aws

Guide du développeur

AMB Access Bitcoin

AMB Access Bitcoin: Guide du développeur

Table of Contents

Qu'est-ce qu'Amazon Managed Blockchain (AMB) Access Bitcoin ?

Amazon Managed Blockchain (AMB) Access vous fournit des nœuds de blockchain publics pour Ethereum et Bitcoin, et vous pouvez également créer des réseaux de chaînes de blocs privés avec le framework Hyperledger Fabric. Choisissez parmi différentes méthodes pour interagir avec les blockchains publiques, notamment les opérations d'API multi-locataires entièrement gérées, à locataire unique (dédiées) et sans serveur vers des nœuds de blockchain publics. Pour les cas d'utilisation où les contrôles d'accès sont importants, vous pouvez choisir parmi des réseaux de blockchain privés entièrement gérés. Les opérations d'API standardisées vous offrent une évolutivité instantanée sur une infrastructure résiliente et entièrement gérée, afin que vous puissiez créer des applications blockchain.

AMB Access vous propose deux types distincts de services d'infrastructure blockchain : les opérations d'API d'accès au réseau blockchain multi-locataires et les nœuds et réseaux blockchain dédiés. Avec une infrastructure blockchain dédiée, vous pouvez créer et utiliser des nœuds de blockchain Ethereum publics et des réseaux de blockchain privés Hyperledger Fabric pour votre propre usage. Les offres multi-locataires basées sur des API, telles que AMB Access Bitcoin, sont toutefois composées d'une flotte de nœuds Bitcoin derrière une couche d'API où l'infrastructure de nœuds blockchain sous-jacente est partagée entre les clients.

Le Bitcoin est un réseau de blockchain décentralisé qui permet des peer-to-peer transactions sécurisées de valeur libellées dans la cryptomonnaie native du réseau, le Bitcoin (BTC). Le réseau Bitcoin est utilisé par les particuliers, les institutions financières, les entreprises de technologie financière, les gouvernements, etc. Le réseau Bitcoin est un moyen d'échange, une matière première d'investissement ou un registre immuable et vérifiable publiquement pour les données inscrites. Avec Amazon Managed Blockchain (AMB) Access Bitcoin, vous pouvez accéder à un pool de réseaux Bitcoin Mainnet et Testnet via des points de terminaison régionaux, via lesquels vous pouvez écrire des transactions, lire les données du registre et invoquer des requêtes JSON-RPC disponibles sur le client du nœud Bitcoin Core. Avec les points de terminaison Bitcoin sans serveur, vous pouvez vous concentrer sur le développement de vos applications au lieu d'investir dans des tâches indifférenciées telles que le provisionnement, la maintenance et l'équilibrage de charge des nœuds Bitcoin. Que vous créiez un portefeuille Bitcoin, créiez un échange cryptographique ou analysiez les données de la blockchain Bitcoin, vous ne payez que pour les demandes que vous effectuez via les points de terminaison Bitcoin en utilisant AMB Access Bitcoin.

Utilisez-vous AMB Access Bitcoin pour la première fois ?

Si vous utilisez AMB Access Bitcoin pour la première fois, nous vous recommandons de commencer par lire les sections suivantes :

- Concepts clés : Amazon Managed Blockchain (AMB) Access Bitcoin
- Commencer à utiliser Amazon Managed Blockchain (AMB) Access Bitcoin
- Cas d'utilisation du Bitcoin avec Amazon Managed Blockchain (AMB) Access Bitcoin
- Bitcoin JSON pris en charge - RPCs avec Amazon Managed Blockchain (AMB) Access Bitcoin

Concepts clés : Amazon Managed Blockchain (AMB) Access Bitcoin

> **Note**
>
> Ce guide part du principe que vous connaissez les concepts essentiels au Bitcoin. Ces concepts incluent la décentralisation, les nœuds, les transactions proof-of-work, les portefeuilles, les clés publiques et privées, les réductions de moitié, etc. Avant d'utiliser Amazon Managed Blockchain (AMB) Access Bitcoin, nous vous recommandons de consulter la documentation relative au développement du Bitcoin et la section Mastering Bitcoin.

Amazon Managed Blockchain (AMB) Access Bitcoin vous fournit un accès sans serveur à la blockchain Bitcoin, sans que vous ayez à configurer et à gérer une quelconque infrastructure Bitcoin, y compris les nœuds. Vous pouvez utiliser ce service géré pour accéder aux réseaux Bitcoin rapidement et à la demande, réduisant ainsi votre coût global de possession.

L'AMB Access Bitcoin vous donne accès au réseau Bitcoin via des nœuds complets exécutant le client Bitcoin Core, la fonctionnalité du portefeuille étant désactivée et prenant en charge plusieurs appels JSON Remote Procedure (JSON-RPC). Vous pouvez invoquer Bitcoin JSON RPCs pour communiquer avec les nœuds Bitcoin gérés par Managed Blockchain afin d'interagir avec les réseaux Bitcoin. Avec le Bitcoin JSON-RPCs, vous pouvez lire des données et écrire des transactions, notamment interroger des données et soumettre des transactions aux réseaux Bitcoin en utilisant le service Amazon Managed Blockchain.

> **Important**
>
> Vous êtes responsable de la création, de la maintenance, de l'utilisation et de la gestion de vos adresses Bitcoin. Vous êtes également responsable du contenu de vos adresses Bitcoin. AWS n'est pas responsable des transactions déployées ou appelées à l'aide de nœuds Bitcoin sur Amazon Managed Blockchain.

