



開発者ガイド

# AMB Bitcoin へのアクセス



# AMB Bitcoin へのアクセス: 開発者ガイド

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

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

# Table of Contents

Amazon Managed Blockchain (AMB) アクセスビットコインとは何ですか？ .....	1
AMB Access ビットコインを初めて使用する方ですか？ .....	2
主要なコンセプト .....	3
考慮事項と制約事項 .....	4
設定 .....	6
前提条件と考慮事項 .....	6
サインアップ: AWS .....	6
適切なアクセス許可を持つ IAM ユーザーを作成する .....	7
のインストールと設定 AWS Command Line Interface .....	7
使用開始 .....	8
IAM ポリシーを作成する .....	8
コンソールRPCの例 .....	9
awscurl RPCの例 .....	10
Node.js RPCの例 .....	11
AMB 経由で Bitcoin にアクセスする PrivateLink .....	15
ビットコインのユースケース .....	16
BTC を送受信するためのビットコイン (BTC) ウォレットを構築する .....	16
ビットコインブロックチェーン上のアクティビティを分析します。 .....	17
ビットコインkey pair を使用して署名されたメッセージを確認する .....	17
ビットコインメモプールを調べてください。 .....	17
ビットコイン JSON RPC .....	19
サポートされている JSON RPC .....	20
セキュリティ .....	24
データ保護 .....	25
データ暗号化 .....	26
転送中の暗号化 .....	26
ID およびアクセス管理 .....	26
対象者 .....	27
アイデンティティを使用した認証 .....	27
ポリシーを使用したアクセスの管理 .....	31
Amazon Managed Blockchain (AMB) Access Bitcoin と の連携方法 IAM .....	34
アイデンティティベースポリシーの例 .....	41
トラブルシューティング .....	45
CloudTrail ログ .....	48

---

AMB: のビットコイン情報にアクセスします。 CloudTrail .....	48
AMB Access のビットコインログファイルエントリについて .....	49
ビットコイン JSON CloudTrail RPC の追跡に使用 .....	50
.....	lii

# Amazon Managed Blockchain (AMB) アクセスビットコインとは何ですか？

Amazon Managed Blockchain (AMB) アクセスでは、イーサリアムとビットコイン用のパブリックブロックチェーンノードが提供され、Hyperledger Fabric フレームワークを使用してプライベートブロックチェーンネットワークを作成することもできます。パブリックブロックチェーンノードへのフルマネージド API オペレーション、シングルテナント (専用)、サーバーレスのマルチテナント API オペレーションなど、さまざまな方法でパブリックブロックチェーンを利用することができます。アクセス制御が重要なユースケースでは、フルマネージドのプライベート・ブロックチェーン・ネットワークを選択できます。標準化された API オペレーションにより、フルマネージド型のレジリエントなインフラストラクチャーですぐにスケーラビリティが得られるため、ブロックチェーンアプリケーションを構築できます。

AMB Access では、マルチテナントのブロックチェーン・ネットワーク・アクセス API オペレーションと、専用のブロックチェーン・ノードとネットワークという2つの異なるタイプのブロックチェーン・インフラストラクチャー・サービスを提供します。専用のブロックチェーン・インフラストラクチャーがあれば、パブリックの Ethereum ブロックチェーンノードとプライベート Hyperledger Fabric ブロックチェーンネットワークを自分用に作成して使用できます。しかし、AMB Access Bitcoin のようなマルチテナント型の API ベースの製品は、基盤となるブロックチェーン・ノード・インフラストラクチャーが顧客間で共有される API レイヤーの背後にある一連のビットコイン・ノードで構成されています。

ビットコインは、ネットワークのネイティブ暗号通貨であるビットコイン (BTC) peer-to-peer 建ての価値を持つ安全な取引を可能にする分散型ブロックチェーンネットワークです。ビットコイン・ネットワークは、個人、金融機関、フィンテック企業、政府などによって使用されています。ビットコイン・ネットワークは、交換媒体、投資商品、または登録データを保管する公的に検証可能で変更不可能な台帳です。Amazon Managed Blockchain (AMB) Access Bitcoin を使用すると、リージョナルエンドポイントを介してビットコインメインネットとテストネットネットワークのプールにアクセスできます。これにより、トランザクションを書き込んだり、台帳からデータを読み取ったり、Bitcoin Core ノードクライアントで利用可能な JSON-RPC リクエストを呼び出したりできます。サーバーレスのビットコインエンドポイントを使用すると、ビットコインノードのプロビジョニング、保守、負荷分散などの差別化されていない作業に投資する代わりに、アプリケーションの構築に集中できます。ビットコイン・ウォレットを構築する場合でも、仮想通貨取引所を構築する場合でも、ビットコイン・ブロックチェーン・データを分析する場合でも、AMB Access Bitcoin を使用してビットコイン・エンドポイントを通じて行うリクエストに対してのみ支払いが発生します。

## AMB Access ビットコインを初めて使用する方ですか？

AMB Access ビットコインを初めて使用する方は、まず以下のセクションを読むことをおすすめします。

- [主な概念:Amazon Managed Blockchain \(AMB\) アクセスビットコイン](#)
- [Amazon Managed Blockchain \(AMB\) Access Bitcoin の開始方法](#)
- [Amazon Managed Blockchain \(AMB\) によるビットコインのユースケースビットコインへのアクセス](#)
- [Amazon Managed Blockchain \(AMB\) によるビットコイン JSON RPC 対応ビットコイン](#)

# 主な概念: Amazon Managed Blockchain (AMB) アクセスビットコイン

## Note

このガイドは、読者がビットコインに不可欠な概念に精通していることを前提としています。これらの概念には、分散化、ノード、トランザクション、ウォレット proof-of-work、公開鍵と秘密鍵、半減法などが含まれます。Amazon Managed Blockchain (AMB) Access Bitcoin を使用する前に、[「ビットコイン開発ドキュメント」](#)と[「ビットコインをマスターする」](#)を確認することをお勧めします。

Amazon Managed Blockchain (AMB) Access Bitcoin を利用すると、ノードを含むビットコインインフラストラクチャをプロビジョニングして管理しなくても、ビットコインブロックチェーンにサーバーレスでアクセスできます。このマネージドサービスを利用すると、ビットコインネットワークにオンデマンドですばやくアクセスでき、総所有コストを削減できます。

AMB Access Bitcoinは、ウォレット機能を無効にした状態で、ビットコインコアクライアントを実行するフルノードを通じてビットコインネットワークへのアクセスを可能にし、複数のJSONリモートプロシージャ (JSON-RPC) 呼び出しをサポートします。ビットコイン JSON RPC を呼び出して、マネージドブロックチェーンが管理するビットコインノードと通信し、ビットコインネットワークと通信することができます。ビットコイン JSON RPC では、Amazon Managed Blockchain サービスを使用して、データのクエリやビットコインネットワークへのトランザクションの送信など、データの読み取りやトランザクションの書き込みを行うことができます。

## Important

ビットコインアドレスの作成、管理、使用、管理はお客様の責任となります。また、ビットコインアドレスの内容についても責任を負います。AWS Amazon Managed Blockchain 上のビットコインノードを使用してデプロイまたは呼び出されたトランザクションについては責任を負いません。

# Amazon Managed Blockchain (AMB) アクセスビットコインを使用する際の考慮事項と制限事項

## • サポートされているビットコインネットワーク

AMB Access ビットコインは以下のパブリックネットワークをサポートしています。

- **メインネット** — proof-of-work コンセンサスによって保護され、ビットコイン (BTC) 暗号通貨の発行と取引が行われるパブリックビットコインブロックチェーン。メインネットでの取引には実際の価値 (つまり、実際のコストがかかる) があり、公開されているブロックチェーンに記録されます。
- **テストネット** — テストネットは、テストに使用される代替ビットコインブロックチェーンです。テストネットコインは実際のビットコイン (BTC) とは別のもので、通常は価値がありません。

### Note

プライベートネットワークはサポートされていません。

## • サポートされるリージョン

このサービスでは以下のリージョンがサポートされています。

リージョン名	Code	リージョン
米国東部 (バージニア北部)	IAD	us-east-1
アジアパシフィック (東京)	NRT	ap-northeast-1
アジアパシフィック (ソウル)	アイコン	ap-northeast-2
アジアパシフィック (シンガポール)	SIN	ap-southeast-1
欧州 (アイルランド)	DUB	eu-west-1
欧州 (ロンドン)	LHR	eu-west-2

