



Guide du développeur

AMBAccédez à Bitcoin



AMBAccédez à Bitcoin: Guide du développeur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon Managed Blockchain (AMB) Access Bitcoin ?	1
Utilisez-vous AMB Access Bitcoin pour la première fois ?	2
Concepts clés	3
Considérations et restrictions	4
Configuration	6
Prérequis et considérations	6
Inscrivez-vous pour AWS	6
Création d'un IAM utilisateur avec les autorisations appropriées	7
Installez et configurez le AWS Command Line Interface	7
Premiers pas	8
Création d'une IAM politique	8
RPCExemple de console	9
exemple awscurl RPC	10
RPCExemple de fichier Node.js	11
AMBAccédez à Bitcoin via PrivateLink	15
Cas d'utilisation du Bitcoin	17
Créez un portefeuille Bitcoin (BTC) pour envoyer et recevoir des BTC	17
Analyser l'activité sur la blockchain Bitcoin	18
Vérifiez les messages signés à l'aide d'une paire de clés Bitcoin	18
Inspectez le mempool Bitcoin	18
Bitcoin JSON-RPC	20
JSON-RPC pris en charge	21
Sécurité	25
Protection des données	26
Chiffrement des données	27
Chiffrement en transit	27
Gestion des identités et des accès	27
Public ciblé	28
Authentification par des identités	29
Gestion des accès à l'aide de politiques	33
Comment fonctionne Amazon Managed Blockchain (AMB) Access Bitcoin avec IAM	35
Exemples de politiques basées sur l'identité	42
Résolution des problèmes	47
CloudTrail journaux	50

Informations sur AMB Access Bitcoin en CloudTrail	50
Comprendre les entrées du fichier journal Bitcoin d'AMB Access	51
Utilisation CloudTrail pour suivre les Bitcoin JSON-RPC	52
.....	iv

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](#)
- [JSON-RPC Bitcoin compatibles 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 des RPC Bitcoin JSON pour communiquer avec des nœuds Bitcoin gérés par Managed Blockchain afin d'interagir avec les réseaux Bitcoin. Avec les Bitcoin JSON-RPC, vous pouvez lire des données et écrire des transactions, notamment en interrogeant des données et en soumettant des transactions aux réseaux Bitcoin à l'aide du 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 les Bitcoin JSON-RPC 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 des RPC Bitcoin individuels.

- 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 vos Bitcoin JSON-RPC. 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 . Le chapitre suivant explique comment commencer à utiliser AMB Access Bitcoin.

Prérequis et considérations

Avant d'utiliser AWS pour la première fois, vous devez avoir un Compte AWS.

Inscrivez-vous pour AWS

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

Si vous avez un Compte AWS déjà, 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 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 AWS est créé. L'utilisateur root a accès à tous Services AWS et les ressources du 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 IAM utilisateur avec les autorisations appropriées

Pour créer et utiliser AMB Access Bitcoin, vous devez disposer d'un AWS Identity and Access Management (IAM) principal (utilisateur ou groupe) doté d'autorisations autorisant les actions nécessaires à Managed Blockchain.

Seuls IAM les mandants peuvent passer des RPC appels BitcoinJSON. Lorsque vous appelez le Bitcoin JSON RPCs sur Amazon Managed Blockchain, vous pouvez le faire via une HTTPS connexion authentifiée à l'aide du [processus de signature Signature Version 4](#). Cela signifie que seuls IAM les directeurs autorisés du AWS le compte peut passer des RPC appels BitcoinJSON. Pour ce faire, AWS des 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 IAM utilisateur, voir [Création d'un IAM utilisateur dans votre AWS compte](#). Pour plus d'informations sur la façon d'associer une politique d'autorisation à un utilisateur, consultez la section [Modification des autorisations d'un IAM utilisateur](#). Pour un exemple de politique d'autorisation que vous pouvez utiliser pour autoriser un utilisateur à travailler avec AMB Access Bitcoin, consultez [Exemples de politiques basées sur l'identité pour Amazon Managed Blockchain \(AMB\) Access Bitcoin](#).

Installez et configurez le AWS Command Line Interface

Si ce n'est pas déjà fait, installez le dernier AWS Interface de ligne de commande (CLI) avec laquelle travailler AWS ressources d'un terminal. Pour plus d'informations, voir [Installation ou mise à jour de la dernière version du AWS CLI](#).