Considérations et limites relatives à l'utilisation d'Amazon Managed Blockchain (AMB) Access Bitcoin

- Réseaux Bitcoin pris en charge

  AMB Access Bitcoin prend en charge les réseaux publics suivants :

  - Réseau principal : chaîne de blocs Bitcoin publique sécurisée par proof-of-work consensus et sur laquelle la cryptomonnaie Bitcoin (BTC) est émise et échangée. Les transactions sur Mainnet ont une valeur réelle (c'est-à-dire qu'elles entraînent des coûts réels) et sont enregistrées sur la blockchain publique.
  - Testnet —Le testnet est une blockchain Bitcoin alternative utilisée pour les tests. Les pièces Testnet sont séparées et distinctes du Bitcoin réel (BTC) et n'ont généralement aucune valeur.

  > **Note**
  >
  > Les réseaux privés ne sont pas pris en charge.

- Régions prises en charge

  Les régions prises en charge pour ce service sont les suivantes :

Nom de la région	Code	Région
USA Est (Virginie du Nord)	IAD	`us-east-1`
Asie-Pacifique (Tokyo)	NRT	ap-northeast-1
Asie-Pacifique (Séoul)	ICN	ap-northeast-2
Asie-Pacifique (Singapour)	SIN	ap-southeast-1
Europe (Irlande)	DUB	eu-west-1
Europe (Londres)	LHR	eu-west-2

- Points de terminaison de service

  Voici les points de terminaison de service pour AMB Access Bitcoin. Pour vous connecter au service, vous devez utiliser un point de terminaison qui inclut l'une des régions prises en charge.

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

  Par exemple : `mainnet.bitcoin.managedblockchain.eu-west-2.amazonaws.com`
- Minage non pris en charge

  AMB Access Bitcoin ne prend pas en charge le minage de bitcoins (BTC).
- Signature Version 4 Signature des appels Bitcoin JSON-RPC

  Lorsque vous appelez le Bitcoin JSON- RPCs sur Amazon Managed Blockchain, vous pouvez le faire via une connexion HTTPS authentifiée à l'aide du processus de signature Signature Version 4. Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent effectuer des appels Bitcoin JSON-RPC. Pour ce faire, des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) doivent être fournies avec l'appel.

  > **Important**
  >
  > - N'intégrez pas les informations d'identification du client dans les applications destinées aux utilisateurs.
  > - Vous ne pouvez pas utiliser les politiques IAM pour restreindre l'accès à un Bitcoin JSON- RPCs individuel.
- Seules les soumissions de transactions brutes sont prises en charge

  Utilisez le `sendrawtransaction` JSON-RPC pour soumettre des transactions qui mettent à jour l'état de la blockchain Bitcoin.
- AWS CloudTrail assistance à la journalisation

  Vous pouvez configurer CloudTrail pour enregistrer votre Bitcoin JSON-RPCs. Pour de plus amples informations, veuillez consulter Enregistrement d'Amazon Managed Blockchain (AMB) Accédez aux événements Bitcoin en utilisant AWS CloudTrail.

Configuration d'Amazon Managed Blockchain (AMB) Access Bitcoin

Avant d'utiliser Amazon Managed Blockchain (AMB) Access Bitcoin pour la première fois, suivez les étapes décrites dans cette section pour créer un AWS compte. Le chapitre suivant explique comment commencer à utiliser AMB Access Bitcoin.

Prérequis et considérations

Avant de l'utiliser AWS pour la première fois, vous devez disposer d'un Compte AWS.

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez AWS, vous êtes automatiquement Compte AWS inscrit à tous Services AWS, y compris à Amazon Managed Blockchain (AMB) Access Bitcoin. Seuls les services que vous utilisez vous sont facturés.

Si vous en avez Compte AWS déjà un, passez à l'étape suivante. Si vous n'avez pas de Compte AWS, utilisez la procédure suivante pour en créer un.

Pour créer un AWS compte

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Création d'un utilisateur IAM avec les autorisations appropriées

Pour créer et utiliser AMB Access Bitcoin, vous devez disposer d'un principal Gestion des identités et des accès AWS (IAM) (utilisateur ou groupe) doté des autorisations autorisant les actions nécessaires à la gestion de la blockchain.

Seuls les principaux IAM peuvent effectuer des appels Bitcoin JSON-RPC. Lorsque vous appelez le Bitcoin JSON- RPCs sur Amazon Managed Blockchain, vous pouvez le faire via une connexion HTTPS authentifiée à l'aide du processus de signature Signature Version 4. Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent effectuer des appels Bitcoin JSON-RPC. Pour ce faire, des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) doivent être fournies avec l'appel.

Pour plus d'informations sur la création d'un utilisateur IAM, consultez la section Création d'un utilisateur IAM dans votre AWS compte. Pour plus d'informations sur la façon d'associer une politique d'autorisations à un utilisateur, consultez la section Modification des autorisations d'un utilisateur IAM. Pour un exemple de politique d'autorisation que vous pouvez utiliser pour autoriser un utilisateur à travailler avec AMB Access Bitcoin, voirExemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin.

Installez et configurez AWS Command Line Interface

Si ce n'est pas déjà fait, installez la dernière interface de AWS ligne de commande (CLI) pour utiliser les AWS ressources d'un terminal. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.

> **Note**
>
> Pour accéder à la CLI, vous avez besoin d'un ID de clé d'accès et d'une clé d'accès secrète. Utilisation des informations d'identification temporaires au lieu des clés d'accès à long terme si possible. Les informations d'identification temporaires incluent un ID de clé d'accès, une clé d'accès secrète et un jeton de sécurité qui indique la date d'expiration des informations d'identification. Pour plus d'informations, consultez la section Utilisation d'informations d'identification temporaires avec AWS des ressources dans le Guide de l'utilisateur IAM.

