aws

Guía para desarrolladores

Acceso AMB a Bitcoin

Acceso AMB a Bitcoin: Guía para desarrolladores

Table of Contents

¿Qué es Amazon Managed Blockchain (AMB) Access Bitcoin?

Amazon Managed Blockchain (AMB) Access le proporciona nodos de cadena de bloques públicos para Ethereum y Bitcoin, y también puede crear redes de cadenas de bloques privadas con el marco Hyperledger Fabric. Elija entre varios métodos para interactuar con las cadenas de bloques públicas, incluidas las operaciones de API de múltiples inquilinos totalmente gestionadas, de un solo inquilino (dedicadas) y sin servidor hasta los nodos de cadenas de bloques públicas. Para los casos de uso en los que los controles de acceso son importantes, puedes elegir entre redes de cadenas de bloques privadas totalmente gestionadas. Las operaciones de API estandarizadas te ofrecen escalabilidad instantánea en una infraestructura resiliente y totalmente gestionada, para que puedas crear aplicaciones de cadena de bloques.

AMB Access le ofrece dos tipos distintos de servicios de infraestructura de cadena de bloques: operaciones de API de acceso a la red de cadena de bloques multiusuario y nodos y redes de cadena de bloques dedicados. Con una infraestructura de cadena de bloques dedicada, puede crear y utilizar nodos públicos de cadenas de bloques de Ethereum y redes de cadenas de bloques privadas de Hyperledger Fabric para su propio uso. Sin embargo, las ofertas multiusuario basadas en API, como AMB Access Bitcoin, se componen de una flota de nodos de Bitcoin situados detrás de una capa de API en la que la infraestructura de nodos de cadena de bloques subyacente se comparte entre los clientes.

Bitcoin es una red de cadena de bloques descentralizada que permite peer-to-peer realizar transacciones seguras de valor denominadas en la criptomoneda nativa de la red, Bitcoin (BTC). La red Bitcoin es utilizada por personas, instituciones financieras, empresas de tecnología financiera, gobiernos y más. La red Bitcoin es un medio de intercambio, una materia prima para la inversión o un libro de contabilidad inmutable y verificable públicamente para los datos inscritos. Con Amazon Managed Blockchain (AMB) Access Bitcoin, puede acceder a un conjunto de redes Mainnet y Testnet de Bitcoin a través de puntos de conexión regionales, a través de los cuales puede escribir transacciones, leer datos del libro mayor e invocar solicitudes JSON-RPC disponibles en el cliente del nodo Bitcoin Core. Con los puntos de conexión de Bitcoin sin servidor, puede centrarse en crear sus aplicaciones en lugar de invertir en tareas indiferenciadas, como el aprovisionamiento, el mantenimiento y el equilibrio de carga de los nodos de Bitcoin. Ya sea que esté creando una cartera de Bitcoin, creando una bolsa de criptomonedas o analizando los datos de la cadena de bloques de Bitcoin, solo pagará por las solicitudes que realice a través de los puntos de conexión de Bitcoin mediante AMB Access Bitcoin.

¿Es la primera vez que utiliza AMB Access Bitcoin?

Si es la primera vez que utiliza AMB Access Bitcoin, le recomendamos que comience leyendo las siguientes secciones:

- Conceptos clave: Amazon Managed Blockchain (AMB) Access Bitcoin
- Primeros pasos con Amazon Managed Blockchain (AMB) Access Bitcoin
- Casos de uso de Bitcoin con Amazon Managed Blockchain (AMB) Access Bitcoin
- Compatible con Bitcoin JSON: RPCs con Amazon Managed Blockchain (AMB) Acceda a Bitcoin

Conceptos clave: Amazon Managed Blockchain (AMB) Access Bitcoin

> **Note**
>
> En esta guía se presupone que está familiarizado con los conceptos que son esenciales para Bitcoin. Estos conceptos incluyen la descentralización, los nodos, las transacciones, las carteras proof-of-work, las claves públicas y privadas, las divisiones a la mitad y otros. Antes de utilizar Amazon Managed Blockchain (AMB) Access Bitcoin, le recomendamos que consulte la documentación de desarrollo de Bitcoin y Mastering Bitcoin.

Amazon Managed Blockchain (AMB) Access Bitcoin le proporciona acceso sin servidor a la cadena de bloques de Bitcoin, sin necesidad de aprovisionar ni gestionar ninguna infraestructura de Bitcoin, incluidos los nodos. Puede utilizar este servicio gestionado para acceder a las redes de Bitcoin de forma rápida y bajo demanda, lo que reduce el coste total de propiedad.

El AMB Access Bitcoin le permite acceder a la red de Bitcoin a través de nodos completos que ejecutan el cliente Bitcoin Core, con la funcionalidad de monedero deshabilitada y admite varias llamadas a JSON Remote Procedure (JSON-RPC). Puedes invocar Bitcoin JSON RPCs para comunicarte con los nodos de Bitcoin gestionados por Managed Blockchain e interactuar con las redes de Bitcoin. Con el JSON- de BitcoinRPCs, puede leer datos y escribir transacciones, incluida la consulta de datos y el envío de transacciones a las redes de Bitcoin mediante el servicio Amazon Managed Blockchain.