## • サービスエンドポイント



AMB Access ビットコインのサービスエンドポイントは次のとおりです。サービスに接続するには、サポートされているリージョンのいずれかを含むエンドポイントを使用する必要があります。

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

例 : `mainnet.bitcoin.managedblockchain.eu-west-2.amazonaws.com`

- マイニングはサポートされていません。

AMB アクセス・ ビットコインはビットコイン (BTC) マイニングをサポートしていません。

- 署名バージョン 4 ビットコイン JSON-RPC 呼び出しの署名

Amazon Managed Blockchain ビットコイン JSON RPC を呼び出す場合は、[署名バージョン 4 署名プロセスを使用して認証された](#) HTTPS 接続を介して呼び出すことができます。つまり、AWS アカウント内の承認された IAM プリンシパルのみがビットコイン JSON-RPC 呼び出しを行うことができます。そのためには、AWS 呼び出し時に認証情報 (アクセスキー ID とシークレットアクセスキー) を提供する必要があります。

#### Important

- ユーザー向けアプリケーションにはクライアント認証情報を埋め込まないでください。
- IAM ポリシーを使用して個々のビットコイン JSON RPC へのアクセスを制限することはできません。

- 未加工のトランザクションの送信のみがサポートされています。

`sendrawtransaction`JSON-RPC を使用して、ビットコインブロックチェーンの状態を更新するトランザクションを送信します。

- AWS CloudTrail ログイングサポート

ビットコイン JSON RPC CloudTrail を記録するように設定できます。詳細については、「[Amazon Managed Blockchain \(AMB\) によるビットコインイベントのログイング: AWS CloudTrail](#)」を参照してください。

# Amazon Managed Blockchain (AMB) Access Bitcoin のセットアップ

Amazon Managed Blockchain (AMB) Access Bitcoin を初めて使用する前に、このセクションの手順に従って を作成します。AWS アカウント。次の章では、AMB Access Bitcoin の使用を開始する方法について説明します。

## 前提条件と考慮事項

を使用する前に AWS を初めて使用する場合は、AWS アカウント。

### サインアップ: AWS

にサインアップするとき AWS、AWS アカウント はすべての に自動的にサインアップされます。AWS のサービス Amazon Managed Blockchain (AMB) Access Bitcoin を含む。サービスを実際に使用した分の料金のみが請求されます。

をお持ちの場合 AWS アカウント 既に、次のステップに進みます。をお持ちでない場合 AWS アカウント、次の手順を使用して作成します。

を作成するには AWS アカウント

1. <https://portal.aws.amazon.com/billing/サインアップ> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

にサインアップするとき AWS アカウント、AWS アカウントのルートユーザー が作成されます。ルートユーザーはすべての にアクセスできます AWS のサービス アカウントの および リソース。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用して [ルートユーザーアクセスが必要なタスク](#) を実行してください。

## 適切なアクセス許可を持つ IAM ユーザーを作成する

AMB Access Bitcoin を作成して使用するには、[が必要](#)です AWS Identity and Access Management (IAM) 必要な Managed Blockchain アクションを許可するアクセス許可を持つプリンシパル (ユーザーまたはグループ)。

Bitcoin JSON-RPC 呼び出しを実行できるのはプリンシパルのみです。Amazon Managed Blockchain で Bitcoin JSON-RPCs を呼び出す場合、[署名バージョン 4 の署名プロセス](#) を使用して認証された HTTPS 接続を介して呼び出すことができます。つまり、の認可された IAM プリンシパルのみが AWS アカウントは Bitcoin JSON-RPC 呼び出しを行うことができます。以下の手順に従ってください。AWS 認証情報 (アクセスキー ID とシークレットアクセスキー) は、呼び出しとともに提供する必要があります。

IAM ユーザーの作成方法については、「[での IAM ユーザーの作成](#)」を参照してください。[AWS アカウント](#)。アクセス許可ポリシーをユーザーにアタッチする方法の詳細については、「[ユーザーのアクセス許可の変更 IAM](#)」を参照してください。Access Bitcoin を操作するアクセス許可をユーザーに付与するために使用できる AMB アクセス許可ポリシーの例については、「[」](#)を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## のインストールと設定 AWS Command Line Interface

まだインストールしていない場合は、最新の AWS で使用するコマンドラインインターフェイス (CLI) AWS ターミナルからの [リソース](#)。詳細については、「[の最新バージョンのインストールまたは更新](#)」を参照してください。 [AWS CLI](#)。

### Note

CLI アクセスには、アクセスキー ID とシークレットアクセスキーが必要です。長期のアクセスキーの代わりに一時的な認証情報をできるだけ使用します。一時的な認証情報には、アクセスキー ID、シークレットアクセスキー、および認証情報の失効を示すセキュリティトークンが含まれています。詳細については、「[での一時的な認証情報の使用](#)」を参照してください。 [AWS IAM ユーザーガイドのリソース](#)。

# Amazon Managed Blockchain (AMB) Access Bitcoin の開始方法

Amazon Managed Blockchain (AMB) Access Bitcoin を使用してタスクを実行する方法については、このセクションの step-by-step チュートリアルを参照してください。これらの例では、いくつかの前提条件を満たす必要があります。Bitcoin AMB に初めてアクセスする場合は、このガイドの「セットアップ」セクションを参照して、これらの前提条件を満たしていることを確認してください。詳細については、「[Amazon Managed Blockchain \(AMB\) Access Bitcoin のセットアップ](#)」を参照してください。

## トピック

- [Bitcoin にアクセスするための IAM ポリシーを作成する JSON-RPCs](#)
- [を使用してアクセスRPCエディタで Bitcoin リモートプロシージャコール \(RPC\) AMB リクエストを行う AWS Management Console](#)
- [Make AMB Access Bitcoin JSON-RPC を使用して awscurl でリクエストを実行する AWS CLI](#)
- [Bitcoin の作成 JSON-RPC Node.js でのリクエスト](#)
- [で AMB Access Bitcoin を使用する AWS PrivateLink](#)

## Bitcoin にアクセスするための IAM ポリシーを作成する JSON-RPCs

Bitcoin Mainnet と Testnet のパブリックエンドポイントにアクセスして JSON-RPC 呼び出しを行うには、Amazon Managed Blockchain (KEY) Access Bitcoin に適切なアクセスIAM許可を持つユーザー認証情報 (AWS\_ACCESSKEY\_ID と AWS\_SECRETACCESS\_AMB) が必要です。を使用するターミナルで AWS CLI がインストールされている場合は、次のコマンドを実行して、両方の Bitcoin エンドポイントにアクセスするための IAM ポリシーを作成します。

```
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

前の例では、Bitcoin Mainnet と Testnet の両方にアクセスできます。特定のエンドポイントにアクセスするには、次のActionコマンドを使用します。

- "managedblockchain:InvokeRpcBitcoinMainnet"
- "managedblockchain:InvokeRpcBitcoinTestnet"

ポリシーを作成したら、そのポリシーをIAMユーザーのロールにアタッチして有効にします。左 AWS Management Console、IAMサービスに移動し、IAMユーザーに割り当てられたロールAmazonManagedBlockchainBitcoinAccessにポリシーをアタッチします。詳細については、[「ロールの作成」とIAM「ユーザーへの割り当て」](#)を参照してください。

## を使用してアクセスRPCエディタで Bitcoin リモートプロシージャコール (RPC) AMB リクエストを行う AWS Management Console

でリモートプロシージャコール (RPCs) を編集して送信できます。AWS Management Console AMB アクセスを使用する。これらの を使用するとRPCs、Bitcoin ネットワークでデータの読み取り、書き込み、トランザクションの送信を行うことができます。

### Example

次の例は、blockhashを使用して00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 getBlock に関する情報を取得する方法を示していますRPC。強調表示された変数を独自の入力に置き換えるか、リストされている他のRPC方法のいずれかを選択して、必要な関連する入力を入力します。

1. で Managed Blockchain コンソールを開きます <https://console.aws.amazon.com/managedblockchain/>。
2. RPC エディタ を選択します。
3. リクエストセクションで、ブロックチェーンネットワーク *BITCOIN\_MAINNET*として を選択します。
4. メソッド *getblock*として を選択します。RPC
5. ブロック番号 *00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09*としてを入力し、詳細度 *0*として を選択します。
6. その後で、[送信RPC] を選択します。
7. このページの「レスポンス」セクションに結果が表示されます。その後、詳細な分析やアプリケーションのビジネスロジックでの使用のために、完全な raw トランザクションをコピーできます。

詳細については、[RPCsAMB「Access Bitcoin でサポートされている」](#)を参照してください。

## Make AMB Access Bitcoin JSON-RPC を使用して awscurl でリクエストを実行する AWS CLI

### Example

[署名バージョン 4 \(SigV4\)](#) を使用して IAM ユーザー認証情報を使用してリクエストに署名し、Bitcoin JSON-RPC AMB Access Bitcoin エンドポイントを呼び出します。[awscurl](#) コマンドラインツールは、へのリクエストの署名に役立ちます。AWS SigV4 を使用する のサービス。詳細については、[awscurl README.md](#) を参照してください。

オペレーティングシステムに適した方法を使用して awscurl をインストールします。macOS では、HomeBrew が推奨アプリケーションです。