Commencer à utiliser Amazon Managed Blockchain (AMB) Access Bitcoin

Utilisez les step-by-step didacticiels de cette section pour apprendre à effectuer des tâches à l'aide d'Amazon Managed Blockchain (AMB) Access Bitcoin. Ces exemples nécessitent que vous remplissiez certaines conditions préalables. Si vous utilisez AMB Access Bitcoin pour la première fois, consultez la section Configuration de ce guide pour vous assurer que vous avez rempli ces prérequis. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Managed Blockchain (AMB) Access Bitcoin.

Rubriques

- Créez une politique IAM pour accéder à Bitcoin JSON- RPCs
- Effectuez des demandes d'appel de procédure à distance (RPC) Bitcoin sur l'éditeur RPC AMB Access à l'aide du AWS Management Console
- Effectuez des requêtes JSON-RPC AMB Access Bitcoin dans awscurl en utilisant le AWS CLI
- Faites des requêtes Bitcoin JSON-RPC dans Node.js
- Utilisez AMB Access Bitcoin over AWS PrivateLink

Créez une politique IAM pour accéder à Bitcoin JSON- RPCs

Pour accéder aux points de terminaison publics du réseau principal Bitcoin et du réseau de test afin d'effectuer des appels JSON-RPC, vous devez disposer des informations d'identification utilisateur (AWS_ACCESS_KEY_ID et AWS_SECRET _ACCESS_KEY) dotées des autorisations IAM appropriées pour Amazon Managed Blockchain (AMB) Access Bitcoin. Dans un terminal sur lequel le AWS CLI est installé, exécutez la commande suivante pour créer une politique IAM permettant d'accéder aux deux points de terminaison Bitcoin :

```
cat <<EOT > ~/amb-btc-access-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AMBBitcoinAccessPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
EOT
aws iam create-policy --policy-name AmazonManagedBlockchainBitcoinAccess --policy-
document file://$HOME/amb-btc-access-policy.json
```

> **Note**
>
> L'exemple précédent vous donne accès à la fois au réseau principal Bitcoin et au réseau Testnet. Pour accéder à un point de terminaison spécifique, utilisez la `Action` commande suivante :
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

Après avoir créé la stratégie, associez-la au rôle de votre utilisateur IAM pour qu'elle prenne effet. Dans le AWS Management Console, accédez au service IAM et attachez la politique `AmazonManagedBlockchainBitcoinAccess` au rôle attribué à votre utilisateur IAM. Pour plus d'informations, consultez Création d'un rôle et attribution à un utilisateur IAM.

Effectuez des demandes d'appel de procédure à distance (RPC) Bitcoin sur l'éditeur RPC AMB Access à l'aide du AWS Management Console

Vous pouvez modifier et envoyer des appels de procédure à distance (RPCs) à l' AWS Management Console aide d'AMB Access. Grâce à ceux-ci RPCs, vous pouvez lire des données, écrire et soumettre des transactions sur le réseau Bitcoin.

Example

L'exemple suivant montre comment obtenir des informations sur le *`blockhash`*00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 à l'aide

du RPC. `getBlock` Remplacez les variables surlignées par vos propres entrées ou choisissez l'une des autres méthodes RPC répertoriées et entrez les entrées pertinentes requises.

1. Ouvrez la console Managed Blockchain à l'adresse https://console.aws.amazon.com/managedblockchain/.
2. Choisissez l'éditeur RPC.
3. Dans la section Demande, choisissez *`BITCOIN_MAINNET`* comme réseau Blockchain.
4. Choisissez *`getblock`* comme méthode RPC.
5. Entrez *`00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09`* comme numéro de bloc et choisissez *`0`* comme verbosité.
6. Choisissez ensuite Soumettre le RPC.
7. Vous trouverez les résultats dans la section Réponse de cette page. Vous pouvez ensuite copier les transactions brutes complètes pour une analyse plus approfondie ou pour les utiliser dans la logique métier de vos applications.

Pour plus d'informations, consultez le RPCs support d'AMB Access Bitcoin

Effectuez des requêtes JSON-RPC AMB Access Bitcoin dans awscurl en utilisant le AWS CLI

Example

Signez les demandes avec vos informations d'identification d'utilisateur IAM en utilisant Signature Version 4 (SigV4) afin de passer des appels Bitcoin JSON-RPC vers les points de terminaison Bitcoin AMB Access. L'outil de ligne de commande awscurl peut vous aider à signer des demandes adressées à des AWS services à l'aide de SigV4. Pour plus d'informations, consultez le fichier readme.md d'awscurl.

Installez awscurl en utilisant la méthode adaptée à votre système d'exploitation. Sur macOS, l'application recommandée HomeBrew est-elle la suivante :

```
brew install awscurl
```

Si vous avez déjà installé et configuré la AWS CLI, vos informations d'identification utilisateur IAM et votre région AWS par défaut sont définies dans votre environnement et ont accès à awscurl. À

l'aide d'awscurl, soumettez une demande au Bitcoin Mainnet et au Testnet en invoquant le RPC. `getblock` Cet appel accepte un paramètre de chaîne correspondant au hachage du bloc pour lequel vous souhaitez récupérer des informations.