> **Important**
>
> Eres responsable de crear, mantener, usar y administrar tus direcciones de Bitcoin. También eres responsable del contenido de tus direcciones de Bitcoin. AWS no se hace responsable de las transacciones desplegadas o solicitadas mediante nodos de Bitcoin en Amazon Managed Blockchain.

Consideraciones y limitaciones para usar Amazon Managed Blockchain (AMB) Access Bitcoin

- Redes de Bitcoin compatibles

  AMB Access Bitcoin es compatible con las siguientes redes públicas:

  - Mainnet: la cadena de bloques pública de Bitcoin asegurada por proof-of-work consenso y en la que se emite y negocia la criptomoneda Bitcoin (BTC). Las transacciones en Mainnet tienen un valor real (es decir, incurren en costes reales) y se registran en la cadena de bloques pública.
  - Testnet: la red de prueba es una cadena de bloques alternativa de Bitcoin que se utiliza para realizar pruebas. Las monedas Testnet están separadas y son distintas del Bitcoin (BTC) real y, por lo general, no tienen ningún valor.

  > **Note**
  >
  > No se admiten redes privadas.

- Regiones admitidas

  Las siguientes son las regiones compatibles con este servicio:

Nombre de la región	Código	Region
Este de EE. UU. (Norte de Virginia)	IAD	`us-east-1`
Asia-Pacífico (Tokio)	NRT	ap-northeast-1
Asia-Pacífico (Seúl)	ICN	ap-northeast-2
Asia-Pacífico (Singapur)	SIN	ap-southeast-1
Europa (Irlanda)	DUB	eu-west-1
Europa (Londres)	LHR	eu-west-2

- Service endpoints

  Los siguientes son los puntos de conexión del servicio para AMB Access Bitcoin. Para conectarse al servicio, debe usar un punto final que incluya una de las regiones compatibles.

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

  Por ejemplo: `mainnet.bitcoin.managedblockchain.eu-west-2.amazonaws.com`
- No se admite la minería

  AMB Access Bitcoin no admite la minería de Bitcoin (BTC).
- Firma: versión 4: firma de llamadas JSON-RPC de Bitcoin

  Cuando realices llamadas al JSON- de Bitcoin RPCs en Amazon Managed Blockchain, puedes hacerlo a través de una conexión HTTPS autenticada mediante el proceso de firma de la versión 4 de Signature. Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden realizar llamadas JSON-RPC de Bitcoin. Para ello, se deben proporcionar AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.

  > **Important**
  >
  > - No inserte las credenciales del cliente en las aplicaciones orientadas al usuario.
  > - No puedes usar las políticas de IAM para restringir el acceso a un JSON- individual de Bitcoin. RPCs
- Solo se admiten los envíos de transacciones sin procesar

  Usa el `sendrawtransaction` JSON-RPC para enviar transacciones que actualicen el estado de la cadena de bloques de Bitcoin.
- AWS CloudTrail soporte de registro

  Puede configurarlo CloudTrail para registrar su JSON- de BitcoinRPCs. Para obtener más información, consulte Registro de eventos de Amazon Managed Blockchain (AMB) Acceda a Bitcoin mediante AWS CloudTrail

Configuración de Amazon Managed Blockchain (AMB) Access Bitcoin

Antes de utilizar Amazon Managed Blockchain (AMB) Access Bitcoin por primera vez, siga los pasos de esta sección para crear una AWS cuenta. En el siguiente capítulo se explica cómo empezar a utilizar AMB Access Bitcoin.

Requisitos y consideraciones previos

Antes de usarlo AWS por primera vez, debe tener un Cuenta de AWS.

Inscríbase en AWS

Cuando te registras AWS, te Cuenta de AWS registras automáticamente para todos Servicios de AWS, incluido Amazon Managed Blockchain (AMB) Access Bitcoin. Solo se le cobrará por los servicios que utilice.

Si Cuenta de AWS ya tienes uno, continúa con el siguiente paso. Si no dispone de una Cuenta de AWS, utilice el siguiente procedimiento para crear una.

Para crear una AWS cuenta

1. Abre el https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar Tareas que requieren acceso de usuario raíz.

Cree un usuario de IAM con los permisos adecuados

Para crear y trabajar con AMB Access Bitcoin, debes tener un director AWS Identity and Access Management (IAM) (usuario o grupo) con permisos que permitan realizar las acciones necesarias en la cadena de bloques gestionada.

Solo los directores de IAM pueden realizar llamadas JSON-RPC de Bitcoin. Cuando realices llamadas al JSON- de Bitcoin RPCs en Amazon Managed Blockchain, puedes hacerlo a través de una conexión HTTPS autenticada mediante el proceso de firma de la versión 4 de Signature. Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden realizar llamadas JSON-RPC de Bitcoin. Para ello, se deben proporcionar AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.

Para obtener información sobre cómo crear un usuario de IAM, consulte Crear un usuario de IAM en su AWS cuenta. Para obtener más información sobre cómo adjuntar una política de permisos a un usuario, consulte Cambiar los permisos de un usuario de IAM. Para ver un ejemplo de una política de permisos que puede utilizar para conceder permiso a un usuario para que trabaje con AMB Access Bitcoin, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

Instale y configure el AWS Command Line Interface

Si aún no lo ha hecho, instale la interfaz de AWS línea de comandos (CLI) más reciente para trabajar con AWS los recursos de un terminal. Para obtener más información, consulte Instalación o actualización de la versión de AWS CLI más reciente.