Note

Pour CLI y accéder, vous avez besoin d'un identifiant 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, voir [Utilisation d'informations d'identification temporaires avec AWS ressources](#) du guide de IAM l'utilisateur.

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 IAM politique pour accéder au Bitcoin JSON - RPCs](#)
- [Effectuez des requêtes Bitcoin Remote Procedure call \(RPC\) sur l'RPCéditeur AMB Access à l'aide du AWS Management Console](#)
- [Make AMB Access Bitcoin JSON - RPC requêtes dans awsurl en utilisant le AWS CLI](#)
- [Make Bitcoin JSON - RPC requêtes dans Node.js](#)
- [Utilisez AMB Access Bitcoin over AWS PrivateLink](#)

Créez une IAM politique pour accéder au Bitcoin JSON - RPCs

Pour accéder aux points de terminaison publics permettant au Bitcoin Mainnet et au Testnet d'effectuer JSON des RPC appels, vous devez disposer d'informations d'identification utilisateur (AWS_ACCESS_KEY_ID et _AWS_SECRET_ACCESS_KEY) disposant des IAM autorisations appropriées pour Amazon Managed Blockchain (AMB) Access Bitcoin. Dans un terminal doté du AWS CLI installé, exécutez la commande suivante pour créer une IAM politique 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 politique, associez-la au rôle de votre IAM utilisateur pour qu'elle prenne effet. Dans le volet AWS Management Console, accédez au IAM service et associez la politique AmazonManagedBlockchainBitcoinAccess au rôle attribué à votre IAM utilisateur. Pour plus d'informations, consultez [Création d'un rôle et attribution à un IAM utilisateur](#).

Effectuez des requêtes Bitcoin Remote Procedure call (RPC) sur l'RPCÉditeur AMB Access à l'aide du AWS Management Console

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

Exemple

L'exemple suivant montre comment obtenir des informations sur le `blockhash00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09` en utilisant. `getBlock` RPC Remplacez les variables surlignées par vos propres entrées ou choisissez l'une des autres RPCméthodes répertoriées et entrez les entrées pertinentes requises.

1. Ouvrez la console Managed Blockchain à l'adresse <https://console.aws.amazon.com/managedblockchain/>.
2. Choisissez un RPC éditeur.
3. Dans la section Demande, choisissez *BITCOIN_MAINNET* comme réseau Blockchain.
4. Choisissez *getBlock* comme RPC méthode.
5. Entrez *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09* comme numéro de bloc et choisissez *0* comme verbosité.
6. Ensuite, choisissez Submit (Soumettre) 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 [RPC support d'AMB Access Bitcoin](#)

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

Exemple

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

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 le AWS CLI, vos informations IAM d'identification utilisateur et votre AWS région 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. `getBlock` RPC Cet appel accepte un paramètre de chaîne correspondant au hachage du bloc pour lequel vous souhaitez récupérer des informations.

Exemple

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 IAM utilisateur.

```
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 defining 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 RPC requêtes au point de terminaison Bitcoin, et il signe ces demandes avec les en-têtes Signature Version 4 (SigV4) appropriés en utilisant le AWS SDK Outils 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,
```

olpPar 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](#)
- [Analyser l'activité sur la blockchain Bitcoin](#)
- [Vérifiez les messages signés à l'aide d'une paire de clés Bitcoin](#)
- [Inspectez le mempool Bitcoin](#)

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 (UTXO) pour un ensemble d'adresses donné, signent et envoient des transactions au réseau Bitcoin et récupèrent des données sur les transactions historiques.

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

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

Pour plus d'informations, consultez [JSON-RPC pris en charge](#).

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 plus d'informations, consultez [JSON-RPC pris en charge](#).

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 plus d'informations, consultez [JSON-RPC pris en charge](#).

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 Bitcoin JSON-RPC comme `getmempoolancestors` et `getmempoolentry`, et `getrawmempool` qui soutiennent cette activité. Ces Bitcoin JSON-RPC aident les applications 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-RPC, qui vous permet de vérifier si une transaction respecte

les règles du protocole et si elle est 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-RPC.

Pour plus d'informations, voir [JSON-RPC pris en charge](#).