La commande suivante extrait les données d'en-tête de bloc à partir du réseau principal Bitcoin en utilisant le hachage de bloc dans le `params` tableau pour sélectionner le bloc spécifique pour lequel récupérer les en-têtes. Cet exemple utilise le `us-east-1` point de terminaison. Vous pouvez le remplacer par votre Bitcoin JSON-RPC et votre AWS région préférés pris en charge par Amazon Managed Blockchain (AMB) Access Bitcoin. De plus, vous pouvez faire une demande sur le réseau Testnet, plutôt que sur le réseau principal, en `mainnet` remplaçant par `testnet` dans la commande.

```
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
```

Les résultats incluent des détails provenant des en-têtes des blocs et une liste des hachages de transactions inclus dans le bloc demandé. Consultez l'exemple suivant:

```
{"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"}
```

Faites des requêtes Bitcoin JSON-RPC dans Node.js

Vous pouvez envoyer des demandes signées en utilisant HTTPS pour accéder aux points de terminaison Bitcoin Mainnet et Testnet et pour effectuer des appels d'API JSON-RPC en utilisant le module https natif dans Node.js, ou vous pouvez utiliser une bibliothèque tierce telle qu'AXIOS.

L'exemple suivant vous montre comment envoyer une requête Bitcoin JSON-RPC aux points de terminaison Bitcoin AMB Access.

Example

Pour exécuter cet exemple de script Node.js, appliquez les conditions préalables suivantes :

1. Le gestionnaire de version de nœud (nvm) et Node.js doivent être installés sur votre machine. Vous trouverez les instructions d'installation pour votre système d'exploitation ici.
2. Utilisez la `node --version` commande et confirmez que vous utilisez la version 14 ou supérieure de Node. Si nécessaire, vous pouvez utiliser la `nvm install 14` commande, suivie de la `nvm use 14` commande, pour installer la version 14.
3. Les variables `AWS_ACCESS_KEY_ID` d'environnement `AWS_SECRET_ACCESS_KEY` doivent contenir les informations d'identification associées à votre compte. Les variables d'environnement `AMB_HTTP_ENDPOINT` doivent contenir vos points de terminaison AMB Access Bitcoin.

   Exportez ces variables sous forme de chaînes sur votre client à l'aide des commandes suivantes. Remplacez les valeurs surlignées dans les chaînes suivantes par les valeurs appropriées de votre compte utilisateur IAM.

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

Après avoir rempli toutes les conditions requises, copiez le `package.json` fichier et le `index.js` script suivants dans votre environnement local à l'aide de votre éditeur :

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();
```

L'exemple de code précédent utilise Axios pour envoyer des requêtes RPC au point de terminaison Bitcoin, et il signe ces demandes avec les en-têtes Signature Version 4 (SigV4) appropriés à l'aide des outils officiels AWS du SDK v3. Pour exécuter le code, ouvrez un terminal dans le même répertoire que vos fichiers et exécutez ce qui suit :

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

Le résultat généré ressemblera à ce qui suit :

```
{"hash":"00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09","
```

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

 "previousblockhash":"0000000008e647742775a230787d66fdf92c46a48c896bfbc85cdc8acc67e87d",
    "nextblockhash":"00000000a2887344f8db859e372e7e4bc26b23b9de340f725afbf2edb265b4c6",
    "strippedsize":216,"size":216,"weight":864,
    "tx":["fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33"]},
    "error":null,"id":"1001"}
```


> **Note**
>
> L'exemple de demande du script précédent effectue l'`getblock`appel avec le même hachage de bloc de paramètres d'entrée que dans l'Effectuez des requêtes JSON-RPC AMB Access Bitcoin dans awscurl en utilisant le AWS CLIexemple. Pour effectuer d'autres appels, modifiez l'`rpc`objet dans le script avec un Bitcoin JSON-RPC différent. Vous pouvez remplacer l'option de propriété de l'hôte par le Bitcoin `testnet` pour passer des appels sur ce point de terminaison.

Utilisez AMB Access Bitcoin over AWS PrivateLink

AWS PrivateLink est une technologie hautement disponible et évolutive que vous pouvez utiliser pour connecter votre VPC à des services en privé comme s'ils se trouvaient dans votre VPC. Vous n'êtes pas obligé d'utiliser une passerelle Internet, un appareil NAT, une adresse IP publique, une connexion AWS Direct Connect ou une connexion VPN AWS Site-to-Site pour communiquer avec le service depuis vos sous-réseaux privés. Pour plus d'informations AWS PrivateLink ou pour le configurer AWS PrivateLink, voir Qu'est-ce que c'est AWS PrivateLink ?

Vous pouvez envoyer des requêtes Bitcoin JSON-RPC à AMB Access Bitcoin AWS PrivateLink via un point de terminaison VPC. Les demandes adressées à ce point de terminaison privé ne sont pas transmises via Internet ouvert. Vous pouvez donc envoyer des demandes directement aux points de terminaison Bitcoin en utilisant la même authentification SigV4. Pour plus d'informations, consultez la section Accès aux AWS services via AWS PrivateLink.

Pour le nom du service, recherchez Amazon Managed Blockchain dans la colonne AWS service. Pour plus d'informations, consultez la section AWS Services intégrés à AWS PrivateLink.
Le nom de service du point de terminaison sera au format suivant :`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*.

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

Cas d'utilisation du Bitcoin avec Amazon Managed Blockchain (AMB) Access Bitcoin

Cette rubrique fournit une liste des cas d'utilisation d'AMB Access Bitcoin

Rubriques

Créez un portefeuille Bitcoin (BTC) pour envoyer et recevoir des BTC

Le BTC, la cryptomonnaie native du réseau Bitcoin, est un élément essentiel du modèle de sécurité du réseau. Il agit également comme une marchandise et un moyen d'échange, largement utilisés par les institutions, les entreprises et les particuliers. Par conséquent, de nombreuses applications de portefeuille s'appuient sur des nœuds Bitcoin pour interagir avec la blockchain Bitcoin. Ces applications calculent le solde des sorties non dépensées (UTXOs) pour un ensemble d'adresses donné, signent et envoient des transactions au réseau Bitcoin et récupèrent des données sur l'historique des transactions.