> **Note**
>
> Para acceder a la CLI, necesita un ID de clave de acceso y una clave de acceso secreta. Cuando sea posible, utilice credenciales temporales en lugar de claves de acceso. Las credenciales temporales incluyen un ID de clave de acceso y una clave de acceso secreta, pero, además, incluyen un token de seguridad que indica cuándo caducan las credenciales. Para obtener más información, consulte Uso de credenciales temporales con AWS recursos en la Guía del usuario de IAM.

Primeros pasos con Amazon Managed Blockchain (AMB) Access Bitcoin

Utilice los step-by-step tutoriales de esta sección para aprender a realizar tareas con Amazon Managed Blockchain (AMB) Access Bitcoin. Estos ejemplos requieren que complete algunos requisitos previos. Si es la primera vez que utiliza AMB Access Bitcoin, consulte la sección de configuración de esta guía para asegurarse de que ha completado esos requisitos previos. Para obtener más información, consulte Configuración de Amazon Managed Blockchain (AMB) Access Bitcoin.

Temas

Cree una política de IAM para acceder a Bitcoin JSON- RPCs

Para acceder a los puntos finales públicos de la red principal y la red de pruebas de Bitcoin para realizar llamadas JSON-RPC, debe tener credenciales de usuario (AWS_ACCESS_KEY_ID y AWS_SECRET _ACCESS_KEY) que tengan los permisos de IAM adecuados para Amazon Managed Blockchain (AMB) Access Bitcoin. En una terminal con los terminales AWS CLI instalados, ejecute el siguiente comando para crear una política de IAM que permita acceder a los dos puntos de conexión de 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**
>
> El ejemplo anterior te da acceso tanto a la red principal como a la red de pruebas de Bitcoin. Para acceder a un punto final específico, usa el siguiente comando: `Action`
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

Después de crear la política, adjúntela al rol de su usuario de IAM para que entre en vigor. En el Consola de administración de AWS, navegue hasta el servicio de IAM y asocie la política `AmazonManagedBlockchainBitcoinAccess` al rol asignado a su usuario de IAM. Para obtener más información, consulte Crear un rol y asignarlo a un usuario de IAM.

Realice solicitudes de llamadas a procedimientos remotos (RPC) de Bitcoin en el editor RPC de AMB Access mediante el Consola de administración de AWS

Puede editar y enviar llamadas a procedimientos remotos (RPCs) Consola de administración de AWS utilizando AMB Access. Con ellos RPCs, puede leer datos, escribir y enviar transacciones en la red Bitcoin.

Example

El siguiente ejemplo muestra cómo obtener información sobre el *`blockhash`*00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 mediante RPC. `getBlock` Sustituya las variables resaltadas por sus propias entradas o elija uno de los otros métodos de RPC de la lista e introduzca las entradas pertinentes necesarias.

1. Abre la consola de Managed Blockchain en https://console.aws.amazon.com/managedblockchain/.
2. Elija el editor RPC.
3. En la sección de solicitudes, elige *BITCOIN_MAINNET* como Blockchain Network.
4. Elija *getblock* como método RPC.
5. Introduzca *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09* como número de bloque y elija *0* como verbosidad.
6. Luego, selecciona Enviar RPC.
7. Obtendrá los resultados en la sección de respuestas de esta página. A continuación, puede copiar todas las transacciones sin procesar para analizarlas más a fondo o utilizarlas en la lógica empresarial de sus aplicaciones.

Para obtener más información, consulte la página RPCs compatible con AMB Access Bitcoin

Realice solicitudes JSON-RPC de AMB Access Bitcoin en awscurl mediante el AWS CLI

Example

Firme las solicitudes con sus credenciales de usuario de IAM mediante la versión 4 de Signature (SiGv4) para realizar llamadas de Bitcoin JSON-RPC a los puntos finales de AMB Access Bitcoin. La herramienta de línea de comandos awscurl puede ayudarle a firmar las solicitudes de servicios mediante SiGv4. AWS Para obtener más información, consulte el archivo README.md de awscurl.

Instale awscurl mediante el método apropiado para su sistema operativo. En macOS, la aplicación recomendada HomeBrew es:

```
brew install awscurl
```

Si ya ha instalado y configurado la AWS CLI, sus credenciales de usuario de IAM y la región de AWS predeterminada se configuran en su entorno y tienen acceso a awscurl. Con awscurl, envíe una solicitud tanto a la red principal de Bitcoin como a la red de prueba invocando el RPC. `getblock` Esta llamada acepta un parámetro de cadena correspondiente al hash del bloque del que desea recuperar información.