```
brew install awscurl
```

を既にインストールして設定している場合 AWS CLI、IAM ユーザー認証情報とデフォルトのAWS リージョンは環境で設定され、awscurl にアクセスできます。awscurl を使用して、を呼び出して Bitcoin Mainnet と Testnet getblock の両方にリクエストを送信しますRPC。この呼び出しは、情報を取得するブロックハッシュに対応する文字列パラメータを受け入れます。

次のコマンドは、params配列のブロックハッシュを使用して、ヘッダーを取得する特定のブロックを選択することで、Bitcoin Mainnet からブロックヘッダーデータを取得します。この例では、us-east-1エンドポイントを使用します。これを任意のBitcoin JSON-RPC および に置き換えることができます。AWS Amazon Managed Blockchain (AMB) Access Bitcoin でサポートされているリージョン。さらに、testnet コマンドでを mainnetに置き換えることで、Mainnet ではなく Testnet ネットワークに対してリクエストを行うことができます。

```
awscurl -X POST -d '{ "jsonrpc": "1.0", "id": "getblockheader-curltest", "method": "getblockheader", "params": ["00000000000000000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0"] }' --service managedblockchain https://mainnet.bitcoin.managedblockchain.us-east-1.amazonaws.com --region us-east-1 -k
```

結果には、ブロックヘッダーの詳細と、リクエストされたブロックに含まれるトランザクションハッシュのリストが含まれます。次の例を参照してください。

```
{"result":{"hash":"000000000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0", "confirmations":2, "height":799243, "version":664485888, "versionHex":"279b4000", "merkleroot":"568e79752e1921ecf40c961435abb41bc5700fe2833ecadc4abfc2f615ddc1b8", "time":1689684290, "mediantime":1689681317, "nonce":2091174943, "bits":"17053894", "difficulty":53911173001054.59, "chainwork":"000000000000000000000000000000000000000000000000000000004f375cf72ff64e2404c1589c", "nTx":2135, "previousblockhash":"00000000000000000002ffe4efe07ae74ec8b92c7696f5e12b5da506f015ba6b", "nextblockhash":"000000000000000000000038f05ddcf3f483fdb74f4be606c022bcb673424fa4ca"}, "error":null, "id":"curltest"}
```

## Bitcoin の作成 JSON-RPC Node.js でのリクエスト

を使用して Bitcoin Mainnet および Testnet エンドポイントHTTPSにアクセスし、[Node.js のネイティブ https モジュール](#)を使用してJSONをRPCAPI呼び出すか、などのサードパーティーライブラリを使用して署名付きリクエストを送信できます[AXIOS](#)。次の例は、Bitcoin JSON-RPC AMB Access Bitcoin エンドポイントへのリクエストを行う方法を示しています。

### Example

このサンプル Node.js スクリプトを実行するには、次の前提条件を適用します。

1. マシンにノードバージョンマネージャー (nvm) と Node.js がインストールされている必要があります。OS のインストール手順については、[「 」を参照してください](#)。
2. `node --version` コマンドを使用して、Node バージョン 14 以降を使用していることを確認します。必要に応じて、`nvm install 14` コマンドの後に `nvm use 14` コマンドを使用して、バージョン 14 をインストールできます。
3. 環境変数 `AWS_ACCESS_KEY_ID` および には、アカウントに関連付けられている認証情報が含まれている `AWS_SECRET_ACCESS_KEY` 必要があります。環境変数には `AMB`、Access Bitcoin エンドポイントが含まれている `AMB_HTTP_ENDPOINT` 必要があります。

次のコマンドを使用して、これらの変数をクライアントの文字列としてエクスポートします。次の文字列の強調表示された値を、IAM ユーザーアカウントの適切な値に置き換えます。

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

すべての前提条件を満たしたら、エディタを使用して次の `package.json` ファイルと `index.js` スクリプトをローカル環境にコピーします。

`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',
```



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

### Note

前のスクリプトのサンプルリクエストは、[Make AMB Access Bitcoin JSON-RPC を使用して awscli でリクエストを実行する AWS CLI](#)例と同じ入力パラメータブロックハッシュを使用してgetblock呼び出しを行います。他の呼び出しを行うには、スクリプト内の rpc オブジェクトを別の Bitcoin JSON- で変更しますRPC。ホストプロパティオプションを Bitcoin に変更testnetして、そのエンドポイントで呼び出しを行うことができます。

## で AMB Access Bitcoin を使用する AWS PrivateLink

AWS PrivateLink は、可用性が高くスケーラブルなテクノロジーであり、 のサービスに のように VPCプライベートに接続するために使用できますVPC。インターネットゲートウェイ、NATデバイス、パブリック IP アドレス、AWS Direct Connect 接続、または AWS プライベートサブネットからサービスと通信するための Site-to-Site VPN接続。の詳細については、「」を参照してください。AWS PrivateLink または を設定 AWS PrivateLink、「 とは」を参照してください。[AWS PrivateLink?](#)

Bitcoin JSON-RPC 経由で Bitcoin AMB にアクセスするためのリクエストを送信できます AWS PrivateLink VPC エンドポイントを使用する。このプライベートエンドポイントへのリクエストはオープンインターネット経由で渡されないため、同じ SigV4 認証を使用して Bitcoin エンドポイントに直接リクエストを送信できます。詳細については、「[アクセス](#)」を参照してください。[AWS による サービス AWS PrivateLink.](#)

サービス名 については、 で Amazon Managed Blockchain を探します。AWS サービス列。詳細については、「[」を参照してくださいAWS と統合する のサービス AWS PrivateLink.](#) エンドポイントのサービス名は、 の形式になります `com.amazonaws.AWS-REGION.managedblockchain.bitcoin.NETWORK-TYPE`。

例: `com.amazonaws.us-east-1.managedblockchain.bitcoin.testnet`。

# Amazon Managed Blockchain (AMB) によるビットコインのユースケース

## ビットコインへのアクセス

このトピックでは、AMB Access ビットコインのユースケースのリストを提供します。

### トピック

- [BTC を送受信するためのビットコイン \(BTC\) ウォレットを構築する](#)
- [ビットコインブロックチェーン上のアクティビティを分析します。](#)
- [ビットコインkey pair を使用して署名されたメッセージを確認する](#)
- [ビットコインメモプールを調べてください。](#)

## BTC を送受信するためのビットコイン (BTC) ウォレットを構築する

ビットコインネットワーク上のネイティブ暗号通貨であるBTCは、ネットワークのセキュリティモデルに欠かせないコンポーネントです。また、商品や交換媒体としても機能し、機関、企業、個人に広く利用されています。そのため、多くのウォレットアプリケーションは、ビットコイン・ブロックチェーンとのやり取りをビットコイン・ノードに依存しています。これらのアプリケーションは、特定のアドレスセットの未使用アウトプット (UTXO) の残高を計算し、トランザクションに署名してビットコインネットワークに送信し、過去のトランザクションに関するデータを取得します。

以下は、Amazon Managed Blockchain (AMB) アクセスビットコインが BTC ウォレットトランザクションでサポートしているビットコイン JSON RPC のサンプルです。

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

詳細については、「[サポートされている JSON RPC](#)」を参照してください。

## ビットコインブロックチェーン上のアクティビティを分析します。

getchaintxstats JSON-RPC メソッドを使用して、ビットコインブロックチェーン上のトランザクションアクティビティの量を分析できます。この JSON-RPC では、1 秒あたりの平均トランザクションレート、合計トランザクション数、ブロック数などのメトリクスにアクセスできます。必要に応じて、ブロック番号のウィンドウやブロックハッシュを区切り文字として定義して、ネットワーク内の特定のブロックセットの統計を計算することもできます。