Voici un exemple de certains des fichiers Bitcoin JSON pris en charge par Amazon Managed Blockchain (AMB) Access Bitcoin pour les transactions de portefeuille BTC : RPCs

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

Pour de plus amples informations, veuillez consulter JSON- pris en charge RPCs.

Analyser l'activité sur la blockchain Bitcoin

Vous pouvez analyser le volume des transactions sur la blockchain Bitcoin en utilisant la méthode `getchaintxstats` JSON-RPC. Ce JSON-RPC vous permet d'accéder à des métriques telles que le taux de transaction moyen par seconde, le nombre total de transactions, le nombre de blocs, etc. Vous pouvez également définir une fenêtre contenant des numéros de blocs ou un hachage de blocs comme délimiteur afin de calculer ces statistiques pour un ensemble spécifique de blocs du réseau, si vous le souhaitez.

Pour de plus amples informations, veuillez consulter JSON- pris en charge RPCs.

Vérifiez les messages signés à l'aide d'une paire de clés Bitcoin

Les portefeuilles Bitcoin ont une clé privée et une clé publique qui constituent une paire de clés. Ces clés sont utilisées pour signer des transactions et servent d'identité à l'utilisateur sur la blockchain. La clé publique est utilisée pour créer des adresses, qui sont des identifiants alphanumériques normalisés (27 à 34 caractères). Ces adresses sont utilisées pour recevoir les sorties BTC et gérer les transactions ou les messages.

Avec un portefeuille Bitcoin, les utilisateurs peuvent également signer et vérifier des messages de manière cryptographique. Ce processus est souvent utilisé pour prouver la propriété d'une adresse de portefeuille spécifique et du BTC qui y est associé. En utilisant le `verifymessage` Bitcoin JSON-RPC, vous pouvez vérifier l'authenticité et la validité d'un message signé par un autre portefeuille. Plus précisément, un nœud Bitcoin peut être utilisé pour vérifier si un message a été signé à l'aide de la clé privée correspondant à l'adresse dérivée de la clé publique fournie dans le message signé lui-même.

Pour de plus amples informations, veuillez consulter JSON- pris en charge RPCs.

Inspectez le mempool Bitcoin

De nombreuses applications ont besoin d'accéder au mempool pour suivre les transactions en attente, obtenir une liste de toutes les transactions en attente ou savoir d'où provient une transaction. Pour ce faire, il existe des Bitcoins de RPCs type `getmempoolancestors` JSON `getrawmempool` qui supportent cette activité. `getmempoolentry` Ces applications Bitcoin JSON- RPCs aident à obtenir les informations dont elles ont besoin à partir du mempool.

Amazon Managed Blockchain (AMB) Access Bitcoin prend également en charge le `testmempoolaccept` Bitcoin JSON-RPCs, qui vous permet de vérifier si une transaction respecte

les règles du protocole et serait acceptée par un nœud avant de la soumettre. Les portefeuilles, les bourses et toute autre entité qui soumettent directement des transactions à la blockchain Bitcoin utilisent ces Bitcoin JSON-RPCs.

Pour de plus amples informations, veuillez consulter JSON- pris en charge RPCs.

Bitcoin JSON pris en charge - RPCs avec Amazon Managed Blockchain (AMB) Access Bitcoin

Cette rubrique fournit une liste et des références au Bitcoin JSON pris en charge par Managed Blockchain. RPCs Chaque JSON-RPC pris en charge est accompagné d'une brève description de son utilisation.

Note

- Vous pouvez authentifier Bitcoin JSON- RPCs sur Managed Blockchain en utilisant le processus de signature Signature Version 4 (SigV4). Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent interagir avec celui-ci en utilisant le Bitcoin JSON-. RPCs Fournissez des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) avec l'appel.
- Si votre réponse HTTP est supérieure à 10 Mo, un message d'erreur s'affichera. Pour corriger cela, vous devez définir les en-têtes de compression sur`Accept-Encoding:gzip`. La réponse compressée que votre client reçoit ensuite contient les en-têtes suivants : `Content-Type: application/json` et`Content-Encoding: gzip`.
- Amazon Managed Blockchain (AMB) Access Bitcoin génère une erreur 400 pour les requêtes JSON-RPC mal formées.
- Utilisez le `sendrawtransaction` JSON-RPC pour soumettre des transactions qui mettent à jour l'état de la blockchain Bitcoin.
- AMB Access Bitcoin a une limite de demandes par défaut de 100 demandes par seconde (RPS)`NETWORK_TYPE`, par région. AWS

  Pour augmenter votre quota, vous devez contacter le AWS support. Pour contacter le AWS support, connectez-vous à la console du centre de AWS support. Choisissez Create case (Créer une demande). Choisissez Technique. Choisissez Managed Blockchain comme service. Choisissez Access:Bitcoin comme catégorie et General Guidance comme niveau de gravité. Entrez RPC Quota comme sujet et dans la zone de texte Description et listez les limites de quota applicables à vos besoins en RPS par réseau Bitcoin et par région. Soumettez votre dossier.

JSON- pris en charge RPCs

AMB Access Bitcoin prend en charge le Bitcoin JSON- RPCs suivant. Chaque appel pris en charge est accompagné d'une brève description de son utilisation.

