aws

Guía para desarrolladores

AMBAccede a Bitcoin

AMBAccede 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) Acceda a Bitcoin
- Casos de uso de Bitcoin con Amazon Managed Blockchain (AMB) Access Bitcoin
- Los JSON-RPC de Bitcoin compatibles con Amazon Managed Blockchain (AMB) Access 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). Puede invocar los RPC JSON de Bitcoin para comunicarse con los nodos de Bitcoin gestionados por Managed Blockchain e interactuar con las redes de Bitcoin. Con los JSON-RPC de Bitcoin, 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**
>
> Usted es responsable de crear, mantener, usar y administrar sus 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	Región
Este de EE. UU. (Norte de Virginia)	IAD	`us-east-1`
Asia-Pacífico (Tokio)	NRT	ap-northeast-1
Asia-Pacífico (Seúl)	ICONO	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 finales del servicio de 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 a los JSON-RPC de Bitcoin 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 los JSON-RPC individuales de Bitcoin.
- 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 sus JSON-RPC de Bitcoin. 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 un AWS account. En el siguiente capítulo, se explica cómo empezar a utilizar AMB Access Bitcoin.

Requisitos y consideraciones previos

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

Registrarse en AWS

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

Si tienes un Cuenta de AWS ya, vaya al siguiente paso. Si no tienes un Cuenta de AWS, utilice el procedimiento siguiente para crear uno.

Para crear un 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 e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, un Usuario raíz de la cuenta de AWSse crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la 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 IAM usuario con los permisos adecuados

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

Solo IAM los directores pueden realizar RPC llamadas con BitcoinJSON. Al realizar llamadas a BitcoinJSON, RPCs en Amazon Managed Blockchain, puedes hacerlo a través de una HTTPS conexión autenticada mediante el proceso de firma Signature Version 4. Esto significa que solo IAM los directores autorizados del AWS la cuenta puede realizar RPC llamadas en BitcoinJSON. Para ello, AWS Las credenciales (un identificador de clave de acceso y una clave de acceso secreta) deben proporcionarse con la llamada.

Para obtener información sobre cómo crear un IAM usuario, consulte Crear un IAM usuario en su AWS cuenta. Para obtener más información sobre cómo adjuntar una política de permisos a un usuario, consulte Cambiar los permisos de un IAM usuario. Para ver un ejemplo de una política de permisos que puede usar para conceder permiso a un usuario para que trabaje con AMB Access Bitcoin, consulteEjemplos 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 última AWS Interfaz de línea de comandos (CLI) con la que trabajar AWS recursos de una terminal. Para obtener más información, consulte Instalación o actualización de la última versión del AWS CLI.

> **Note**
>
> Para CLI acceder, necesita un identificador 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 de la Guía IAM del usuario.

Primeros pasos con Amazon Managed Blockchain (AMB) Acceda a 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 AMB utiliza 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 IAM política para acceder a Bitcoin - JSON RPCs
- Realice solicitudes de llamada a procedimientos remotos de Bitcoin (RPC) en el RPC editor de AMB Access mediante el AWS Management Console
- Haga que AMB Access Bitcoin JSON RPC solicite en awscurl utilizando el AWS CLI
- Realice RPC solicitudes de Bitcoin JSON en Node.js
- Usa AMB Access Bitcoin en lugar de AWS PrivateLink

Cree una IAM política 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 JSON RPC llamadas, debe tener credenciales de usuario (AWS_ACCESS_ KEY _ID y _ AWS_SECRET ACCESS _KEY) que tengan los IAM permisos adecuados para Amazon Managed Blockchain (AMB) Access Bitcoin. En una terminal con AWS CLI instalado, ejecute el siguiente comando para crear una IAM política que permita acceder a los dos puntos finales 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 IAM usuario para que surta efecto. En el navegador AWS Management Console, navegue hasta el IAM servicio y adjunte la política `AmazonManagedBlockchainBitcoinAccess` al rol asignado a su IAM usuario. Para obtener más información, consulte Crear un rol y asignarlo a un IAM usuario.