詳細については、「[サポートされている JSON RPC](#)」を参照してください。

## ビットコインkey pair を使用して署名されたメッセージを確認する

ビットコインウォレットには、キーペアを構成する秘密鍵と公開鍵があります。これらの鍵は取引の署名に使用され、ブロックチェーン上でユーザーのIDとして使用されます。公開鍵は、標準化された英数字識別子 (長さ27~34文字) であるアドレスを作成するために使用されます。これらのアドレスは BTC アウトプットの受信やトランザクションやメッセージの処理に使用されます。

ビットコインウォレットでは、ユーザーは暗号を使ってメッセージに署名したり検証したりすることもできます。このプロセスは、特定のウォレットアドレスとそれに関連するBTCの所有権を証明するためによく使用されます。verifymessageBitcoin JSON-RPCを使うことで、別のウォレットが署名したメッセージの信憑性と有効性をチェックできます。具体的には、ビットコインノードを使用して、署名されたメッセージ自体に含まれる公開鍵から派生したアドレスに対応する秘密鍵を使用してメッセージが署名されているかどうかを確認できます。

詳細については、「[サポートされている JSON RPC](#)」を参照してください。

## ビットコインメモプールを調べてください。

保留中のトランザクションを追跡したり、保留中のすべてのトランザクションのリストを取得したり、トランザクションがどこから来たのかを調べたりするために、多くのアプリケーションがメモリプールにアクセスする必要があります。getrawmempoolそのためには、やのようなビットコイン JSON RPC がありgetmempoolancestorsgetmempoolentry、このアクティビティをサポートしています。これらのビットコイン JSON RPC は、アプリケーションが必要な情報をメモリプールから取得するのに役立ちます。

Amazon Managed Blockchain (AMB) Access Bitcoin は、testmempoolacceptビットコイン JSON RPCS もサポートしています。これにより、トランザクションがプロトコルルールを満たしているかどうか、また送信前にノードによって承認されるかどうかを確認できます。ウォレット、取引所、

およびビットコインブロックチェーンに直接トランザクションを送信するその他のエンティティは、これらのビットコイン JSON RPC を利用します。

詳細については、「[サポートされている JSON RPC](#)」を参照してください。

# Amazon Managed Blockchain (AMB) によるビットコイン JSON RPC 対応ビットコイン

このトピックでは、マネージドブロックチェーンがサポートするビットコイン JSON RPC のリストと参照先を紹介します。サポートされている各 JSON-RPC には、その使用方法についての簡単な説明があります。

## Note

- マネージドブロックチェーン上のビットコイン JSON-RPC は、[署名バージョン 4 \(SigV4\) 署名プロセスを使用して認証できます](#)。つまり、AWS アカウント内の承認された IAM プリンシパルのみがビットコイン JSON RPC を使用して操作できるということです。AWS 呼び出し時に認証情報 (アクセスキー ID とシークレットアクセスキー) を指定します。
- HTTP レスポンスが 10 MB を超えると、エラーになります。これを修正するには、圧縮ヘッダーをに設定する必要があります Accept-Encoding:gzip。その後、クライアントが受信する圧縮レスポンスには、Content-Type: application/jsonとというヘッダーが含まれます Content-Encoding: gzip。
- Amazon Managed Blockchain (AMB) アクセスビットコインは、不正な形式の JSON-RPC リクエストに対して 400 エラーを生成します。
- sendrawtransactionJSON-RPC を使用して、ビットコインブロックチェーンの状態を更新するトランザクションを送信します。
- AMB Access Bitcoinには、1リージョンあたり1秒あたり100リクエスト (RPS) というデフォルトのリクエスト制限があります。NETWORK\_TYPE AWS

クォータを増やすには、サポートに連絡する必要があります。AWS AWS Support に連絡するには、[AWS サポートセンターコンソールにサインインしてください](#)。[ケースを作成] を選択します。[テクニカル] を選択します。マネージド・ブロックチェーンをサービスとして選択してください。カテゴリとして「アクセス:ビットコイン」を選択し、「重要度」として「一般ガイダンス」を選択します。件名に「RPC クォータ」を入力し、「説明」テキストボックスに「RPC クォータ」と入力し、ニーズに合ったクォータ制限を地域ごとのビットコインネットワークあたりの RPS ( RPS ) で記載します。ケースを送信してください。

## サポートされている JSON RPC

AMB アクセスビットコインは、以下のビットコイン JSON RPC をサポートしています。サポートされている各コールには、その使用法の簡単な説明があります。

カテゴリ	JSON-RPC	説明
<a href="#">ブロックチェーンRPC</a>	<a href="#">最適なブロックハッシュを取得</a>	最も処理が行き届いていて完全に検証されたチェーンの中で最良の (先端) ブロックのハッシュを返します。
	<a href="#">getblock</a>	verbosity が 0 の場合、ブロック 'hash' のシリアル化されたデータを 16 進数でエンコードした文字列を返します。verbosity が 1 の場合、ブロック 'hash' に関する情報を含むオブジェクトを返します。verbosity が 2 の場合、ブロック 'hash' に関する情報と各トランザクションに関する情報を含むオブジェクトを返します。verbosity が 3 の場合、ブロックの「ハッシュ」に関する情報と、入力情報を含む各トランザクションに関する情報を含む Object を返します。prevout
	<a href="#">getblockchaininfo</a>	ブロックチェーン処理に関するさまざまな状態情報を含むオブジェクトを返します。
	<a href="#">get/ブロック/カウント</a>	最も作業が多く、完全に検証されたチェーンの高さを返します。ジェネシスブロックの高さは 0 です。
	<a href="#">[ブロック/フィルターを取得]</a>	ブロックハッシュを使用して特定のブロックの BIP 157 コンテンツフィルタを取得します。
	<a href="#">get/ブロック/ハッシュ</a>	best-block-chain 指定した高さのブロックのハッシュを返します。
	<a href="#">ブロックヘッダを取得する。</a>	verbose が false の場合、ブロックヘッダー 'hash' のデータをシリアル化して 16 進数でエ



カテゴリ	JSON-RPC	説明
		ンコードした文字列を返します。verbose が true の場合、ブロックヘッダー 'hash' に関する情報を含むオブジェクトを返します。
	<a href="#">getblockstats</a>	特定のウィンドウのブロックごとの統計を計算します。金額はすべてサトシ単位です。高さによっては刈り込みでは効きません。
	<a href="#">チェーンチップを入手してください。</a>	メインチェーンや孤立したブランチなど、ブロックツリー内のすべての既知のチップに関する情報を返します。
	<a href="#">getchaintxstats</a>	チェーン内のトランザクションの総数と割合に関する統計を計算します。
	<a href="#">難易度が上がる</a>	proof-of-work 難易度を最小難易度の倍数で返します。
	<a href="#">@mempool の祖先を取得する。</a>	txid がメモリプールにある場合は、メモリプール内の上位オブジェクトをすべて返します。
	<a href="#">mempool の下位オブジェクトを取得します。</a>	txid がメモリプールにある場合は、メモリプール内のすべての下位オブジェクトを返します。
	<a href="#">mempool エントリを取得します。</a>	指定したトランザクションの mempool データを返します。
	<a href="#">getmempoolinfo</a>	TX メモリプールのアクティブ状態に関する詳細を返します。

カテゴリ	JSON-RPC	説明
	<a href="#">getrawmempool</a>	<p>メモリプール内のすべてのトランザクション ID を、文字列トランザクション ID の JSON 配列として返します。</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p><code>verbose = true</code> はサポートされていません。</p> </div>
	<a href="#">gettxout</a>	未使用のトランザクション出力に関する詳細を返します。
	<a href="#">.txoutproof を取得してください。</a>	「txid」がブロックに含まれていたことの証明を16進数でエンコードして返します。
<a href="#">ロートランザクション (RPC)</a>	<a href="#">未加工トランザクションの作成</a>	与えられたインプットを使ってトランザクションを作成し、新しいアウトプットを作成します。
	<a href="#">トランザクションをデコードします。</a>	シリアル化され、16進数でエンコードされたトランザクションを表す JSON オブジェクトを返します。
	<a href="#">デコードスクリプト</a>	16進数でエンコードされたスクリプトをデコードします。
	<a href="#">未処理のトランザクションを取得</a>	未加工のトランザクションデータを返します。
	<a href="#">未処理のトランザクションを送信</a>	未加工のトランザクション (シリアル化、16進数エンコード) をローカルノードとネットワークに送信します。