Catégorie	JSON-RPC	Description
Blockchain RPCs	getbestblockhash	Renvoie le hachage du meilleur bloc (pointe) de la chaîne entièrement validée la plus travaillée.
	getblock	Si la verbosité est égale à 0, renvoie une chaîne sérialisée contenant des données codées en hexadécimal pour le « hachage » du bloc. Si la verbosité est égale à 1, renvoie un objet contenant des informations sur le « hachage » du bloc. Si la verbosité est égale à 2, renvoie un objet contenant des informati ons sur le « hachage » du bloc et des informati ons sur chaque transaction. Si la verbosité est égale à 3, renvoie un objet contenant des informations sur le « hachage » du bloc et des informations sur chaque transaction, y compris les `prevout` informations pour les entrées.
	obtenir des informations sur la blockchain	Renvoie un objet contenant diverses informati ons d'état concernant le traitement de la blockchain.
	obtenir le nombre de blocs	Renvoie la hauteur de la chaîne entièrement validée la plus travaillée. Le bloc de genèse a une hauteur de 0.
	filtre getblock	Récupère un filtre de contenu BIP 157 pour un bloc particulier à l'aide du hachage du bloc.
	getblockhash	Renvoie le hachage du bloc best-block-chain à la hauteur fournie.

Catégorie	JSON-RPC	Description
	getblockheader	Si verbose est faux, renvoie une chaîne sérialisée contenant des données codées en hexadécimal pour le « hachage » de l'en-tête de bloc. Si verbose est vrai, renvoie un objet contenant des informations sur le blockheader 'hash'.
	obtenir des statistiques sur les blocs	Calcule les statistiques par bloc pour une fenêtre donnée. Tous les montants sont en satoshis. Cela ne fonctionnera pas sur certaines hauteurs avec l'élagage.
	obtenir des conseils sur les chaînes	Renvoie des informations sur toutes les pointes connues de l'arbre à blocs, y compris la chaîne principale et les branches orphelines.
	getchaintxstats	Calcule des statistiques sur le nombre total et le taux de transactions dans la chaîne.
	avoir de la difficulté	Renvoie la proof-of-work difficulté sous la forme d'un multiple de la difficulté minimale.
	découvrez les ancêtres de Mempool	Si txid se trouve dans le mempool, renvoie tous les ancêtres du mempool.
	obtenir des descendants de mempool	Si txid se trouve dans le mempool, renvoie tous les descendants du mempool.
	getmempool entry	Renvoie les données mempool pour une transaction donnée.
	obtenir des informations sur Mempool	Renvoie des informations sur l'état actif du pool de mémoire TX.

Catégorie	JSON-RPC	Description
	getrawmempool	Renvoie toutes les transactions du pool de mémoire IDs sous la forme d'un tableau JSON de transactions sous forme de chaîne IDs. **Note** `verbose = true` n'est pas pris en charge.
	sortir	Renvoie les détails d'une sortie de transaction non dépensée.
	gettxoutproof	Renvoie une preuve codée en hexadécimal indiquant que « txid » a été inclus dans un bloc.
Transactions brutes RPCs	créer une transaction brute	Crée une transaction en dépensant les entrées données et en créant de nouvelles sorties.
	décoder une transaction brute	Renvoie un objet JSON représentant la transaction sérialisée codée en hexadécimal.
	décodécrire	Décode un script codé en hexadécimal.
	transaction getraw	Renvoie les données de transaction brutes.
	envoyer une transaction brute	Soumet une transaction brute (sérialisée, codée en hexadécimal) au nœud et au réseau locaux.
	testez mempool accept	Renvoie le résultat des tests d'acceptation de mempool indiquant si la transaction brute (sérialisée, codée en hexadécimal) serait acceptée par mempool. Cela permet de vérifier si la transaction enfreint les règles de consensus ou de politique.

Catégorie	JSON-RPC	Description
Utilitaire RPCs	créer un multisig	Crée une adresse multisignature avec aucune signature de mes clés requise.
	estimer les frais intelligents	Estime les frais approximatifs par kilo-octet requis pour qu'une transaction commence à être confirmée dans les blocs conf_target, si possible, et renvoie le nombre de blocs pour lesquels l'estimation est valide. Utilise la taille de transaction virtuelle, telle que définie dans le BIP 141 (les données des témoins sont réduites).
	valider l'adresse	Renvoie des informations sur l'adresse bitcoin donnée.
	vérifier le message	Vérifie un message signé.

Sécurité dans Amazon Managed Blockchain (AMB) Access Bitcoin

La sécurité du cloud AWS est une priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Managed Blockchain (AMB) Access Bitcoin, consultez la section AWS Services concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables.

Pour assurer la protection des données, l'authentification et le contrôle d'accès, Amazon Managed Blockchain utilise les AWS fonctionnalités et les fonctionnalités du framework open source exécuté dans Managed Blockchain.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AMB Access Bitcoin. Les rubriques suivantes vous montrent comment configurer AMB Access Bitcoin pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Bitcoin AMB Access.

Rubriques

Protection des données dans Amazon Managed Blockchain (AMB) Access Bitcoin

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon Managed Blockchain (AMB) Access Bitcoin. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec AMB Access Bitcoin ou autre Services AWS en utilisant la console AWS CLI, l'API ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

Le chiffrement des données permet d'empêcher les utilisateurs non autorisés de lire les données d'un réseau blockchain et des systèmes de stockage de données associés. Cela inclut les données susceptibles d'être interceptées lorsqu'elles circulent sur le réseau, appelées données en transit.