El siguiente comando recupera los datos del encabezado del bloque de la red principal de Bitcoin utilizando el hash de bloque de la `params` matriz para seleccionar el bloque específico del que se van a recuperar los encabezados. En este ejemplo se utiliza el punto final. `us-east-1` Puede sustituirlo por el JSON-RPC y la AWS región de Bitcoin que prefiera y que sea compatible con Amazon Managed Blockchain (AMB) Access Bitcoin. Además, puede realizar una solicitud en la red Testnet, en lugar de en la red principal, sustituyéndola por en el 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
```

Los resultados incluyen detalles de las cabeceras de los bloques y una lista de los hashes de transacciones incluidos en el bloque solicitado. Vea el siguiente ejemplo:

```
{"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"}
```

Realice solicitudes JSON-RPC de Bitcoin en Node.js

Puede enviar solicitudes firmadas mediante HTTPS para acceder a los puntos finales de Bitcoin Mainnet y Testnet y realizar llamadas a la API JSON-RPC mediante el módulo https nativo de Node.js, o puede utilizar una biblioteca de terceros, como AXIOS. El siguiente ejemplo muestra cómo realizar una solicitud JSON-RPC de Bitcoin a los puntos finales de AMB Access Bitcoin.

Example

Para ejecutar este script Node.js de ejemplo, aplique los siguientes requisitos previos:

1. Debe tener el administrador de versiones de nodos (nvm) y Node.js instalados en el equipo. Puede encontrar las instrucciones de instalación de su sistema operativo aquí.
2. Utilice el `node --version` comando y confirme que está utilizando la versión 14 o superior de Node. Si es necesario, puede usar el `nvm install 14` comando, seguido del `nvm use 14` comando, para instalar la versión 14.
3. Las variables `AWS_ACCESS_KEY_ID` de entorno `AWS_SECRET_ACCESS_KEY` deben contener las credenciales asociadas a su cuenta. Las variables de entorno `AMB_HTTP_ENDPOINT` deben contener sus puntos finales de AMB Access Bitcoin.

   Exporte estas variables como cadenas en su cliente mediante los siguientes comandos. Sustituya los valores resaltados en las siguientes cadenas por los valores adecuados de su cuenta de usuario de IAM.

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

Una vez que haya completado todos los requisitos previos, copie el siguiente `package.json` archivo y `index.js` script en su entorno local mediante su editor:

package.json

```
{
  "name": "bitcoin-rpc",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "@aws-crypto/sha256-js": "^4.0.0",
    "@aws-sdk/credential-provider-node": "^3.360.0",
    "@aws-sdk/protocol-http": "^3.357.0",
    "@aws-sdk/signature-v4": "^3.357.0",
    "axios": "^1.4.0"
  }
}
```

index.js

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

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


const rpcRequest = async () => {

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

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

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

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

```
      host: url.hostname,
    }
  });


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

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

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


}

rpcRequest();
```

El código de ejemplo anterior utiliza Axios para realizar solicitudes de RPC al punto final de Bitcoin y las firma con los encabezados correspondientes de la versión 4 de firma (SiGv4) mediante las herramientas oficiales AWS del SDK v3. Para ejecutar el código, abre un terminal en el mismo directorio que tus archivos y ejecuta lo siguiente:

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

El resultado que se genere será similar al siguiente:

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
    confirmations":784126,"height":1000, "version":1,"versionHex":"00000001",
    "merkleroot":"fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33",
    "time":1232346882,
    "mediantime":1232344831,"nonce":2595206198,"bits":"1d00ffff","difficulty":1,
    "chainwork":"0000000000000000000000000000000000000000000000000000000000000003e903e903e9",
    "nTx":1,

 "previousblockhash":"0000000008e647742775a230787d66fdf92c46a48c896bfbc85cdc8acc67e87d",
```

```
"nextblockhash":"00000000a2887344f8db859e372e7e4bc26b23b9de340f725afbf2edb265b4c6",
"strippedsize":216,"size":216,"weight":864,
"tx":["fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33"]},
"error":null,"id":"1001"}
```

> **Note**
>
> La solicitud de ejemplo del script anterior realiza la `getblock` llamada con el mismo hash de bloque de parámetros de entrada que en el Realice solicitudes JSON-RPC de AMB Access Bitcoin en awscurl mediante el AWS CLI ejemplo. Para realizar otras llamadas, modifique el `rpc` objeto del script con un JSON-RPC de Bitcoin diferente. Puedes cambiar la opción de propiedad anfitriona a Bitcoin `testnet` para realizar llamadas en ese punto final.

Utilice AMB Access Bitcoin en lugar de AWS PrivateLink

AWS PrivateLink es una tecnología escalable y de alta disponibilidad que puede utilizar para conectar su VPC a los servicios de forma privada como si estuvieran en su VPC. No tiene que usar una puerta de enlace a Internet, un dispositivo NAT, una dirección IP pública, una conexión AWS Direct Connect o una conexión VPN AWS Site-to-Site para comunicarse con el servicio desde sus subredes privadas. Para obtener más información AWS PrivateLink o para configurarlo AWS PrivateLink, consulte ¿Qué es? AWS PrivateLink

Puede enviar solicitudes JSON-RPC de Bitcoin a AMB Access Bitcoin AWS PrivateLink mediante un punto final de VPC. Las solicitudes a este punto final privado no se transmiten a través de Internet abierto, por lo que puedes enviar solicitudes directamente a los puntos finales de Bitcoin mediante la misma autenticación SigV4. Para obtener más información, consulta Acceder a los AWS servicios a través de. AWS PrivateLink

Para el nombre del servicio, busca Amazon Managed Blockchain en la columna del AWS servicio. Para obtener más información, consulte AWS los servicios que se integran con AWS PrivateLink. El nombre del servicio del punto final tendrá el siguiente formato:`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