カテゴリ	JSON-RPC	説明
	<a href="#">テスト/メモリプール/受け入れ</a>	未処理のトランザクション (シリアル化、16 進数エンコード) が mempool で受け入れられるかどうかを示す mempool 受け入れテストの結果を返します。トランザクションがコンセンサスルールまたはポリシールールに違反していないかをチェックします。
<a href="#">RPC まで</a>	<a href="#">マルチサイトを作成</a>	m キーの署名を必要としないマルチ署名アドレスを作成します。
	<a href="#">スマート料金の見積もり</a>	トランザクションが確認を開始するまでに必要な KB あたりのおおよその料金を conf_target ブロック内で見積もり、その見積もりが有効なブロック数を返します。BIP 141 で定義されている仮想トランザクションサイズを使用します (監視データは割引されます)。
	<a href="#">住所を検証します。</a>	指定したビットコインアドレスに関する情報を返します。
	<a href="#">検証/メッセージ</a>	署名されたメッセージを検証します。

# Amazon Managed Blockchain (AMB) のセキュリティビットコインへのアクセス

AWS クラウドセキュリティは最優先事項です。AWS お客様は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

セキュリティは、AWS お客様とお客様との間で共有される責任です。[責任分担モデル](#)では、これをクラウドのセキュリティとクラウドのセキュリティの両方と表現しています。

- **クラウドのセキュリティ** — AWS AWS AWS クラウドクラウド内でサービスを実行するインフラストラクチャを保護する責任があります。AWS また、安全に使用できるサービスも提供します。サードパーティーの監査人は、[AWS コンプライアンスプログラム](#) の一環として、セキュリティの有効性を定期的にテストおよび検証します。Amazon Managed Blockchain (AMB) Access Bitcoin に適用されるコンプライアンスプログラムについては、「[AWS コンプライアンスプログラムによる対象サービス](#)」を参照してください。
- **クラウドのセキュリティ** — お客様の責任は、AWS 使用するサービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律や規制といった他の要因についても責任を担います。

データ保護、認証、アクセス制御を提供するために、Amazon Managed Blockchain は、AWS マネージドブロックチェーンで実行されているオープンソースフレームワークの機能と機能を使用しています。

このドキュメントは、AMB Access Bitcoin を使用する際に責任分担モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目標を満たすように AMB Access Bitcoin を設定する方法を示しています。また、AMB Access AWS ビットコインリソースの監視と保護に役立つ他のサービスの使い方についても学びます。

## トピック

- [Amazon Managed Blockchain \(AMB\) Access Bitcoin でのデータ保護](#)
- [Amazon Managed Blockchain \(AMB\) Access Bitcoin の Identity and Access Management](#)

# Amazon Managed Blockchain (AMB) Access Bitcoin でのデータ保護

- AWS [責任共有モデル](#)、Amazon Managed Blockchain (AMB) Access Bitcoin でのデータ保護に適用されます。このモデルで説明されているように、AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。AWS のサービス 使用する。データプライバシーの詳細については、「[データプライバシーFAQ](#)」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。[AWS の責任共有モデルとGDPR](#) ブログ記事 AWS セキュリティブログ。

データ保護の目的で、 を保護することをお勧めします。AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management (IAM)。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が 必要で、1.3 TLS をお勧めします。
- で API とユーザーアクティビティのログ記録を設定する AWS CloudTrail。CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。AWS アクティビティ、「」の「[証 CloudTrail 跡の使用](#)」を参照してください。AWS CloudTrail ユーザーガイド。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介して API、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、AMB Access Bitcoin または他の を使用する場合も同様です。AWS のサービス コンソール、API、AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログ

に使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

## データ暗号化

データ暗号化は、権限のないユーザーがブロックチェーンネットワークおよび関連するデータストレージシステムからデータを読み取るのを防ぐのに役立ちます。これには、ネットワークを移動するときに傍受される可能性のあるデータが含まれます。これは、転送中のデータと呼ばれます。

## 転送中の暗号化

デフォルトでは、Managed Blockchain は HTTPS/TLS 接続を使用して、 を実行するクライアントコンピュータから送信されるすべてのデータを暗号化します。AWS CLI から AWS サービスエンドポイント。

HTTPS/ の使用を有効にするために何もする必要はありませんTLS。個人に対して明示的に無効にしない限り、常に有効になります。AWS CLI コマンドを使用して `--no-verify-ssl` コマンドを実行します。

## Amazon Managed Blockchain (AMB) Access Bitcoin の Identity and Access Management

AWS Identity and Access Management ( IAM) は AWS のサービス 管理者は へのアクセスを安全に制御できます。AWS リソースの使用料金を見積もることができます。IAM 管理者は、誰を認証 (サインイン) し、誰に AMB Access Bitcoin リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は AWS のサービス 追加料金なしで使用できます。

### トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [Amazon Managed Blockchain \(AMB\) Access Bitcoin と の連携方法 IAM](#)
- [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)
- [Amazon Managed Blockchain \(AMB\) Access Bitcoin Identity and Access のトラブルシューティング](#)

## 対象者

の使用方法 AWS Identity and Access Management (IAM) は、AMB Access Bitcoin で行う作業によって異なります。

サービスユーザー - AMB Access Bitcoin サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AMB Access Bitcoin 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておく、管理者に適切な許可をリクエストするうえで役立ちます。AMB Access Bitcoin の機能にアクセスできない場合は、「」を参照してください[Amazon Managed Blockchain \(AMB\) Access Bitcoin Identity and Access のトラブルシューティング](#)。

サービス管理者 - 社内の AMB Access Bitcoin リソースを担当している場合は、通常、Access Bitcoin AMB へのフルアクセスがあります。サービスユーザーがどの AMB Access Bitcoin 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、の基本概念を理解してくださいIAM。会社で AMB Access Bitcoin IAMを使用する方法の詳細については、「」を参照してください[Amazon Managed Blockchain \(AMB\) Access Bitcoin との連携方法 IAM](#)。

IAM 管理者 - IAM管理者は、Access Bitcoin AMB へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。で使用できる AMB Access Bitcoin アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してください[Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## アイデンティティを使用した認証

認証は、にサインインする方法です。AWS ID 認証情報を使用する。認証されている必要があります (にサインインします AWSとして) AWS アカウントのルートユーザー、IAM ユーザーとして、または IAMロールを引き受ける方法。

にサインインできます。AWS ID ソースを通じて提供された認証情報を使用して、フェデレーテッド ID としてを指定します。AWS IAM Identity Center (IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーテッド ID の例です。フェデレーテッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。にアクセスする場合 AWS フェデレーションを使用すると、間接的にロールを引き受けることになります。



ユーザーのタイプに応じて、にサインインできます。AWS Management Console または AWS アクセスポータル。へのサインインの詳細については、「」を参照してください。AWS [「にサインインする方法」](#)を参照してください。[AWS アカウント](#) ( )AWS サインイン ユーザーガイド。

アクセスする場合 AWS プログラムにより、AWS は、認証情報を使用してリクエストに暗号で署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) を提供します。を使用しない場合 AWS ツールの場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストに自分で署名する方法の詳細については、[「署名」を参照してください](#)。[AWS API IAMユーザーガイドのリクエスト](#)。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、[MFA](#)などです AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「」の[「多要素認証」](#)を参照してください。AWS IAM Identity Center ユーザーガイドと [での多要素認証 \(MFA\) の使用 AWS 「」](#) (IAM ユーザーガイド) を参照してください。

## AWS アカウント ルートユーザー

を作成する場合 AWS アカウントでは、すべてのへの完全なアクセス権を持つ1つのサインインアイデンティティから始めます。AWS のサービス アカウントの および リソース。この ID はと呼ばれます。AWS アカウント root ユーザー とには、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAMユーザーガイド」の[「ルートユーザーの認証情報を必要とするタスク」](#)を参照してください。

## フェデレーテッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用してにアクセスすることを要求します。AWS のサービス一時的な認証情報を使用する。

フェデレーテッド ID は、エンタープライズユーザーディレクトリのユーザー、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリ、またはにアクセスする任意のユーザー AWS のサービス ID ソースを通じて提供された認証情報を使用する。フェデレーテッド ID がにアクセスする場合 AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。



