aws

開發人員指南

AMB Access 比特幣

AMB Access 比特幣: 開發人員指南

Table of Contents

什麼是 Amazon Managed Blockchain (AMB) Access Bitcoin？

Amazon Managed Blockchain (AMB) Access 為您提供 Ethereum 和 Bitcoin 的公有區塊鏈節點，您也可以使用 Hyperledger Fabric 架構建立私有區塊鏈網路。從各種方法中選擇，以與公有區塊鏈互動，包括全受管、單一租戶（專用）和公有區塊鏈節點的無伺服器多租戶 API 操作。對於存取控制很重要的使用案例，您可以選擇全受管私有區塊鏈網路。標準化 API 操作可在全受管、彈性的基礎設施上提供立即的可擴展性，因此您可以建置區塊鏈應用程式。

AMB Access 為您提供兩種不同類型的區塊鏈基礎設施服務：多租用戶區塊鏈網路存取 API 操作和專用區塊鏈節點和網路。使用專用區塊鏈基礎設施，您可以建立和使用公有 Ethereum 區塊鏈節點和私有 Hyperledger Fabric 區塊鏈網路，供您自己使用。不過，AMB Access Bitcoin 等以 API 為基礎的多租戶產品，是由 API 層後方的 Bitcoin 節點機群組成，其中基礎區塊鏈節點基礎設施與客戶共用。

Bitcoin 是一種分散式區塊鏈網路，可啟用以網路原生加密貨幣 Bitcoin (BTC) 計價之價值的安全peer-to-peer交易。Bitcoin 網路供個人、金融機構、金融科技公司、政府等使用。比特幣網路是一種交換媒介、投資商品，或用於內嵌資料的可公開驗證和不可變分類帳。使用 Amazon Managed Blockchain (AMB) Access Bitcoin，您可以透過區域端點存取 Bitcoin Mainnet 和 Testnet 網路的集區，您可以透過該集區撰寫交易、從總帳讀取資料，以及叫用 Bitcoin Core 節點用戶端上可用的 JSON-RPC 請求。使用無伺服器比特幣端點，您可以專注於建置應用程式，而不是投資未區分的工作，例如佈建、維護和負載平衡比特幣節點。無論您是建置比特幣錢包、建置密碼交換，還是分析比特幣區塊鏈資料，您只需要支付使用 AMB Access Bitcoin 透過比特幣端點提出的請求。

您是第一次使用 AMB Access Bitcoin 嗎？

如果您是第一次使用 AMB Access Bitcoin，建議您先閱讀以下章節：

- 關鍵概念：Amazon Managed Blockchain (AMB) Access Bitcoin
- Amazon Managed Blockchain (AMB) Access Bitcoin 入門
- 使用 Amazon Managed Blockchain (AMB) Access Bitcoin 的比特幣使用案例
- 支援搭配 Amazon Managed Blockchain (AMB) Access Bitcoin 的 Bitcoin JSON-RPCs

關鍵概念：Amazon Managed Blockchain (AMB) Access Bitcoin

> **Note**
>
> 本指南假設您熟悉比特幣不可或缺的概念。這些概念包括分散式、節點、交易、proof-of-work、錢包、公有和私有金鑰、分片等。在使用 Amazon Managed Blockchain (AMB) Access Bitcoin 之前，建議您檢閱 Bitcoin 開發文件和 Mastering Bitcoin。

Amazon Managed Blockchain (AMB) Access Bitcoin 可讓您無伺服器存取 Bitcoin 區塊鏈，而無需您佈建和管理任何 Bitcoin 基礎設施，包括節點。您可以使用此受管服務快速且隨需地存取比特幣網路，進而降低整體擁有成本。

AMB Access Bitcoin 可讓您透過執行 Bitcoin Core 用戶端的完整節點存取 Bitcoin 網路，停用錢包功能，並支援多個 JSON 遠端程序 (JSON-RPC) 呼叫。您可以叫用 Bitcoin JSON RPCs 與 Managed Blockchain 管理的 Bitcoin 節點通訊，以與 Bitcoin 網路互動。透過 Bitcoin JSON-RPCs，您可以使用 Amazon Managed Blockchain 服務讀取資料和寫入交易，包括查詢資料和將交易提交至 Bitcoin 網路。

> **Important**
>
> 您負責建立、維護、使用和管理 Bitcoin 地址。您也必須負責 Bitcoin 地址的內容。對於在 Amazon Managed Blockchain 上使用 Bitcoin 節點部署或呼叫的任何交易 AWS ， 概不負責。