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

Casos de uso de Bitcoin con Amazon Managed Blockchain (AMB) Access Bitcoin

En este tema se proporciona una lista de los casos de uso de AMB Access Bitcoin

Temas

Cree una cartera de Bitcoin (BTC) para enviar y recibir BTC

El BTC, la criptomoneda nativa de la red de Bitcoin, es un componente esencial del modelo de seguridad de la red. También actúa como una mercancía y un medio de intercambio, muy utilizado por instituciones, empresas y particulares. En consecuencia, muchas aplicaciones de monedero dependen de los nodos de Bitcoin para interactuar con la cadena de bloques de Bitcoin. Estas aplicaciones calculan el saldo de los productos no utilizados (UTXOs) para un conjunto determinado de direcciones, firman y envían transacciones a la red de Bitcoin y recuperan datos sobre transacciones históricas.

La siguiente es una muestra de algunos de los JSON de Bitcoin RPCs que Amazon Managed Blockchain (AMB) Access Bitcoin admite para las transacciones de monederos de BTC:

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

Para obtener más información, consulte Compatible con JSON- RPCs.

Analice la actividad en la cadena de bloques de Bitcoin

Puede analizar el volumen de actividad de las transacciones en la cadena de bloques de Bitcoin mediante el método `getchaintxstats` JSON-RPC. Este JSON-RPC te permite acceder a métricas como las tasas medias de transacciones por segundo, el recuento total de transacciones, el recuento de bloques, etc. Si lo desea, también puede definir una ventana de números de bloque o un hash de bloques como delimitador para calcular estas estadísticas para un conjunto específico de bloques de la red.

Para obtener más información, consulte Compatible con JSON- RPCs.

Verifica los mensajes firmados con un key pair de Bitcoin

Las carteras de Bitcoin tienen una clave privada y una clave pública que forman un key pair. Estas claves se utilizan para firmar transacciones y sirven como identidad del usuario en la cadena de bloques. La clave pública se utiliza para crear direcciones, que son identificadores alfanuméricos estandarizados (de 27 a 34 caracteres). Estas direcciones se utilizan para recibir salidas de BTC y gestionar transacciones o mensajes.

Con una cartera de Bitcoin, los usuarios también pueden firmar y verificar los mensajes criptográficamente. Este proceso suele utilizarse para demostrar la propiedad de una dirección de monedero específica y del BTC asociado a ella. Al utilizar el JSON-RPC de `verifymessage` Bitcoin, puedes comprobar la autenticidad y validez de un mensaje firmado por otro monedero. En concreto, se puede usar un nodo de Bitcoin para verificar si un mensaje se ha firmado con la clave privada correspondiente a la dirección derivada de la clave pública proporcionada en el propio mensaje firmado.

Para obtener más información, consulte Compatible con JSON- RPCs.

Inspecciona el repositorio de notas de Bitcoin

Muchas aplicaciones necesitan acceder al mempool para realizar un seguimiento de las transacciones pendientes, obtener una lista de todas las transacciones pendientes o averiguar el origen de una transacción. Para ello, existen bitcoins RPCs tipo JSON `getmempoolancestorsgetmempoolentry`, y `getrawmempool` que admiten esta actividad. Estas aplicaciones de Bitcoin JSON RPCs ayudan a obtener la información que necesitan del mempool.

Amazon Managed Blockchain (AMB) Access Bitcoin también es compatible con el `testmempoolaccept` Bitcoin JSON-RPCs, que le permite verificar si una transacción cumple con

las reglas del protocolo y si un nodo la aceptaría antes de enviarla. Las carteras, bolsas y cualquier otra entidad que envíe transacciones directamente a la cadena de bloques de Bitcoin utilizan estos Bitcoin JSON-. RPCs

Para obtener más información, consulte Compatible con JSON- RPCs.

Compatible con Bitcoin JSON: RPCs con Amazon Managed Blockchain (AMB) Acceda a Bitcoin

En este tema, se proporciona una lista y referencias al JSON de Bitcoin compatible con Managed BlockchainRPCs . Cada JSON-RPC compatible incluye una breve descripción de su uso.

Note

- Puedes autenticar Bitcoin con JSON RPCs en una cadena de bloques gestionada mediante el proceso de firma de la versión 4 (SiGv4). Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden interactuar con ella mediante el JSON- de Bitcoin. RPCs Proporcione AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.
- Si la respuesta HTTP supera los 10 MB, aparecerá un error. Para corregir esto, debes configurar los encabezados de compresión en. `Accept-Encoding:gzip` La respuesta comprimida que recibe su cliente contiene los siguientes encabezados: `Content-Type: application/json` y. `Content-Encoding: gzip`
- Amazon Managed Blockchain (AMB) Access Bitcoin genera un error 400 cuando las solicitudes JSON-RPC tienen un formato incorrecto.
- Usa el `sendrawtransaction` JSON-RPC para enviar transacciones que actualicen el estado de la cadena de bloques de Bitcoin.
- AMB Access Bitcoin tiene un límite de solicitudes predeterminado de 100 solicitudes por segundo (RPS), por región. `NETWORK_TYPE` AWS

  Para aumentar su cuota, debe ponerse en contacto con AWS el servicio de asistencia. Para ponerse en contacto con el servicio de AWS asistencia, inicie sesión en la consola del AWS Support Center. Seleccione Crear caso. Elija Técnico. Elija Managed Blockchain como su servicio. Elija Access:Bitcoin como su categoría y las instrucciones generales como su gravedad. Introduzca la cuota de RPC como asunto y, en el cuadro de texto de descripción, indique los límites de cuota aplicables a sus necesidades en RPS por red de Bitcoin y región. Envíe su caso.