JSON-RPC Bitcoin compatibles avec Amazon Managed Blockchain (AMB) Access Bitcoin

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

Note

- Vous pouvez authentifier les Bitcoin JSON-RPC 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 les Bitcoin JSON-RPC. 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-RPC pris en charge

AMB Access Bitcoin prend en charge les Bitcoin JSON-RPC suivants. Chaque appel pris en charge est accompagné d'une brève description de son utilisation.

Catégorie	JSON-RPC	Description
RPC Blockchain	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 informations sur le « hachage » du bloc et des informations 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 preuves d'informations pour les entrées.
	obtenir des informations sur la blockchain	Renvoie un objet contenant diverses informations 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	Revoie 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	Revoie 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	Revoie les données mempool pour une transaction donnée.
	obtenir des informations sur Mempool	Revoie des informations sur l'état actif du pool de mémoire TX.

Catégorie	JSON-RPC	Description
	<u>getrawmempool</u>	<p>Renvoie tous les identifiants de transaction du pool de mémoire sous la forme d'un tableau JSON d'identifiants de transaction sous forme de chaîne.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note <code>verbose = true</code> n'est pas pris en charge.</p> </div>
	<u>sortir</u>	Renvoie les détails d'une sortie de transaction non dépensée.
	<u>gettxoutproof</u>	Renvoie une preuve codée en hexadécimal indiquant que « txid » a été inclus dans un bloc.
<u>RPC de transactions brutes</u>	<u>créer une transaction brute</u>	Crée une transaction dépensant les entrées données et créant de nouvelles sorties.
	<u>décoder une transaction brute</u>	Renvoie un objet JSON représentant la transaction sérialisée codée en hexadécimal.
	<u>décodécrire</u>	Décode un script codé en hexadécimal.
	<u>transaction getraw</u>	Renvoie les données de transaction brutes.
	<u>envoyer une transaction brute</u>	Soumet une transaction brute (sérialisée, codée en hexadécimal) au nœud et au réseau locaux.
	<u>testez mempool accept</u>	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
Util RPC	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	Revoie 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 conformité AWS](#). 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](#)
- [Gestion des identités et des accès pour Amazon Managed Blockchain \(AMB\) Access Bitcoin](#)

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

Le AWS modèle de [responsabilité partagée 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. Vous êtes responsable du contrôle de votre contenu hébergé sur cette infrastructure. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section [Confidentialité des données FAQ](#). Pour plus d'informations sur la protection des données en Europe, consultez le [AWS Modèle de responsabilité partagée et article de GDPR](#) blog sur le AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or AWS Identity and Access Management (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) pour chaque compte.
- Utilisez SSL/TLS pour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir [Travailler avec les CloudTrail sentiers](#) dans le AWS CloudTrail Guide de l'utilisateur.
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou un API, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir [Federal Information Processing Standard \(FIPS\) 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 Name (Nom). Cela inclut lorsque vous travaillez avec AMB Access, Bitcoin ou autre Services AWS à l'aide de la console API, AWS CLI, 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 un URL à un serveur externe, nous vous recommandons vivement de ne pas y inclure d'informations d'identification URL pour valider votre demande auprès de 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 TLS connexion HTTPS pour chiffrer toutes les données transmises depuis un ordinateur client qui exécute le AWS CLI to AWS points de terminaison de service.

Vous n'avez rien à faire pour activer l'utilisation de HTTPS/TLS. Il est toujours activé sauf si vous le désactivez explicitement pour un individu AWS CLI commande à l'aide de la `--no-verify-ssl` commande.

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

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

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment fonctionne Amazon Managed Blockchain \(AMB\) Access Bitcoin 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

Comment utilisez-vous AWS Identity and Access Management (IAM) diffère en fonction du travail que vous effectuez dans AMB Access Bitcoin.

Utilisateur du service — Si vous utilisez le service AMB Access Bitcoin pour faire votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'AMBAccess Bitcoin pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité AMB d'Access Bitcoin, consultez [Résolution des problèmes liés à l'identité et à l'accès à Amazon Managed Blockchain \(AMB\) Access Bitcoin](#).