Realice solicitudes de llamada a procedimientos remotos de Bitcoin (RPC) en el RPC editor de AMB Access mediante el AWS Management Console

Puede editar y enviar llamadas a procedimientos remotos (RPCs) en el AWS Management Console mediante AMB Access. Con ellasRPCs, puede leer datos, escribir y enviar transacciones en la red Bitcoin.

Example

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

1. Abre la consola de Managed Blockchain en https://console.aws.amazon.com/managedblockchain/.
2. Elija el RPCeditor.
3. En la sección Solicitud, elige `BITCOIN_MAINNET` como Blockchain Network.
4. Elija `getblock` como RPCmétodo.
5. Introduzca `00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09` como número de bloque y elija `0` como verbosidad.
6. A continuación, seleccione Submit (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 RPCspágina compatible con AMB Access Bitcoin

Haga que AMB Access Bitcoin JSON RPC solicite en awscurl utilizando el AWS CLI

Example

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

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 el AWS CLI, sus credenciales IAM de usuario y su AWS región predeterminada están configuradas en su entorno y tienen acceso a awscurl. Con awscurl, envíe una solicitud tanto a la red principal como a la red de pruebas de Bitcoin invocando la. `getblock` RPC 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` Puedes sustituirlo por tu Bitcoin preferidoJSON, RPC y AWS Región compatible con Amazon Managed Blockchain (AMB) Access Bitcoin. Además, puede realizar una solicitud en la red Testnet, en lugar de en la red principal, `mainnet` sustituyéndola por `testnet` en el 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
```

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 RPC solicitudes de Bitcoin JSON en Node.js

Puede enviar solicitudes firmadas utilizando el módulo https nativo de Node.js HTTPS para acceder a los puntos finales de la red principal y la red de pruebas de Bitcoin y realizar JSON RPC API llamadas con el módulo https nativo de, o puede utilizar una biblioteca de terceros, como. AXIOS En el siguiente ejemplo, se muestra cómo realizar una RPC solicitud de Bitcoin a los JSON 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 de conexión 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 IAM usuario.

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

Tras completar todos los requisitos previos, copie el siguiente `package.json` archivo y `index.js` script en su entorno local mediante el 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 RPC solicitudes al punto final de Bitcoin y las firma con los encabezados correspondientes de la versión 4 de firma (SiGv4) utilizando el código oficial AWS SDKherramientas de la versión 3. Para ejecutar el código, abre una 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":"0000000000000000000000000000000000000000000000000003e903e903e9",
    "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 Haga que AMB Access Bitcoin JSON RPC solicite en awscurl utilizando el AWS CLI ejemplo. Para realizar otras llamadas, modifique el `rpc` objeto del script con un Bitcoin JSON - diferenteRPC. Puedes cambiar la opción de propiedad anfitriona a Bitcoin `testnet` para realizar llamadas en ese punto final.

Usa AMB Access Bitcoin en lugar de AWS PrivateLink

AWS PrivateLink es una tecnología escalable y de alta disponibilidad que puede utilizar para conectarse VPC a sus servicios de forma privada como si estuvieran en el suyoVPC. No tiene que usar una puerta de enlace de Internet, un NAT dispositivo, una dirección IP pública, AWS Conexión Direct Connect, o AWS VPNConexión de sitio a sitio para comunicarse con el servicio desde sus subredes privadas. Para obtener más información acerca de AWS PrivateLink o para configurar AWS PrivateLink, consulte ¿Qué es AWS PrivateLink?

Puedes enviar RPC solicitudes de AMB acceso a Bitcoin a través de JSON AWS PrivateLink mediante un VPC punto final. 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 Acceso AWS servicios a través de AWS PrivateLink.

Para el nombre del servicio, busca Amazon Managed Blockchain en la AWS columna de servicio. Para obtener más información, consulte AWS 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 mercancía y 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 las salidas no utilizadas (UTXO) de un conjunto determinado de direcciones, firman y envían transacciones a la red de Bitcoin y recuperan datos sobre el historial de transacciones.

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

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

Para obtener más información, consulte JSON-RPC compatibles.

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 JSON-RPC compatibles.

Verificar 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 JSON-RPC compatibles.

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 JSON-RPC de Bitcoin tipo `getmempoolancestorsgetmempoolentry`, y `getrawmempool` que admiten esta actividad. Estos JSON-RPC de Bitcoin ayudan a las aplicaciones a obtener la información que necesitan del mempool.

Amazon Managed Blockchain (AMB) Access Bitcoin también es compatible con el JSON-RPC de `testmempoolaccept` Bitcoin, 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 JSON-RPC de Bitcoin.

Para obtener más información, consulte JSON-RPC compatibles.

Los JSON-RPC de Bitcoin compatibles con Amazon Managed Blockchain (AMB) Access Bitcoin

En este tema se proporciona una lista y referencias a los JSON-RPC de Bitcoin compatibles con Managed Blockchain. Cada JSON-RPC compatible incluye una breve descripción de su uso.

Note

- Puedes autenticar los JSON-RPC de Bitcoin 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 los JSON-RPC de Bitcoin. 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. Elija 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.

JSON-RPC compatibles

AMB Access Bitcoin es compatible con los siguientes JSON-RPC de Bitcoin. Cada llamada admitida tiene una breve descripción de su uso.

Categoría	JSON-RPC	Descripción
RPC de cadena de bloques	obtén el mejor hash de bloques	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 hexadecimal 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. Todos los importes están expresados en satoshis. No funcionará en algunas alturas con la poda.
	consigue las puntas de las cadenas	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 todos los identificadores de transacción del pool de memoria como una matriz JSON de identificadores de transacciones en cadena. **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 (RPC)	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 una secuencia de comandos codificada 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.