一元的なアクセス管理を行うには、を使用することをお勧めします。AWS IAM Identity Center。Identity Center でユーザーとグループを作成するか、独自の IAM ID ソース内のユーザーとグループのセットに接続して同期し、すべてので使用できます。AWS アカウント および アプリケーション。IAM Identity Center の詳細については、「」の[IAM 「Identity Center とは」](#)を参照してください。AWS IAM Identity Center ユーザーガイド。

## IAM ユーザーとグループ

[IAM ユーザー](#)は 内のアイデンティティです。AWS アカウント 1 人のユーザーまたはアプリケーションに対して特定のアクセス許可を持つ。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「[ユーザーガイド](#)」の「[長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM](#)」を参照してください。

[IAM グループ](#)は、IAMユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「[ユーザーガイド](#)」の[IAM 「\(ロールの代わりに\) ユーザーを作成する場合IAM](#)」を参照してください。

## IAM ロール

[IAM ロール](#)は 内のアイデンティティです。AWS アカウント 特定のアクセス許可を持つ。これは IAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。で一時的に IAMロールを引き受けることができます。AWS Management Console [ロールを切り替えます](#)。を呼び出すことでロールを引き受けることができます。AWS CLI または AWS API オペレーション、またはカスタムの使用URL。ロールの使用の詳細については、「[ユーザーガイド](#)」の[IAM 「ロールの使用IAM](#)」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーテッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、[「ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」](#)を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAM Identity Center はアクセス許可セットをのロールに関連付けますIAM。アクセス許可セットの詳細については、[「」の「アクセス許可セット」](#)を参照してください。AWS IAM Identity Center ユーザーガイド。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、AWS のサービスでは、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、[「ユーザーガイド」の「でのクロスアカウントリソースアクセスIAMIAM」](#)を参照してください。
- クロスサービスアクセス – 一部 AWS のサービス 他の の機能を使用する AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用します。AWS のサービス、 リクエストとの組み合わせ AWS のサービス ダウンストリームサービスにリクエストを行う。FAS リクエストは、他の とのやり取りを必要とするリクエストをサービスが受信した場合にのみ行われます。AWS のサービス または完了するリソース。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、[「転送アクセスセッション」](#)を参照してください。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAMロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、[「にアクセス許可を委任するロールの作成」](#)を参照してください。[AWS のサービス「」](#) (IAM ユーザーガイド) を参照してください。

- サービスにリンクされたロール – サービスにリンクされたロールは、にリンクされたサービスロールの一種です。AWS のサービス。このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールが に表示されます。AWS アカウント とは サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 を作成しているアプリケーションの一時的な認証情報を管理できます。AWS CLI または AWS API リクエスト。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。を割り当てるには AWS EC2 インスタンスにロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「[ユーザーガイド](#)」の「[IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM](#)」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、「[ユーザーガイド](#)」の「[\(ユーザーではなく\) IAMロールを作成する場合IAM](#)」を参照してください。

## ポリシーを使用したアクセスの管理

でアクセスをコントロールする AWS ポリシーを作成して にアタッチする AWS ID またはリソース。ポリシーは のオブジェクトです。AWS ID またはリソースに関連付けられている場合、そのアクセス許可を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは に保存されます。AWS JSON ドキュメントとして。JSON ポリシードキュメントの構造と内容の詳細については、「[ユーザーガイド](#)」の[JSON「ポリシーの概要IAM](#)」を参照してください。

管理者は を使用できます AWS JSON ポリシー。誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、iam:GetRoleアクションを許可するポリシーがあるとします。そのポリシー

を持つユーザーは、 からロール情報を取得できます。AWS Management Console、AWS CLI、または AWS API。

## アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「ユーザーガイド」の [IAM「ポリシーの作成IAM」](#) を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです。AWS アカウント。管理ポリシーには以下が含まれます。AWS 管理ポリシーとカスタマー管理ポリシー。管理ポリシーとインラインポリシーのどちらかを選択する方法については、IAM ユーザーガイドの [「管理ポリシーとインラインポリシーの選択」](#) を参照してください。

## リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチする JSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーテッドユーザー、または AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。は使用できません AWS リソースベースのポリシーIAMの からの マネージドポリシー。

## アクセスコントロールリスト (ACLs )

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、AWS WAF、および Amazon VPCは、 をサポートする のサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの [「アクセスコントロールリスト \(ACL\) の概要」](#) を参照してください。

## その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- **アクセス許可の境界** – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAMユーザーガイド」の「[IAMエンティティのアクセス許可の境界](#)」を参照してください。
- **サービスコントロールポリシー (SCPs)** – SCPsは、の組織または組織単位 (OU) の最大アクセス許可を指定するJSONポリシーです。AWS Organizations. AWS Organizations は、複数のをグループ化して一元管理するためのサービスです。AWS アカウント お客様のビジネスが所有する。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します。AWS アカウントのルートユーザー。Organizations との詳細についてはSCPs、「」の「[サービスコントロールポリシー](#)」を参照してください。AWS Organizations ユーザーガイド。
- **セッションポリシー** - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合があります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「ユーザーガイド」の「[セッションポリシーIAM](#)」を参照してください。

## 複数のポリシータイプ

1つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。方法を学ぶには AWS は、複数のポリシータイプが関与する場合にリクエストを許可するかどうかを決定します。「ユーザーガイド」の「[ポリシー評価ロジックIAM](#)」を参照してください。

## Amazon Managed Blockchain (AMB) Access Bitcoin と の連携方法 IAM

IAM を使用して Access Bitcoin AMB へのアクセスを管理する前に、Access Bitcoin AMB で使用できるIAM機能を確認してください。

### IAM Amazon Managed Blockchain (AMB) Access Bitcoin で使用できる の機能

IAM 機能	AMB Bitcoin サポートにアクセスする
<a href="#">アイデンティティベースのポリシー</a>	あり
<a href="#">リソースベースのポリシー</a>	なし
<a href="#">ポリシーアクション</a>	あり
<a href="#">ポリシーリソース</a>	いいえ
<a href="#">ポリシー条件キー</a>	なし
<a href="#">ACLs</a>	なし
<a href="#">ABAC (ポリシー内のタグ)</a>	なし
<a href="#">一時的な認証情報</a>	いいえ
<a href="#">プリンシパル権限</a>	いいえ
<a href="#">サービスロール</a>	いいえ
<a href="#">サービスリンクロール</a>	なし

Bitcoin およびその他の AMB へのアクセス方法の概要を把握するには AWS のサービスはほとんどの IAM機能で動作します。「」を参照してください。 [AWS ユーザーガイドIAM](#)の「と連携する IAM のサービス」。

### AMB Access Bitcoin のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり



ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「ユーザーガイド」の [IAM「ポリシーの作成IAM」](#) を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「ユーザーガイド」の「[IAMJSONポリシー要素のリファレンスIAM](#)」を参照してください。

## AMB Access Bitcoin のアイデンティティベースのポリシーの例

AMB Access Bitcoin アイデンティティベースのポリシーの例を表示するには、「」を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## AMB Access Bitcoin 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。リソースベースのポリシーの例としては、IAM ロール信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーテッドユーザー、または AWS のサービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーで、アカウント全体または別のアカウントの IAM エンティティをプリンシパルとして指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、リソースにアクセスするためのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさ

らに付与する必要はありません。詳細については、「[ユーザーガイド](#)」の「[でのクロスアカウントリソースアクセスIAMIAM](#)」を参照してください。

## AMB Access Bitcoin のポリシーアクション

ポリシーアクションのサポート: あり

管理者は を使用できます AWS JSON ポリシー。誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションは通常、関連付けられていると同じ名前です。AWS API オペレーション。一致するAPIオペレーションを持たないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AMB Access Bitcoin アクションのリストを確認するには、「[サービス認証リファレンス](#)」の「[Amazon Managed Blockchain \(AMB\) Access Bitcoin で定義されるアクション](#)」を参照してください。

AMB Access Bitcoin のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
managedblockchain:
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

ワイルドカード (\*) を使用して複数アクションを指定できます。例えば、InvokeRpcBitcoin という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。



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

AMB Access Bitcoin アイデンティティベースのポリシーの例を表示するには、「」を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## AMB Access Bitcoin のポリシーリソース

ポリシーリソースのサポート： いいえ

管理者は を使用できます AWS JSON ポリシー。誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、[Amazon リソースネーム \(ARN\) を使用してリソース](#)を指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (\*) を使用します。