Compatible con JSON- RPCs

AMB Access Bitcoin es compatible con el siguiente código JSON- de Bitcoin. RPCs Cada llamada admitida tiene una breve descripción de su uso.

Categoría	JSON-RPC	Descripción
Cadena de bloques RPCs	obtener el mejor hash de bloque	Devuelve el hash del mejor bloque (de consejos) de la cadena más trabajada y totalmente validada.
	getblock	Si la verbosidad es 0, devuelve una cadena con datos serializados y codificados en hexadecimal para el bloque 'hash'. Si la verbosidad es 1, devuelve un objeto con información sobre el bloque «hash». Si el nivel de verbosidad es 2, devuelve un objeto con información sobre el «hash» del bloque e información sobre cada transacción. Si el nivel de verbosidad es 3, devuelve un objeto con información sobre el «hash» del bloque e información sobre cada transacción, incluida la información de las `prevout` entradas.
	getblockchaininfo	Devuelve un objeto que contiene información de estado diversa relacionada con el procesami ento de la cadena de bloques.
	getblockcount	Devuelve la altura de la cadena más trabajada y totalmente validada. El bloque génesis tiene una altura de 0.
	getblock filter	Recupera un filtro de contenido BIP 157 para un bloque en particular mediante el hash del bloque.
	getblockhash	Devuelve el hash del bloque con la best-block-chain altura indicada.

Categoría	JSON-RPC	Descripción
	getblockheader	Si verbose es falso, devuelve una cadena con datos serializados y codificados en hexadecim al para el encabezado de bloque «hash». Si verbose es verdadero, devuelve un objeto con información sobre el encabezado de bloque «hash».
	getblockstats	Calcula las estadísticas por bloque para una ventana determinada. Todas las cantidades están en satoshis. No funcionará en algunas alturas con la poda.
	consigue puntas de cadena	Devuelve información sobre todas las puntas conocidas del árbol de bloques, incluida la cadena principal y las ramas huérfanas.
	getchaintx stats	Calcula las estadísticas sobre el número total y la tasa de transacciones de la cadena.
	tener dificultades	Devuelve la proof-of-work dificultad como un múltiplo de la dificultad mínima.
	getmempool ancestros	Si txid está en el mempool, devuelve todos los antepasados del mempool.
	los descendientes de getmempool	Si txid está en el mempool, devuelve todos los descendientes del mempool.
	getmempool entry	Devuelve los datos de mempool de una transacción determinada.
	getmempoolinfo	Devuelve detalles sobre el estado activo del pool de memoria TX.

Categoría	JSON-RPC	Descripción
	getrawmempool	Devuelve todas las transacciones del pool IDs de memoria como una matriz JSON de transacciones de cadenas. IDs **Note** `verbose = true` no se admite.
	gettxout	Devuelve detalles sobre el resultado de una transacción no utilizada.
	getxoutproof	Devuelve una prueba codificada en hexadecimal de que se incluyó «txid» en un bloque.
Transacciones sin procesar RPCs	crear una transacción sin procesar	Crea una transacción gastando las entradas dadas y creando nuevas salidas.
	decodificar una transacción sin procesar	Devuelve un objeto JSON que representa la transacción serializada y codificada en hexadecimal.
	decodificar	Decodifica un script codificado en hexadecimal.
	obtener una transacción sin procesar	Devuelve los datos brutos de la transacción.
	envía una transacción sin procesar	Envía una transacción sin procesar (serializada, codificada en hexadecimal) al nodo y la red locales.
	testmempool accept	Devuelve el resultado de las pruebas de aceptación de mempool, que indican si mempool aceptaría una transacción sin procesar (serializada, codificada en hexadecimal). Esto comprueba si la transacción infringe el consenso o las reglas políticas.

Categoría	JSON-RPC	Descripción
Util RPCs	crear multisig	Crea una dirección con múltiples firmas sin necesidad de firmar mis claves.
	Calcule la tarifa inteligente	Calcula la tarifa aproximada por kilobyte necesaria para que una transacción comience a confirmarse dentro de los bloques conf_target, si es posible, y devuelve el número de bloques para los que la estimación es válida. Utiliza el tamaño de la transacción virtual, tal como se define en el BIP 141 (no se incluyen los datos de los testigos).
	valida la dirección	Devuelve información sobre la dirección de bitcoin proporcionada.
	verifica el mensaje	Verifica un mensaje firmado.

Seguridad en Amazon Managed Blockchain (AMB) Access Bitcoin

La seguridad en la nube AWS es de máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon Managed Blockchain (AMB) Access Bitcoin, consulte AWS Services in Scope by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Para proporcionar protección de datos, autenticación y control de acceso, Amazon Managed Blockchain utiliza AWS características y características del marco de código abierto que se ejecuta en Managed Blockchain.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar AMB Access Bitcoin. Los siguientes temas le muestran cómo configurar AMB Access Bitcoin para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Bitcoin de AMB Access.