Categoría	JSON-RPC	Descripción
	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.
Hasta RPC	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

La AWS modelo de responsabilidad compartida de se aplica a la 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. Usted es responsable de mantener el control sobre el contenido que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilices. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte la AWS Modelo de responsabilidad compartida y entrada de GDPR blog sobre AWS Blog de seguridad.

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS 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:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UtiliceSSL/TLSpara comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Trabajar con CloudTrail senderos en la AWS CloudTrail Guía del usuario.
- Uso AWS soluciones de cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS a través de una interfaz de línea de comandos oAPI, utilice un FIPS punto final. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma Federal de Procesamiento de Información (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 utilizando la consolaAPI, AWS CLI, o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Cifrado de datos

El cifrado de datos ayuda a evitar que usuarios no autorizados lean datos de una red de cadena de bloques 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 TLS conexiónHTTPS/para cifrar todos los datos que se transmiten desde un ordenador cliente que ejecuta el AWS CLI a AWS puntos finales de servicio.

No necesita hacer nada para habilitar el uso deHTTPS/TLS. Siempre está habilitada, a menos que la deshabilites explícitamente para una persona AWS CLI comando mediante el `--no-verify-ssl` comando.

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

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de AMB Access Bitcoin. IAMes un Servicio de AWS que puede utilizar sin coste adicional.

Temas

- 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

¿Cómo se usa AWS Identity and Access Management (IAM) varía según el trabajo que realice en AMB Access Bitcoin.

Usuario del servicio: si utiliza el servicio AMB Access Bitcoin para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AMB Access Bitcoin para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AMB Access Bitcoin, consulteSolución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access a Bitcoin.

Administrador de servicios: si está a cargo de los recursos de AMB Access Bitcoin en su empresa, probablemente tenga acceso total a AMB Access Bitcoin. Su trabajo consiste en determinar a qué funciones y recursos de AMB Access Bitcoin deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM AMB Access Bitcoin, consulteCómo funciona Amazon Managed Blockchain (AMB) Access Bitcoin con IAM.

IAMadministrador: si es IAM administrador, tal vez le interese obtener más información sobre cómo redactar políticas para administrar el acceso a AMB Access Bitcoin. Para ver ejemplos de políticas basadas en la identidad de AMB Access Bitcoin que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidad para Amazon Managed Blockchain (AMB) Access Bitcoin

Autenticación con identidades

La autenticación es la forma de iniciar sesión en AWS utilizando tus credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como IAM usuario o asumiendo un IAM rol.

Puede iniciar sesión en AWS como identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios de (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son

ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accedes AWS al usar la federación, está asumiendo un rol de manera indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en AWS Management Console o el AWS portal de acceso. Para obtener más información sobre cómo iniciar sesión en AWS, consulta Cómo iniciar sesión en tu Cuenta de AWS en la AWS Sign-In Guía del usuario.

Si accedes AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no usa AWS herramientas, debe firmar las solicitudes usted mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS APIsolicitudes en la Guía IAM del usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo: AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la AWS IAM Identity Center Guía del usuario y Uso de la autenticación multifactorial () MFA en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Al crear un Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todas Servicios de AWS y los recursos de la cuenta. Esta identidad se denomina Cuenta de AWS usuario root y se accede a él iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web, AWS Directory Service, el directorio del Centro de identidades o cualquier usuario que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de

identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para la administración centralizada del acceso, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todos sus Cuentas de AWS y aplicaciones. Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en el AWS IAM Identity Center Guía del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a un AWS CLI o AWS APIoperación o mediante una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la AWS IAM Identity Center Guía del usuario.
- Permisos de IAM usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para saber la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un Servicio de AWS. El servicio puede asumir la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y se están creando AWS CLI o AWS APIsolicitudes. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS Un rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia que se adjunte a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

Usted controla el acceso en AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto en AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden utilizar AWS JSONpolíticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre su función en el AWS Management Console, el AWS CLI, o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su Cuenta de AWS. Las políticas gestionadas incluyen AWS las políticas gestionadas y las políticas gestionadas por el cliente. Para saber cómo elegir entre una política gestionada o una política en línea, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAMusuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

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

Listas de control de acceso () ACLs

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

Amazon S3, AWS WAF, y Amazon VPC son ejemplos de servicios que admitenACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.
- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada múltiples Cuentas de AWS que es propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar las políticas de control de servicios (SCPs) a cualquiera de tus cuentas o a todas ellas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas todas Usuario raíz de la cuenta de AWS. Para obtener más información acerca de OrganizationsSCPs, consulte Políticas de control de servicios en AWS Organizations Guía del usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS determina si se permite una

solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

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

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

IAMfunciones que puedes usar con Amazon Managed Blockchain (AMB) Access Bitcoin

IAMcaracterística	AMBAcceda al soporte de Bitcoin
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No
ABAC(etiquetas en las 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 AMB acceder a Bitcoin y otros AWS los servicios funcionan con la mayoría de IAM las funciones, consulte AWS servicios con los que funcionan IAM en la Guía IAM del usuario.

Políticas basadas en la identidad para Access Bitcoin AMB

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en la identidad para Access Bitcoin AMB

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

Políticas basadas en recursos de Access Bitcoin AMB

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para

acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones políticas para AMB Access Bitcoin

Compatibilidad con las acciones de política: sí

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que las asociadas AWS APIoperación. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Recursos de políticas para Access Bitcoin AMB

Recursos de políticas compatibles: No

Los administradores pueden usar AWS JSONpolíticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 correspondientesARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Access Bitcoin en la referencia de autorización del servicio. Para saber con qué acciones puede especificar cada recurso, consulte Acciones definidas por Amazon Managed Blockchain (AMB) Access Bitcoin. ARN

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

Claves de condición de la política de Access AMB Bitcoin

Admite claves de condición de política específicas del servicio: No

Los administradores pueden usar AWS JSONpolíticas 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones

condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios `Condition` elementos en una declaración o varias claves en un solo `Condition` elemento, AWS los evalúa mediante una `AND` operación lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas AWS claves de condición globales, consulte AWS claves de contexto de condiciones globales en la Guía IAM del usuario.

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 Actions Defined by Amazon Managed Blockchain (AMB) Access Bitcoin.

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

ACLsen AMB Access Bitcoin

SoportaACLs: 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. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABACcon Access Bitcoin AMB

Soportes ABAC (etiquetas en las políticas): No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchas AWS recursos. Etiquetar entidades

y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

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 al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con Access Bitcoin AMB

Admite credenciales temporales: no

Alguno Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluyendo qué Servicios de AWS trabaje con credenciales temporales, consulte Servicios de AWS que funcionan IAM en la Guía IAM del usuario.

Está utilizando credenciales temporales si inicia sesión en AWS Management Console utilizando cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de su empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente mediante el AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. 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.

Permisos principales entre servicios para AMB Access Bitcoin

Admite sesiones de acceso directo (FAS): No

Cuando utiliza un IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

Funciones de servicio de AMB Access Bitcoin

Compatible con roles de servicio: No

Una función de servicio es una IAMfunción que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. 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 proporcione instrucciones para hacerlo.

Funciones vinculadas al servicio para Access Bitcoin AMB

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 la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte AWS servicios con los que funcionan. 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. Tampoco pueden realizar tareas mediante el AWS Management Console, AWS Command Line Interface (AWS CLI), o AWS API. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

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 del servicio. ARNs

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AMB Access Bitcoin de su cuenta. Estas acciones pueden suponer costes para su Cuenta de AWS. Al crear o editar políticas basadas en la identidad, siga estas directrices y recomendaciones:

- Comience con AWS políticas gestionadas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice la AWS políticas gestionadas que conceden permisos para muchos casos de uso habituales. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo AWS políticas gestionadas por el cliente que sean específicas para sus casos de uso. Para obtener más

información, consulte AWS políticas gestionadas o AWS políticas gestionadas para las funciones laborales en la Guía IAM del usuario.

- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puede utilizar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de un procedimiento específico Servicio de AWS, como, por ejemplo, AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si tiene un escenario que requiere IAM usuarios o un usuario raíz en su Cuenta de AWS, actívala MFA para mayor seguridad. Para solicitarlo MFA cuando se cancelen API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

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

Uso de la consola AMB Access Bitcoin

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 AMB Access Bitcoin en su Cuenta de AWS. Si creas una política basada en la identidad que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades (usuarios o roles) que cuenten con esa política.

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

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

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante el AWS CLI o 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": "*"
        }
    ]
}
```