Chiffrement en transit

Par défaut, Managed Blockchain utilise une connexion HTTPS/TLS pour chiffrer toutes les données transmises depuis un ordinateur client qui exécute les points de terminaison du AWS CLI service. AWS

Vous n'avez pas besoin de faire quoi que ce soit pour activer l'utilisation de HTTP/TLS. Il est toujours activé, sauf si vous le désactivez explicitement pour une AWS CLI commande individuelle à l'aide de la `--no-verify-ssl` commande.

Gestion des identités et des accès pour Amazon Managed Blockchain (AMB) Access Bitcoin

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Bitcoin d'AMB Access. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Gestion de l’accès à l’aide de politiques
- Comment Amazon Managed Blockchain (AMB) Access Bitcoin fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin
- Résolution des problèmes liés à l'identité et à l'accès à Amazon Managed Blockchain (AMB) Access Bitcoin

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes liés à l'identité et à l'accès à Amazon Managed Blockchain (AMB) Access Bitcoin)
- Administrateur du service : déterminez l’accès des utilisateurs et soumettez les demandes d’autorisation (voir Comment Amazon Managed Blockchain (AMB) Access Bitcoin fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l’accès (voir Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d’informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l’utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d’informations, consultez Signature AWS Version 4 pour les demandes d’API dans le Guide de l’utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les

ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon Managed Blockchain (AMB) Access Bitcoin fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AMB Access Bitcoin, découvrez quelles fonctionnalités IAM peuvent être utilisées avec AMB Access Bitcoin.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Managed Blockchain (AMB) Access Bitcoin

Fonctionnalité IAM	Assistance avec AMB Access Bitcoin
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d'une politique	Non
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Non
Autorisations de principals	Non
Rôles du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AMB Access Bitcoin et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AMB Access Bitcoin

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur

l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour AMB Access Bitcoin

Pour voir des exemples de politiques basées sur l'identité d'AMB Access Bitcoin, consultez. Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin

Politiques basées sur les ressources au sein d'AMB Access Bitcoin

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour AMB Access Bitcoin

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d'AMB Access Bitcoin, consultez la section Actions définies par Amazon Managed Blockchain (AMB) Access Bitcoin dans le Service Authorization Reference.