Temas

Protección de datos en Amazon Managed Blockchain (AMB) Access Bitcoin

El modelo de se aplica a protección de datos en Amazon Managed Blockchain (AMB) Access Bitcoin. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato

libre, tales como el campo Nombre. Esto incluye cuando trabaja con AMB Access Bitcoin u otro Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

El cifrado de datos ayuda a evitar que usuarios no autorizados lean datos de una red blockchain y de los sistemas de almacenamiento de datos asociados. Esto incluye los datos que podrían interceptarse a medida que viajan por la red, lo que se conoce como datos en tránsito.

Cifrado en tránsito

De forma predeterminada, Managed Blockchain utiliza una conexión HTTPS/TLS para cifrar todos los datos que se transmiten desde un ordenador cliente que ejecuta los puntos finales del servicio. AWS CLI AWS

No es necesario hacer nada para habilitar el uso de HTTPS/TLS. Siempre está habilitada, a menos que la inhabilites explícitamente para un AWS CLI comando individual mediante el comando. `--no-verify-ssl`

Gestión de identidad y acceso para Amazon Managed Blockchain (AMB) Access Bitcoin

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Bitcoin de AMB Access. El IAM es un servicio Servicio de AWS que puede utilizar sin coste adicional.

Temas

- Cómo funciona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM
- Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin
- Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access a Bitcoin

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access a Bitcoin).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se

recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM

Antes de utilizar IAM para gestionar el acceso a AMB Access Bitcoin, infórmese sobre las funciones de IAM disponibles para su uso con AMB Access Bitcoin.

Funciones de IAM que puede utilizar con Amazon Managed Blockchain (AMB) Access Bitcoin

Característica de IAM	Soporte de AMB Access para Bitcoin
Políticas basadas en identidades	Sí

Característica de IAM	Soporte de AMB Access para Bitcoin
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	No
Permisos de entidades principales	No
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo funcionan AMB Access Bitcoin y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad de AMB Access Bitcoin

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones.

Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AMB Access Bitcoin

Para ver ejemplos de políticas basadas en la identidad de AMB Access Bitcoin, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

Políticas basadas en recursos en AMB Access Bitcoin

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AMB Access Bitcoin

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AMB Access Bitcoin, consulte Acciones definidas por Amazon Managed Blockchain (AMB) Access Bitcoin en la Referencia de autorización de servicio.

Las acciones políticas de AMB Access Bitcoin utilizan el siguiente prefijo antes de la acción:

```
managedblockchain:
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `InvokeRpcBitcoin`, incluya la siguiente acción:

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

Para ver ejemplos de políticas de AMB Access basadas en la identidad de Bitcoin, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

Recursos de políticas para AMB Access Bitcoin

Compatibilidad con recursos de políticas: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de AMB Access Bitcoin y sus correspondientes ARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Access Bitcoin en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon Managed Blockchain (AMB) Access Bitcoin.

Para ver ejemplos de políticas basadas en la identidad de AMB Access Bitcoin, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

Claves de condición de la política de AMB Access Bitcoin

Compatibilidad con claves de condición de políticas específicas del servicio: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de AMB Access Bitcoin, consulte Claves de condición para Amazon Managed Blockchain (AMB) Access Bitcoin en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon Managed Blockchain (AMB) Access Bitcoin.

Para ver ejemplos de políticas basadas en la identidad de AMB Access Bitcoin, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

ACLs en AMB Access Bitcoin

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AMB Access Bitcoin

Compatibilidad con ABAC (etiquetas en las políticas): no

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AMB Access Bitcoin

Compatible con el uso de credenciales temporales: no

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos principales entre servicios para AMB Access Bitcoin

Compatibilidad con sesiones de acceso directo (FAS): no

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama y Servicio de AWS, además, la que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para AMB Access Bitcoin

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AMB Access Bitcoin. Edite las funciones de servicio solo cuando AMB Access Bitcoin le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para AMB Access Bitcoin

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AMB Access Bitcoin. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AMB Access Bitcoin, incluido el formato de cada uno de los tipos de recursos, consulte Actions, Resources and Condition Keys for Amazon Managed Blockchain (AMB) Access Bitcoin en la Referencia de autorización de servicios. ARNs

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola Bitcoin de AMB Access
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceder a las redes de Bitcoin

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear los recursos de AMB Access Bitcoin de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola Bitcoin de AMB Access

Para acceder a la consola Amazon Managed Blockchain (AMB) Access Bitcoin, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Bitcoin de AMB Access que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola AMB Access Bitcoin, adjunte también la política *ReadOnly* AWS gestionada *ConsoleAccess* o la política gestionada de AMB Access a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la 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": "*"
        }
    ]
}
```

Acceder a las redes de Bitcoin

> **Note**
>
> Para acceder a los puntos finales públicos de Bitcoin `mainnet` y `testnet` realizar llamadas JSON-RPC, necesitará credenciales de usuario (`AWS_ACCESS_KEY_IDyAWS_SECRET_ACCESS_KEY`) disponer de los permisos de IAM adecuados para AMB Access Bitcoin.