Administrateur du service — Si vous êtes responsable des ressources AMB Access Bitcoin dans votre entreprise, vous avez probablement un accès complet à AMB Access Bitcoin. C'est à vous de déterminer les fonctionnalités et les ressources d'AMBAccess Bitcoin auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM AMB Access Bitcoin, consultez [Comment fonctionne Amazon Managed Blockchain \(AMB\) Access Bitcoin avec IAM](#).

IAM administrateur — Si vous êtes IAM administrateur, vous souhaitez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AMB Access Bitcoin. Pour voir des exemples de politiques basées sur l'identité AMB Access Bitcoin que vous pouvez utiliser IAM, consultez [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 en utilisant vos informations d'identification. Vous devez être authentifié (connecté) à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez AWS en utilisant la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au AWS Management Console ou le AWS portail d'accès. Pour plus d'informations sur la connexion à AWS, voir [Comment se connecter à votre Compte AWS](#) dans le .Connexion à AWS Guide de l'utilisateur

Si vous accédez AWS programmatiquement, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, voir [Signature AWS API demandes](#) dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section [Authentification multifactorielle](#) dans le AWS IAM Identity Center Guide de l'utilisateur et [utilisation de l'authentification multifactorielle \(MFA\) dans AWS](#) dans le guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion qui donne un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle Compte AWS utilisateur root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez

en tant qu'utilisateur root, consultez la section [Tâches nécessitant des informations d'identification utilisateur root](#) dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, AWS Directory Service, le répertoire Identity Center ou tout utilisateur accédant Services AWS en utilisant les informations d'identification fournies par le biais d'une source d'identité. Lorsque les identités fédérées accèdent Comptes AWS, ils assument des rôles, et les rôles fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans tous vos Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez [Qu'est-ce qu'IAM Identity Center ?](#) dans le AWS IAM Identity Center Guide de l'utilisateur

Utilisateurs et groupes IAM

Un [IAMutilisateur](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme](#) dans le Guide de IAM l'utilisateur.

Un [IAMgroupe](#) est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir [Quand créer un IAM utilisateur \(au lieu d'un rôle\)](#) dans le Guide de IAM l'utilisateur.

IAM rôles

Un [IAM rôle](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans AWS Management Console en [changeant de rôle](#). Vous pouvez assumer un rôle en appelant un AWS CLI or AWS API opération ou en utilisant une option personnalisée URL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section [Utilisation IAM des rôles](#) dans le Guide de IAM l'utilisateur.

IAM Les rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- **Accès utilisateur fédéré** : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir [Création d'un rôle pour un fournisseur d'identité tiers](#) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les ensembles d'autorisations, voir [Ensembles d'autorisations](#) dans le AWS IAM Identity Center Guide de l'utilisateur
- **Autorisations IAM utilisateur temporaires** : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- **Accès entre comptes** : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Cependant, avec certains Services AWS, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir [Accès aux ressources entre comptes IAM dans le guide](#) de l'IAM utilisateur.
- **Accès multiservices** — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service

exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès transmises (FAS) : lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FAS les demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section [Transférer les sessions d'accès](#).
- Rôle de service — Un rôle de service est un [IAMrôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, voir [Création d'un rôle pour déléguer des autorisations à un Service AWS](#) dans le guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle lié à un service Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui créent AWS CLI or AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2 instance. Pour attribuer un AWS pour attribuer un rôle à une EC2 instance et le mettre à la disposition de toutes ses applications, vous créez un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir [Quand créer un IAM rôle \(au lieu d'un utilisateur\)](#) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès dans AWS en créant des politiques et en les associant à AWS identités ou ressources. Une politique est un objet dans AWS qui, lorsqu'elle est associée à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir [Présentation des JSON politiques](#) dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, 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. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console, le AWS CLI, ou le AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent AWS politiques gérées et politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir [Choisir entre des politiques gérées et des politiques intégrées dans le Guide](#) de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de 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.

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

Listes de contrôle d'accès (ACLs)

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 du document JSON de stratégie.

Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui prennent en charge ACLs. Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limites d'autorisations** — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAM utilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, voir [Limites d'autorisations pour les IAM entités](#) dans le Guide de IAM l'utilisateur.