Acceder a las redes de Bitcoin

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

Example IAMPolítica de acceso a todas las redes de Bitcoin

Este ejemplo concede a un IAM usuario de su Cuenta de AWS acceso a todas las redes de Bitcoin.

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

Example IAMPolítica de acceso a la red Bitcoin Testnet

Este ejemplo concede a un IAM usuario de su Cuenta de AWS acceso a la `testnet` red Bitcoin.

```
{
    "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 para ayudarle a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AMB Access Bitcoin yIAM.

Temas

- No estoy autorizado a realizar ninguna acción en AMB Access Bitcoin
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de AMB Access Bitcoin

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.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio pero no tiene los `managedblockchain::`*`GetWidget`* permisos ficticios.

```
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 necesitas ayuda, ponte en contacto con tu 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.

Alguno 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 el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar 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 el rol 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 mi Cuenta de AWS para acceder a mis recursos de AMB Access Bitcoin

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. 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 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 sus recursos en Cuentas de AWS que te pertenezca, consulta Proporcionar acceso a un IAM usuario en otro Cuenta de AWS que le pertenezca en la Guía IAM del usuario.
- Para obtener información sobre cómo proporcionar acceso a sus recursos a terceros Cuentas de AWS, consulte Proporcionar acceso a Cuentas de AWS propiedad de terceros en la Guía IAM del usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. 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 AWS Management Console, 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 utiliza CloudTrail para rastrear los JSON-RPC de Bitcoin
- 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 lo 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 CloudTrail UserIdentity.

Descripción de las entradas de los archivos 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 utiliza CloudTrail para rastrear los JSON-RPC de Bitcoin

Puede usarlo 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 AWS Management Console 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.