使用 Amazon Managed Blockchain (AMB) Access Bitcoin 的考量和限制

- 支援的比特幣網路

  AMB Access Bitcoin 支援下列公有網路：

  - Mainnet - 受proof-of-work共識保護的公有比特幣區塊鏈，以及發行和交易比特幣 (BTC) 加密貨幣。Mainnet 上的交易具有實際值 （即會產生實際成本），並記錄在公有區塊鏈上。
  - Testnet - testnet 是用於測試的替代比特幣區塊鏈。Testnet 金幣與實際比特幣 (BTC) 不同，通常沒有任何值。

> **Note**
>
> 不支援私有網路。

- 支援的區域

  以下是此服務支援的 區域：

區域名稱	Code	區域
美國東部 (維吉尼亞北部)	IAD	us-east-1
亞太地區 (東京)	NRT	ap-northeast-1
亞太地區 (首爾)	ICN	ap-northeast-2
亞太地區 (新加坡)	SIN	ap-southeast-1
歐洲 (愛爾蘭)	DUB	eu-west-1
歐洲 (倫敦)	LHR	eu-west-2

- 服務端點

  以下是 AMB Access Bitcoin 的服務端點。若要與服務連線，您必須使用包含其中一個支援區域的端點。

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

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

- 不支援探勘

  AMB Access Bitcoin 不支援比特幣 (BTC) 挖掘。

- 簽署第 4 版 Bitcoin JSON-RPC 呼叫簽署

  在 Amazon Managed Blockchain 上呼叫 Bitcoin JSON-RPCs 時，您可以透過使用 Signature 第 4 版簽署程序驗證的 HTTPS 連線來執行此操作。這表示只有帳戶中的授權 IAM AWS 主體才能進行比特幣 JSON-RPC 呼叫。若要這樣做，必須使用 呼叫提供 AWS 憑證 （ 存取金鑰 ID 和私密存取金鑰 ）。

> **Important**
>
> - 請勿在面向使用者的應用程式中嵌入用戶端登入資料。
> - 您無法使用 IAM 政策來限制對個別 Bitcoin JSON-RPCs存取。

- 僅支援提交原始交易

  使用 `sendrawtransaction` JSON-RPC 提交更新比特幣區塊鏈狀態的交易。

- AWS CloudTrail 記錄支援

  您可以設定 CloudTrail 來記錄 Bitcoin JSON-RPCs。如需詳細資訊，請參閱使用 記錄 Amazon Managed Blockchain (AMB) 存取比特幣事件 AWS CloudTrail

設定 Amazon Managed Blockchain (AMB) Access Bitcoin

第一次使用 Amazon Managed Blockchain (AMB) Access Bitcoin 之前，請遵循本節中的步驟來建立 AWS 帳戶。下一章討論如何開始使用 AMB Access Bitcoin。

先決條件和考量事項

AWS 第一次使用 之前，您必須擁有 AWS 帳戶。

註冊 AWS

當您註冊 時 AWS，您的 AWS 帳戶 會自動註冊所有 AWS 服務，包括 Amazon Managed Blockchain (AMB) Access Bitcoin。您只需針對所使用的服務付費。

如果您已有 AWS 帳戶 ，請前往下一個步驟。如果您還沒有 AWS 帳戶，請使用下列程序建立新帳戶。

建立 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

建立具有適當許可的 IAM 使用者

若要建立和使用 AMB Access Bitcoin，您必須擁有允許必要受管區塊鏈動作的 AWS Identity and Access Management (IAM) 委託人 （ 使用者或群組 ）。

只有 IAM 主體可以進行比特幣 JSON-RPC 呼叫。在 Amazon Managed Blockchain 上呼叫 Bitcoin JSON-RPCs 時，您可以透過使用 Signature 第 4 版簽署程序驗證的 HTTPS 連線來執行此操作。這表示只有帳戶中的授權 IAM AWS 主體可以進行比特幣 JSON-RPC 呼叫。若要這樣做，必須隨呼叫提供 AWS 憑證 （ 存取金鑰 ID 和私密存取金鑰 ）。

如需如何建立 IAM 使用者的資訊，請參閱在 AWS 帳戶中建立 IAM 使用者。如需如何將許可政策連接至使用者的詳細資訊，請參閱變更 IAM 使用者的許可。如需可用於授予使用者許可以使用 AMB

Access Bitcoin 的許可政策範例，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例。

安裝和設定 AWS Command Line Interface

如果您尚未這麼做，請安裝最新的 AWS Command-Line Interface (CLI) 以使用來自終端機 AWS 的資源。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI。

> **Note**
>
> 對於 CLI 存取，您需要存取金鑰 ID 和私密存取金鑰。盡可能使用臨時憑證，而不是長期存取金鑰。臨時憑證包含存取金鑰 ID、私密存取金鑰，以及指出憑證何時到期的安全符記。如需詳細資訊，請參閱《IAM 使用者指南》中的將臨時登入資料與 AWS 資源搭配使用。