- **Politiques de contrôle des services (SCPs) :** SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service de regroupement et de gestion centralisée de plusieurs Comptes AWS dont votre entreprise est propriétaire. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités figurant dans les comptes des membres, y compris chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et SCPs consultez les [politiques de contrôle des services](#) dans le AWS Organizations Guide de l'utilisateur
- **Politiques de séance :** les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section [Politiques de session](#) dans le guide de IAM l'utilisateur.

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 détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, voir la [logique d'évaluation des politiques](#) dans le guide de IAM l'utilisateur.

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

Avant de commencer IAM à gérer l'AMB accès à Access Bitcoin, découvrez quelles IAM fonctionnalités sont disponibles avec AMB Access Bitcoin.

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

IAM fonctionnalité	AMB Accédez au support Bitcoin
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non

IAM fonctionnalité	AMB Accédez au support Bitcoin
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d'une politique	Non
ACLs	Non
ABAC(balises dans les politiques)	Non
Informations d'identification temporaires	Non
Autorisations de principaux	Non
Fonctions du service	Non
Rôles liés à un service	Non

Pour avoir une vue d'ensemble de la façon dont AMB Access Bitcoin et d'autres AWS les services fonctionnent avec la plupart IAM des fonctionnalités, voir [AWS services compatibles avec IAM](#) le Guide de l'IAM utilisateur.

Politiques basées sur l'identité pour Access Bitcoin AMB

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

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAM utilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la [référence aux éléments de IAM JSON politique](#) dans le Guide de IAM l'utilisateur.

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

Pour voir des exemples de politiques basées sur l'identité 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 AMB d'Access Bitcoin

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de 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 activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez [la section Accès aux ressources entre comptes IAM dans](#) le Guide de IAM l'utilisateur.

Actions politiques pour AMB Access Bitcoin

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSONpolitiques 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'Actionélément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions politiques portent généralement le même nom que les actions associées AWS APIopération. Il existe certaines exceptions, telles que les actions

avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions 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 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 politiques : Non

Les administrateurs peuvent utiliser AWS JSONpolitiques 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 `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier

une ressource en utilisant son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, 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 pour chaque ressource, consultez [Actions définies par Amazon Managed Blockchain \(AMB\) Access Bitcoin](#). ARN

Pour voir des exemples de politiques basées sur l'identité 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 AWS JSON politiques 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 (ou le bloc Condition) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément Condition est facultatif. 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.

Si vous spécifiez plusieurs Condition éléments dans une instruction ou plusieurs clés dans un seul Condition élément, AWS les évalue à l'aide d'une AND opération logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-

ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez [IAM la section Éléments de politique : variables et balises](#) dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour tout voir AWS clés de condition globales, voir [AWS clés contextuelles des conditions globales](#) dans le guide de IAM l'utilisateur.

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 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 du document JSON de stratégie.

ABAC avec AMB Access Bitcoin

Supports ABAC (balises dans les politiques) : Non

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Entrée AWS, ces attributs sont appelés balises. Vous pouvez associer des tags à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape de ABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABAC est utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

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 ABAC, voir [Qu'est-ce que c'est ABAC ?](#) dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configuration ABAC, voir [Utiliser le contrôle d'accès basé sur les attributs \(ABAC\)](#) dans le guide de l'IAM utilisateur.

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

Supporte les informations d'identification temporaires : Non

Momentanée Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris lesquelles Services AWS utilisent des informations d'identification temporaires, voir [Services AWS qui fonctionnent avec IAM](#) le Guide de l'IAM utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez au AWS Management Console en utilisant n'importe quelle méthode, à l'exception du nom d'utilisateur et du mot de passe. Par exemple, lorsque vous accédez AWS à l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section [Passage à un rôle \(console\)](#) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI or AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder AWS. 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 la section Informations [d'identification de sécurité temporaires dans IAM](#).

Autorisations principales interservices pour AMB Access Bitcoin

Prend en charge les sessions d'accès transféré (FAS) : Non

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux

services en aval. FASLes demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section [Transférer les sessions d'accès](#).

Rôles de service pour AMB Access Bitcoin

Supporte les rôles de service : Non

Un rôle de service est un [IAMrôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, voir [Création d'un rôle pour déléguer des autorisations à un Service AWS](#) dans le guide de l'utilisateur IAM.