Les actions politiques dans AMB Access Bitcoin utilisent le préfixe suivant avant l'action :

```
managedblockchain:
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `InvokeRpcBitcoin`, incluez l'action suivante :

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

Pour voir des exemples de politiques basées sur l'identité d'AMB Access Bitcoin, consultez. Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin

Ressources politiques pour AMB Access Bitcoin

Prend en charge les ressources de politique : non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les

actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources AMB Access Bitcoin et leurs caractéristiques ARNs, consultez la section Resources Defined by Amazon Managed Blockchain (AMB) Access Bitcoin dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Managed Blockchain (AMB) Access Bitcoin.

Pour voir des exemples de politiques basées sur l'identité d'AMB Access Bitcoin, consultez. Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin

Clés de conditions de politique pour AMB Access Bitcoin

Prend en charge les clés de condition de politique spécifiques au service : non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition AMB Access Bitcoin, consultez la section Clés de condition pour Amazon Managed Blockchain (AMB) Access Bitcoin dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Managed Blockchain (AMB) Access Bitcoin.

Pour voir des exemples de politiques basées sur l'identité d'AMB Access Bitcoin, consultez. Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin

ACLs dans AMB Access Bitcoin

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AMB Access Bitcoin

Prise en charge d'ABAC (balises dans les politiques) : non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AMB Access Bitcoin

Supporte les informations d'identification temporaires : Non

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour AMB Access Bitcoin

Prend en charge les sessions d’accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d’accès.

Rôles de service pour AMB Access Bitcoin

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu’un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut perturber les fonctionnalités d'AMB Access Bitcoin. Modifiez les rôles de service uniquement lorsque AMB Access Bitcoin fournit des conseils pour le faire.

Rôles liés aux services pour AMB Access Bitcoin

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d’effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d’informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain (AMB) Access Bitcoin

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources AMB Access Bitcoin. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AMB Access Bitcoin, y compris le format du ARNs pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon Managed Blockchain (AMB) Access Bitcoin dans le Service Authorization Reference.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources AMB Access Bitcoin de votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule

tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AMB Access Bitcoin

Pour accéder à la console Amazon Managed Blockchain (AMB) Access Bitcoin, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des ressources AMB Access Bitcoin de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console AMB Access Bitcoin, associez également la politique AMB Access Bitcoin *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès aux réseaux Bitcoin

> **Note**
>
> Pour accéder aux points de terminaison publics du Bitcoin `mainnet` et `testnet` passer des appels JSON-RPC, vous aurez besoin d'informations d'identification utilisateur (`AWS_ACCESS_KEY_IDetAWS_SECRET_ACCESS_KEY`) disposant des autorisations IAM appropriées pour AMB Access Bitcoin.

Example Politique IAM pour accéder à tous les réseaux Bitcoin

Cet exemple permet à un utilisateur IAM d' Compte AWS accéder à tous les réseaux Bitcoin.

JSON

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

Example Politique IAM pour accéder au réseau Bitcoin Testnet

Cet exemple accorde à un utilisateur IAM l' Compte AWS accès au `testnet` réseau Bitcoin.

JSON

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

Résolution des problèmes liés à l'identité et à l'accès à Amazon Managed Blockchain (AMB) Access Bitcoin

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AMB Access Bitcoin et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AMB Access Bitcoin
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources AMB Access Bitcoin

Je ne suis pas autorisé à effectuer une action dans AMB Access Bitcoin

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `managedblockchain::`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `managedblockchain::`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AMB Access Bitcoin.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AMB Access Bitcoin. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources AMB Access Bitcoin

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez

spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d’informations, consultez les éléments suivants :

- Pour savoir si AMB Access Bitcoin prend en charge ces fonctionnalités, consultezComment Amazon Managed Blockchain (AMB) Access Bitcoin fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d’identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d’identité) dans le Guide de l’utilisateur IAM.
- Pour en savoir plus sur la différence entre l’utilisation des rôles et des politiques basées sur les ressources pour l’accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Enregistrement d'Amazon Managed Blockchain (AMB) Accédez aux événements Bitcoin en utilisant AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin ne prend pas en charge les événements de gestion.

Amazon Managed Blockchain est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Managed Blockchain. CloudTrail capture qui a invoqué les points de terminaison AMB Access Bitcoin pour Managed Blockchain en tant qu'événements du plan de données.

Si vous créez un journal correctement configuré auquel vous êtes abonné pour recevoir les événements du plan de données souhaités, vous pouvez bénéficier de la diffusion continue des CloudTrail événements liés à AMB Access Bitcoin vers un compartiment Amazon S3. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer si une demande a été envoyée à l'un des points de terminaison AMB Access Bitcoin, l'adresse IP d'origine de la demande, l'auteur de la demande, la date à laquelle elle a été faite et d'autres informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur AMB Access Bitcoin en CloudTrail

AWS CloudTrail est activé par défaut lorsque vous créez votre Compte AWS. Toutefois, pour savoir qui a invoqué les points de terminaison AMB Access Bitcoin, vous devez configurer CloudTrail pour enregistrer les événements du plan de données.

Pour conserver un enregistrement permanent des événements survenus dans votre compte Compte AWS, y compris les événements du plan de données pour AMB Access Bitcoin, vous devez créer une trace. Un suivi permet de CloudTrail transférer des fichiers journaux vers un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans le AWS Management Console, le parcours s'applique à tous Régions AWS. Le journal enregistre les événements de toutes les régions

prises en charge dans la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser ces données de manière plus approfondie et agir sur les données d'événements collectées dans les CloudTrail journaux. Pour plus d'informations, consultez les ressources suivantes :

- Utilisation CloudTrail pour suivre Bitcoin JSON- RPCs
- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

En analysant les événements CloudTrail liés aux données, vous pouvez contrôler qui a invoqué les points de terminaison AMB Access Bitcoin.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (IAM).
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal Bitcoin d'AMB Access

Pour les événements du plan de données, un suivi est une configuration qui permet de transmettre les événements sous forme de fichiers journaux à un compartiment S3 spécifié. Chaque fichier CloudTrail journal contient une ou plusieurs entrées de journal qui représentent une seule demande provenant de n'importe quelle source. Ces entrées fournissent des détails sur l'action demandée, notamment la date et l'heure de l'action, ainsi que les éventuels paramètres de demande associés.

> **Note**
>
> CloudTrail les événements de données dans les fichiers journaux ne constituent pas une trace ordonnée des appels de l'API Bitcoin d'AMB Access. Ils n'apparaissent donc pas dans un ordre spécifique.

Utilisation CloudTrail pour suivre Bitcoin JSON- RPCs

Vous pouvez l'utiliser CloudTrail pour savoir qui, dans votre compte, a invoqué les points de terminaison AMB Access Bitcoin et quel JSON-RPC a été invoqué en tant qu'événements de données. Par défaut, lorsque vous créez un suivi, les événements liés aux données ne sont pas enregistrés. Pour enregistrer les personnes qui ont invoqué les points de terminaison AMB Access Bitcoin en tant qu'événements de CloudTrail données, vous devez ajouter explicitement les ressources prises en charge ou les types de ressources pour lesquels vous souhaitez collecter des activités à un suivi. Amazon Managed Blockchain prend en charge l'ajout d'événements de données à l'aide du AWS Management Console AWS SDK et AWS CLI. Pour plus d'informations, voir Enregistrer les événements à l'aide de sélecteurs avancés dans le Guide de l'AWS CloudTrail utilisateur.

Pour enregistrer les événements liés aux données dans un suivi, utilisez l'put-event-selectorsopération après avoir créé le suivi. Utilisez l'`--advanced-event-selectors`option pour spécifier les types de `AWS::ManagedBlockchain::Network` ressources afin de commencer à enregistrer les événements de données afin de déterminer qui a invoqué les points de terminaison AMB Access Bitcoin.

Example Entrée dans le journal des événements de toutes les demandes de points de terminaison Bitcoin AMB Access de votre compte

L'exemple suivant montre comment utiliser l'`put-event-selectors`opération pour enregistrer toutes les demandes du point de terminaison AMB Access Bitcoin de votre compte pour le parcours `my-bitcoin-trail` dans la `us-east-1` région.

```
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"] } ]}]'
```

Une fois inscrit, vous pouvez suivre l'utilisation dans le compartiment S3 connecté à la piste spécifiée dans l'exemple précédent.

Le résultat suivant montre une entrée dans le journal des événements de CloudTrail données contenant les informations collectées par CloudTrail. Vous pouvez déterminer qu'une demande Bitcoin JSON-RPC a été envoyée à l'un des points de terminaison Bitcoin d'AMB Access, l'adresse IP d'origine de la demande, le nom de l'auteur de la demande, la date à laquelle elle a été faite et d'autres informations supplémentaires.


```
{
        "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"
}
```

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.