Example Política de IAM para acceder a todas las redes de Bitcoin

En este ejemplo, se concede a un usuario de IAM el Cuenta de AWS acceso a todas las redes de Bitcoin.

JSON

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

Example Política de IAM para acceder a la red Bitcoin Testnet

En este ejemplo, se concede a un usuario de IAM el Cuenta de AWS acceso a la red de Bitcoin. `testnet`

JSON

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

Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access a Bitcoin

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AMB Access, Bitcoin e IAM.

Temas

No estoy autorizado a realizar ninguna acción en AMB Access Bitcoin

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `managedblockchain::`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `managedblockchain::`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a AMB Access Bitcoin.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AMB Access Bitcoin. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir la función al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AMB Access Bitcoin

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AMB Access Bitcoin admite estas funciones, consulte. Cómo funciona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro Cuenta de AWS de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro de eventos de Amazon Managed Blockchain (AMB) Acceda a Bitcoin mediante AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin no admite eventos de administración.

Amazon Managed Blockchain está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Managed Blockchain. CloudTrail captura quién invocó los puntos finales de AMB Access Bitcoin para Managed Blockchain como eventos del plano de datos.

Si crea una ruta correctamente configurada que esté suscrita para recibir los eventos del plano de datos deseados, podrá recibir la entrega continua de los eventos relacionados con Bitcoin de AMB Access a CloudTrail un bucket de Amazon S3. Con la información recopilada por ellos CloudTrail, puede determinar si se ha realizado una solicitud a uno de los puntos de conexión de AMB Access Bitcoin, la dirección IP de la que procede la solicitud, quién la ha realizado, cuándo se ha realizado y otros detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

AMB Acceda a la información sobre Bitcoin en CloudTrail

AWS CloudTrail está activado de forma predeterminada al crear su. Cuenta de AWS Sin embargo, para ver quién invocó los puntos finales de AMB Access Bitcoin, debe configurarlos CloudTrail para que registren los eventos del plano de datos.

Para mantener un registro continuo de los eventos en su cuenta Cuenta de AWS, incluidos los eventos del plano de datos de AMB Access Bitcoin, debe crear un registro. Un rastro hace que los archivos de registro se CloudTrail entreguen a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en el Consola de administración de AWS, la ruta se aplica a todos Regiones de AWS. La ruta registra los eventos de todas las regiones compatibles en la AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo estos datos y actuar en función de los datos de eventos recopilados en los CloudTrail registros. Para más información, consulte los siguientes temas:

- Se usa CloudTrail para rastrear Bitcoin JSON- RPCs
- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Al analizar los eventos de CloudTrail los datos, puede controlar quién invocó los puntos finales de AMB Access Bitcoin.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas del archivo de registro de Bitcoin de AMB Access

En el caso de los eventos del plano de datos, un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de S3 específico. Cada archivo de CloudTrail registro contiene una o más entradas de registro que representan una única solicitud de cualquier fuente. Estas entradas proporcionan detalles sobre la acción solicitada, incluidas la fecha y la hora de la acción, y cualquier parámetro de solicitud asociado.

> **Note**
>
> CloudTrail Los eventos de datos de los archivos de registro no son un rastreo ordenado de las llamadas a la API Bitcoin de AMB Access, por lo que no aparecen en ningún orden específico.

Se usa CloudTrail para rastrear Bitcoin JSON- RPCs

Puede utilizarlo CloudTrail para rastrear quién de su cuenta invocó los puntos finales de AMB Access Bitcoin y qué JSON-RPC se invocó como eventos de datos. De forma predeterminada, al crear un registro, los eventos de datos no se registran. Para registrar quién invocó los puntos finales de AMB Access Bitcoin como eventos de CloudTrail datos, debe añadir explícitamente a un registro los recursos o tipos de recursos compatibles para los que desea recopilar la actividad. Amazon Managed Blockchain admite la adición de eventos de datos mediante el Consola de administración de AWS AWS SDK y AWS CLI. Para obtener más información, consulte Registrar eventos mediante selectores avanzados en la Guía del AWS CloudTrail usuario.

Para registrar los eventos de datos en una ruta, utilice la put-event-selectorsoperación después de crear la ruta. Utilice la `--advanced-event-selectors` opción para especificar los tipos de `AWS::ManagedBlockchain::Network` recursos para empezar a registrar los eventos de datos y determinar quién invocó los puntos finales de AMB Access Bitcoin.

Example Entrada en el registro de eventos de datos de todas las solicitudes de puntos finales de AMB Access Bitcoin de su cuenta

En el siguiente ejemplo, se muestra cómo utilizar la `put-event-selectors` operación para registrar todas las solicitudes de puntos finales de AMB Access Bitcoin de su cuenta para el seguimiento de la `my-bitcoin-trail` región. `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"] } ]}]'
```

Después de suscribirse, puede realizar un seguimiento del uso en el depósito de S3 que está conectado a la ruta especificada en el ejemplo anterior.

El siguiente resultado muestra una entrada en el registro de eventos de CloudTrail datos con la información recopilada por CloudTrail. Puede determinar si se ha realizado una solicitud JSON-RPC de Bitcoin a uno de los puntos finales de AMB Access Bitcoin, la dirección IP de la que procede la solicitud, quién la ha realizado, cuándo se ha realizado y otros detalles adicionales.

```
{
        "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"
}
```

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.