Warning

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

Rôles liés à un service pour Access Bitcoin AMB

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 assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, voir [AWS services 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. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management

Console, AWS Command Line Interface (AWS CLI), ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section [Création de IAM politiques](#) dans le guide de l'IAM utilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AMB Access Bitcoin, y compris le ARNs format de chaque type de ressource, 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](#)
- [Utilisation de la console AMB Access Bitcoin](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Accès aux réseaux Bitcoin](#)

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 coûts pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez les directives et recommandations suivantes :

- Commencez avec AWS politiques gérées et évolution vers des autorisations de moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez le AWS politiques 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 AWS des politiques gérées par le client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [.AWS politiques gérées](#) ou [AWS politiques gérées pour les fonctions professionnelles](#) dans le guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une 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 IAM pour appliquer des autorisations, consultez la section [Politiques et autorisations IAM dans](#) le guide de IAM l'utilisateur.

- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisant 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 AWS, comme AWS CloudFormation. Pour plus d'informations, voir [Éléments IAM JSON de politique : Condition](#) dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section [Validation des politiques d'IAM Access Analyzer](#) dans le guide de IAM l'utilisateur.
- Exiger une authentification multifactorielle (MFA) — Si vous avez un scénario qui nécessite IAM des utilisateurs ou un utilisateur root dans votre Compte AWS, activez MFA pour plus de sécurité. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez [la section Configuration de l'API accès MFA protégé](#) dans le Guide de l'IAM utilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de [sécurité IAM](#), consultez la section [Bonnes pratiques en matière](#) de sécurité IAM dans le Guide de IAM l'utilisateur.

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 dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) dotées de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'API opération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console AMB Access Bitcoin, joignez également l'AMBAccess Bitcoin *ConsoleAccess* ou *ReadOnly* AWS politique gérée pour les entités. Pour plus d'informations, consultez la section [Ajouter des autorisations à un utilisateur](#) dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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 pour le Bitcoin mainnet et pour testnet passer des RPC appels, vous aurez besoin d'informations d'identification utilisateur (AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY) disposant des IAM autorisations appropriées pour AMB Access Bitcoin. JSON

Exemple IAM Politique d'accès à tous les réseaux Bitcoin

Cet exemple accorde à un IAM utilisateur le statut de votre Compte AWS accès à tous les réseaux Bitcoin.

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

Exemple IAM Politique d'accès au réseau Bitcoin Testnet

Cet exemple accorde à un IAM utilisateur le statut de votre Compte AWS accès au testnet réseau Bitcoin.

```
{
  "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 pourriez 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 à mon Compte AWS pour 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 lorsque l'utilisateur IAM `mateojacksonIAMutilisateur` essaie d'utiliser la console pour afficher les détails d'une `my-example-widget` ressource fictive mais ne dispose pas des `managedblockchain::GetWidget` autorisations 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:PassRoleaction, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AMB Access Bitcoin.

Momentanée Services AWS vous 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, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur 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 ne dispose pas des autorisations nécessaires pour transférer 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 à mon Compte AWS pour 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 en savoir plus, consultez les éléments suivants :

- Pour savoir si AMB Access Bitcoin prend en charge ces fonctionnalités, consultez [Comment fonctionne Amazon Managed Blockchain \(AMB\) Access Bitcoin avec IAM.](#)

- Pour savoir comment fournir un accès à vos ressources sur Comptes AWS dont vous êtes le propriétaire, voir [Fournir un accès à un IAM utilisateur dans un autre Compte AWS dont vous êtes propriétaire](#) dans le guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, voir [Fournir un accès à Comptes AWS appartenant à des tiers](#) dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section [Fournir un accès aux utilisateurs authentifiés de manière externe \(fédération d'identité\)](#) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux [ressources entre comptes IAM dans le guide](#) de l'IAMutilisateur.

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 les Bitcoin JSON-RPC](#)
- [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 AWS Identity and Access Management (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 plus d'informations, consultez l'élément [CloudTrail UserIdentity](#).

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, y compris 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 les Bitcoin JSON-RPC

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-selectors](#) opération après avoir créé le suivi. Utilisez l'`--advanced-event-selector` 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.

Exemple 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-selector` 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": "ARO0A554U062RJ7KSB7FAX: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.