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

AMB Access Bitcoin リソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」の「[Amazon Managed Blockchain \(AMB\) Access Bitcoin で定義されるリソース](#)」を参照してください。各リソースARNの を指定できるアクションについては、「[Amazon Managed Blockchain \(AMB\) Access Bitcoin で定義されるアクション](#)」を参照してください。

AMB Access Bitcoin アイデンティティベースのポリシーの例を表示するには、「」を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## AMB Access Bitcoin のポリシー条件キー

サービス固有のポリシー条件キーをサポート： いいえ

管理者は `Condition` を使用できます AWS JSON ポリシー。誰が何にアクセスできるかを指定します。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。イコールや未満などの [条件演算子](#) を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

ステートメントで複数の `Condition` 要素を指定するか、単一の `Condition` 要素で複数のキーを指定する場合は、AWS は論理 AND オペレーションを使用してそれら进行评估します。1 つの条件キーに複数の値を指定する場合は、AWS は論理 OR オペレーションを使用して条件进行评估します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、リソースに IAM ユーザー名でタグ付けされている場合にのみ、リソースへのアクセス許可を IAM ユーザーに付与できます。詳細については、「[ユーザーガイド](#)」の [IAM 「ポリシー要素: 変数とタグ IAM」](#) を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべてを表示するには AWS グローバル条件キー、「`aws:iam:*`」を参照してください。[AWS IAM ユーザーガイドのグローバル条件コンテキストキー](#)。

AMB Access Bitcoin の条件キーのリストを確認するには、「[サービス認証リファレンス](#)」の「[Amazon Managed Blockchain \(AMB\) Access Bitcoin の条件キー](#)」を参照してください。条件キーを使用できるアクションとリソースについては、「[Amazon Managed Blockchain \(AMB\) Access Bitcoin で定義されるアクション](#)」を参照してください。

AMB Access Bitcoin アイデンティティベースのポリシーの例を表示するには、「`aws:iam:*`」を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin のアイデンティティベースのポリシーの例](#)。

## ACLs AMB Access Bitcoin の

をサポート ACLs : いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式を使用しません。

## ABAC AMB Access Bitcoin を使用する

サポート ABAC (ポリシー内のタグ): いいえ

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。In AWSでは、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くのタグをアタッチできます。AWS リソースの使用料金を見積もることができます。エンティティとリソースのタグ付けは、最初のステップですABAC。次に、プリンシパルのタグが、アクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの [条件要素](#) でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「[ユーザーガイド](#)」の「[とはABACIAM](#)」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「[ユーザーガイド](#)」の「[属性ベースのアクセスコントロール \(ABAC\)](#)」を使用するIAM」を参照してください。

## AMB Access Bitcoin での一時的な認証情報の使用

一時的な認証情報をサポート：いいえ

ある程度 AWS のサービス 一時的な認証情報を使用してサインインすると、は機能しません。以下を含む追加情報 AWS のサービス 一時的な認証情報の使用については、「[IAM ユーザーガイド](#)」の「[AWS のサービス ユーザーガイドの IAM](#)」で動作する IAM。

にサインインする場合、一時的な認証情報を使用している AWS Management Console ユーザー名とパスワード以外の方法を使用する。例えば、にアクセスする場合 AWS 会社のシングルサインオン (SSO) リンクを使用すると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「[IAMユーザーガイド](#)」の「[ロールへの切り替え \(コンソール\)](#)」を参照してください。

を使用して、一時的な認証情報を手動で作成できます。AWS CLI または AWS API。その後、これらの一時的な認証情報を使用してにアクセスできます。AWS. AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「[IAM ユーザーガイド](#)」の「[一時的なセキュリティ認証情報IAM](#)」を参照してください。

## AMB Access Bitcoin のクロスサービスプリンシパル許可

転送アクセスセッションをサポート (FAS): いいえ

IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用します。AWS のサービス、リクエスト元との組み合わせ AWS のサービス ダウンストリームサービスにリクエストを行う。FAS リクエストは、他の とのやり取りを必要とするリクエストをサービスが受信した場合にのみ行われます。AWS のサービス または完了するリソース。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、[「転送アクセスセッション」](#)を参照してください。

## AMB Access Bitcoin のサービスロール

サービスロールのサポート: なし

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAM ロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、[「にアクセス許可を委任するロールの作成」](#)を参照してください。AWS のサービス「」(IAM ユーザーガイド) を参照してください。

### Warning

サービスロールのアクセス許可を変更すると、AMBAccess Bitcoin の機能が破損する可能性があります。AMB Access Bitcoin が指示する場合以外は、サービスロールを編集しないでください。

## AMB Access Bitcoin のサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。AWS のサービス。このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールが に表示されます。AWS アカウント とは サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「」を参照してください。  
[AWS と連携する のサービスIAM](#)。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

## Amazon Managed Blockchain (AMB) Access Bitcoin のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには Access Bitcoin AMB リソースを作成または変更するアクセス許可はありません。また、 を使用してタスクを実行することはできません。AWS Management Console, AWS Command Line Interface (AWS CLI )、または AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「ユーザーガイド」の [IAM 「ポリシーの作成IAM」](#) を参照してください。

ARNs 各リソースタイプの の形式など、AMB Access Bitcoin で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「[Amazon Managed Blockchain \(AMB\) Access Bitcoin のアクション、リソース、および条件キー](#)」を参照してください。

### トピック

- [ポリシーのベストプラクティス](#)
- [AMB Access Bitcoin コンソールの使用](#)
- [自分の権限の表示をユーザーに許可する](#)
- [Bitcoin ネットワークへのアクセス](#)

### ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AMB Access Bitcoin リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 のコストが発生する可能性があります。AWS アカウント。アイデンティティベースのポリシーを作成または編集するときは、以下のガイドラインと推奨事項に従ってください。

- の使用を開始する AWS 管理ポリシーと最小特権のアクセス許可への移行 – ユーザーとワークロードへのアクセス許可の付与を開始するには、 を使用します。AWS 多くの一般的なユースケース

にアクセス許可を付与する マネージドポリシー。これらは で利用できます。AWS アカウント。を定義してアクセス許可をさらに減らすことをお勧めします。AWS ユースケースに固有の カスタマー管理ポリシー。詳細については、「」を参照してください[AWS マネージドポリシー](#)または [AWS ユーザーガイドの ジョブ機能の IAM マネージドポリシー](#)。

- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「ユーザーガイド」の「[のポリシーとアクセス許可IAMIAM](#)」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。特定の を通じてサービスアクションが使用されている場合、条件を使用してサービスアクションへのアクセスを許可することもできます。AWS のサービスまたは AWS CloudFormation。詳細については、「ユーザーガイド」の[IAMJSON 「ポリシー要素: 条件IAM」](#)を参照してください。
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「ユーザーガイド」の[IAM 「Access Analyzer ポリシーの検証IAM」](#)を参照してください。
- 多要素認証を要求する (MFA ) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合 AWS アカウントのセキュリティを強化するMFAには、 をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、「IAMユーザーガイド」の[MFA 「で保護されたAPIアクセスの設定」](#)を参照してください。

のベストプラクティスの詳細についてはIAM、「ユーザーガイド」の「[のセキュリティのベストプラクティスIAMIAM](#)」を参照してください。

## AMB Access Bitcoin コンソールの使用

Amazon Managed Blockchain (AMB) Access Bitcoin コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AMB Access Bitcoin リソースの詳細を一覧表示および表示できます。AWS アカウント。最小限必要なアクセス許可よりも制限され



たアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。AWS CLI または AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続き AMB Access Bitcoin コンソールを使用できるようにするには、Access Bitcoin AMB *ConsoleAccess* または もアタッチします。 *ReadOnly* AWS エンティティへの マネージドポリシー。詳細については、「ユーザーガイド」の「[ユーザーへのアクセス許可の追加IAM](#)」を参照してください。

## 自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。AWS CLI または 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": "*"
}
]
}

```

## Bitcoin ネットワークへのアクセス

### Note

Bitcoin のパブリックエンドポイントにアクセスし mainnet、JSON-RPC 呼び出し testnet を行うには、AMB Access Bitcoin に適切なアクセス IAM 許可を持つユーザー認証情報 (AWS\_ACCESS\_KEY\_ID および AWS\_SECRET\_ACCESS\_KEY) が必要です。

### Example IAM すべての Bitcoin Networks にアクセスするためのポリシー

この例では、の IAM ユーザーに を付与します。AWS アカウント すべての Bitcoin ネットワークへのアクセス。

