelle politiche)	No
Credenziali temporanee	No
Autorizzazioni del principale	No
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale del funzionamento di AMB Access Bitcoin e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per Access Bitcoin AMB

Supporta le policy basate su identità: sì

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

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Access Bitcoin AMB

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

Politiche basate sulle risorse all'interno di Access Bitcoin AMB

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per AMB Access Bitcoin

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di AMB Access Bitcoin, 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 () Access Bitcoin AMB

Risorse politiche per Access Bitcoin AMB

Supporta risorse politiche: No

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse AMB Access Bitcoin e relativiARNs, consulta Resources Defined by Amazon Managed Blockchain (AMB) Access Bitcoin nel Service Authorization Reference. Per sapere con quali azioni puoi specificare le caratteristiche ARN di ogni risorsa, consulta Azioni definite da 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 () Access Bitcoin AMB

Chiavi relative alle condizioni delle politiche per Access Bitcoin AMB

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi 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.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il

suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

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 () Access Bitcoin AMB

ACLsin Access Bitcoin AMB

SupportiACLs: 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon Access Bitcoin AMB

Supporti ABAC (tag nelle politiche): No

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni in meritoABAC, vedere Definizione delle autorizzazioni con ABAC autorizzazione nella Guida per l'IAMutente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Use Attribute-based access control (ABAC) nella Guida per l'utente. IAM

Utilizzo di credenziali temporanee con Access Bitcoin AMB

Supporta credenziali temporanee: No

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione Servizi AWS relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare da un utente a un IAM ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali multiservizio per Access Bitcoin AMB

Supporta sessioni di accesso diretto (FAS): No

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle

autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per AMB Access Bitcoin

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.

> **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 Access Bitcoin AMB

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

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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 () Access Bitcoin AMB

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse di AMB Access Bitcoin. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di

eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

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

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

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse AMB Access Bitcoin nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui 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 ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL.

È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.

- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle politiche con IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta Secure API access with MFA nella Guida IAM per l'utente.

Per ulteriori informazioni sulle best practice inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida IAM per l'utente.

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 AMB Access Bitcoin 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 per la console per gli utenti che effettuano chiamate solo verso la AWS CLI o la. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console AMB Access Bitcoin, allega anche AMB Access Bitcoin `ConsoleAccess` o la policy `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le

autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

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

Accesso alle reti Bitcoin

> **Note**
>
> Per accedere agli endpoint pubblici di Bitcoin `mainnet` ed `testnet` effettuare JSON RPC chiamate, avrai bisogno di credenziali utente

(`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) che dispongano delle IAM autorizzazioni appropriate per AMB Access Bitcoin.

Example IAMPolitica di accesso a tutte le reti Bitcoin

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

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

Example IAMPolitica di accesso alla rete Bitcoin Testnet

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

```
{
    "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 eIAM.

Argomenti

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

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

```
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 assistenza, contatta l'amministratore. AWS 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 assegnare un ruolo ad AMB Access Bitcoin.

Alcuni Servizi AWS consentono di passare 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 IAM utente 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 passare 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 concedere alle persone l'accesso alle tue risorse.

Per ulteriori 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 sapere come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.

- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM 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, è necessario configurare CloudTrail la registrazione degli 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 AWS Management Console, 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-RPC

- 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, vedete l'elemento CloudTrail userIdentity.

Informazioni sulle 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-RPC

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 in modo esplicito 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' AWS Management Console 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 Registrazione nel registro degli eventi relativi ai 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.