```

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

```

### Example IAM Bitcoin Testnet ネットワークにアクセスするためのポリシー

この例では、の IAM ユーザーに を付与します。AWS アカウント Bitcoin testnet ネットワークへのアクセス。



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

## Amazon Managed Blockchain (AMB) Access Bitcoin Identity and Access のトラブルシューティング

以下の情報は、AMB Access Bitcoin と の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

### トピック

- [AMB Access Bitcoin でアクションを実行する権限がない](#)
- [iam を実行する権限がありません。PassRole](#)
- [自分の 以外のユーザーに許可したい AWS アカウント AMB Access Bitcoin リソースにアクセスする](#)

### AMB Access Bitcoin でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の *my-example-widget* リソースの詳細を表示しようとしているが、架空の `managedblockchain::GetWidget` アクセス許可がない場合に発生します。

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

この場合、`managedblockchain::GetWidget` アクションを使用して `my-example-widget` リソースへのアクセスを許可するように、`mateojackson` ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、お問い合わせください。AWS 管理者。サインイン認証情報を提供した担当者が管理者です。

## iam を実行する権限がありません。PassRole

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Access Bitcoin AMB にロールを渡すことができるようにする必要があります。

ある程度 AWS のサービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、という IAM ユーザーがコンソールを使用して AMB Access Bitcoin でアクションを実行しようとする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、お問い合わせください。AWS 管理者。サインイン認証情報を提供した担当者が管理者です。

## 自分の 以外のユーザーに許可したい AWS アカウント AMB Access Bitcoin リソースにアクセスする

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- AMB Access Bitcoin がこれらの機能をサポートしているかどうかを確認するには、「」を参照してください [Amazon Managed Blockchain \(AMB\) Access Bitcoin と の連携方法 IAM](#)。
- 全体で リソースへのアクセスを提供する方法を学ぶには AWS アカウント 所有している。「別の [IAMユーザーへのアクセスの許可](#)」を参照してください。 [AWS アカウント ユーザーガイドで 所有している IAM](#)。
- リソースへのアクセスをサードパーティーに提供する方法を学ぶには AWS アカウント、「 [へのアクセスの提供](#)」を参照してください。 [AWS アカウント ユーザーガイドの「第三者が所有していますIAM」](#)。
- ID フェデレーションを通じてアクセスを提供する方法については、IAMユーザーガイドの「 [外部認証されたユーザーへのアクセスの提供 \(ID フェデレーション\)](#)」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、ユーザーガイドの「 [でのクロスアカウントリソースアクセスIAMIAM](#)」を参照してください。

# Amazon Managed Blockchain (AMB) によるビットコインイベントのロギング: AWS CloudTrail

## Note

Amazon Managed Blockchain (AMB) アクセスビットコインは管理イベントをサポートしていません。

Amazon Managed Blockchain は AWS CloudTrail、マネージドブロックチェーンのユーザー、ロール、AWS またはサービスが実行したアクションの記録を提供するサービスと統合されています。CloudTrail 誰がマネージドブロックチェーンの AMB Access Bitcoin エンドポイントをデータプレーンイベントとして呼び出したかをキャプチャします。

目的のデータプレーンイベントを受信するように登録された適切に設定されたトレイルを作成すると、Amazon S3 バケットへの AMB Access Bitcoin CloudTrail 関連イベントの継続的な配信を受け取ることができます。によって収集された情報を使用して CloudTrail、AMB Access Bitcoin エンドポイントの 1 つに対してリクエストが行われたかどうか、リクエストの送信元の IP アドレス、リクエストの実行者、実行日時、その他の詳細情報を判断できます。

詳細については CloudTrail、[AWS CloudTrail ユーザーガイド](#)をご覧ください。

## AMB: のビットコイン情報にアクセスします。 CloudTrail

AWS CloudTrail AWS アカウントを作成すると、デフォルトで有効になっています。ただし、AMB Access Bitcoin エンドポイントを起動したユーザーを確認するには、CloudTrail データプレーンイベントをログに記録するように設定する必要があります。

AMB Access Bitcoinのデータプレーンイベントを含め AWS アカウント、内のイベントを継続的に記録しておくには、証跡を作成する必要があります。トレイルによって Amazon S3 CloudTrail バケットにログファイルが配信されます。デフォルトでは、証跡を作成すると AWS Management Console、その証跡はすべてに適用されます AWS リージョン。トレイルは、AWS パーティション内のサポートされているすべてのリージョンのイベントを記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、このデータをさらに分析し、AWS CloudTrail ログに収集されたイベントデータに基づいて処理するように他のサービスを設定できます。詳細については、次を参照してください:

- [ビットコイン JSON CloudTrail RPC の追跡に使用](#)
- 「[証跡作成の概要](#)」
- [CloudTrail サポート対象のサービスとインテグレーション](#)
- [の Amazon SNS 通知の設定 CloudTrail](#)
- [CloudTrail 複数のリージョンからのログファイルの受信、CloudTrail および複数のアカウントからのログファイルの受信](#)

CloudTrail データイベントを分析することで、誰がAMB Access Bitcoinエンドポイントを呼び出したかを監視できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報のどちらで行われたか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらかの一時的なセキュリティ認証情報を使用して送信されたかどうか。
- AWS リクエストが別のサービスによって行われたかどうか。

詳細については、「[CloudTrail userIdentity エlement](#)」を参照してください。

## AMB Access のビットコインログファイルエントリについて

データプレーンイベントの場合、トレイルとは、指定した S3 バケットにイベントをログファイルとして配信できるようにする設定です。CloudTrail 各ログファイルには、任意のソースからの 1 つのリクエストを表す 1 つ以上のログエントリが含まれます。これらのエントリには、アクションの日時、関連するリクエストパラメータなど、リクエストされたアクションに関する詳細が記録されます。

### Note

CloudTrail ログファイル内のデータイベントは、AMB Access Bitcoin API 呼び出しの順序付けられたスタックトレースではないため、特定の順序で表示されることはありません。

## ビットコイン JSON CloudTrail RPC の追跡に使用

CloudTrail を使用して、アカウント内の誰が AMB Access ビットコインエンドポイントを呼び出したのか、どの JSON-RPC がデータイベントとして呼び出されたのかを追跡できます。デフォルトでは、証跡を作成しても、データイベントは記録されません。誰が AMB Access CloudTrail Bitcoin エンドポイントをデータイベントとして呼び出したかを記録するには、アクティビティを収集したいサポート対象のリソースまたはリソースタイプを明示的にトレイルに追加する必要があります。Amazon Managed Blockchain は AWS Management Console、AWS SDK、およびを使用したデータイベントの追加をサポートしています AWS CLI。詳細については、AWS CloudTrail ユーザーガイドの「[高度なセレクトクを使用してイベントをログに記録する](#)」を参照してください。

証跡のデータイベントを記録するには、[put-event-selectors](#) 証跡を作成した後で操作を使用してください。--advanced-event-selectors AWS::ManagedBlockchain::Network オプションを使用してリソースタイプを指定し、データイベントのロギングを開始して、AMB Access Bitcoin エンドポイントを呼び出したユーザーを特定します。

Example アカウントのすべての AMB Access ビットコインエンドポイントリクエストのデータイベントログエントリ

以下の例は、put-event-selectors オペレーションを使用して、my-bitcoin-trail リージョン内のトレイルに関するアカウントの AMB Access Bitcoin エンドポイントリクエストをすべて記録する方法を示しています。us-east-1

```
aws cloudtrail put-event-selectors \  
  
--region us-east-1 \  
--trail-name my-bitcoin-trail \  
--advanced-event-selectors '[{  
  "Name": "Test",  
  "FieldSelectors": [  
    { "Field": "eventCategory", "Equals": ["Data"] },  
    { "Field": "resources.type", "Equals": ["AWS::ManagedBlockchain::Network"] } ] ]'
```

登録すると、前の例で指定したトレイルに接続されている S3 バケットの使用状況を追跡できます。

次の結果は、CloudTrail によって収集された情報のデータイベントログエントリを示しています CloudTrail。ビットコイン JSON-RPC リクエストが AMB Access のビットコインエンドポイントのいずれかに送信されたかどうか、リクエストの送信元 IP アドレス、リクエストの実行者、実行日時、およびその他の詳細情報を確認できます。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA554U062RJ7KSB7FAX: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"
}
```

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。