Amazon Managed Blockchain (AMB) Access Bitcoin 入門

使用本節中的step-by-step教學課程，了解如何使用 Amazon Managed Blockchain (AMB) Access Bitcoin 執行任務。這些範例需要您完成一些先決條件。如果您是初次使用 AMB Access Bitcoin，請檢閱本指南的設定一節，確認您已完成這些先決條件。如需詳細資訊，請參閱設定 Amazon Managed Blockchain (AMB) Access Bitcoin。

主題

建立 IAM 政策以存取比特幣 JSON-RPCs

若要存取 Bitcoin Mainnet 和 Testnet 的公有端點以進行 JSON-RPC 呼叫，您必須擁有具有 Amazon Managed Blockchain (AMB) Access Bitcoin 適當 IAM 許可的使用者登入資料 (AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY)。在 AWS CLI 已安裝 的終端機中，執行下列命令來建立 IAM 政策，以存取這兩個 Bitcoin 端點：

```
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**
>
> 上述範例可讓您同時存取 Bitcoin Mainnet 和 Testnet。若要存取特定端點，請使用下列`Action`命令：
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

建立政策後，將該政策連接至 IAM 使用者的角色，讓政策生效。在 中 AWS 管理主控台，導覽至 IAM 服務，並將政策連接至指派給 IAM 使用者`AmazonManagedBlockchainBitcoinAccess`的角色。如需詳細資訊，請參閱建立角色並指派給 IAM 使用者。

使用 在 AMB Access RPC 編輯器上發出比特幣遠端程序呼叫 (RPC) 請求 AWS 管理主控台

您可以使用 AWS 管理主控台 AMB Access 在 上編輯和提交遠端程序呼叫 (RPCs)。透過這些 RPCs，您可以在比特幣網路上讀取資料、寫入和提交交易。

Example

下列範例顯示如何使用 `blockhash getBlock` RPC 取得 00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09 的相關資訊。使用您自己的輸入取代反白顯示的變數，或選擇列出的其他 RPC 方法之一，然後輸入所需的相關輸入。

1. 開啟位於 https：//https://console.aws.amazon.com/managedblockchain/ 的 Managed Blockchain 主控台。
2. 選擇 RPC 編輯器。
3. 在請求區段中，選擇 *`BITCOIN_MAINNET`*做為區塊鏈網路。
4. 選擇 *`getblock`*作為 RPC 方法。
5. 輸入 *`00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09`*做為封鎖號碼，然後選擇 *`0`*做為詳細資訊。
6. 然後，選擇提交 RPC。

7. 您將在此頁面的回應區段中取得結果。然後，您可以複製完整的原始交易以進行進一步分析，或在應用程式的商業邏輯中使用 。

如需詳細資訊，請參閱 AMB Access Bitcoin 支援的 RPCs

使用 在 awscurl 中提出 AMB Access Bitcoin JSON-RPC 請求 AWS CLI

Example

使用 Signature 第 4 版 (SigV4) 使用您的 IAM 使用者憑證簽署請求，以便對 AMB Access Bitcoin 端點進行 Bitcoin JSON-RPC 呼叫。awscurl 命令列工具可協助您使用 SigV4 簽署對 AWS 服務的請求。如需詳細資訊，請參閱 awscurl https：//README.md。

使用適用於您作業系統的 方法安裝 awscurl。在 macOS 上，建議使用 HomeBrew 應用程式：

```
brew install awscurl
```

如果您已安裝並設定 AWS CLI，您的 IAM 使用者登入資料和預設 AWS 區域會在您的環境中設定，並可存取 awscurl。使用 awscurl，透過叫用 `getblock` RPC 向 Bitcoin Mainnet 和 Testnet 提交請求。此呼叫接受對應至您要擷取資訊的區塊雜湊的字串參數。

下列命令會使用`params`陣列中的區塊雜湊，從 Bitcoin Mainnet 擷取區塊標頭資料，以選取要擷取標頭的特定區塊。此範例使用 `us-east-1`端點。您可以使用 Amazon Managed Blockchain (AMB) Access Bitcoin 支援的慣用 Bitcoin JSON-RPC 和 AWS 區域來取代此選項。此外，您可以在 命令`testnet`中將 取代`mainnet`為 ，以對 Testnet 網路提出請求，而非 Mainnet。

```
awscurl -X POST -d '{ "jsonrpc": "1.0", "id": "getblockheader-curltest", "method":
 "getblockheader", "params":
 ["000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0"] }' --service
 managedblockchain https://mainnet.bitcoin.managedblockchain.us-east-1.amazonaws.com
 --region us-east-1 -k
```

結果包含來自區塊標頭的詳細資訊，以及包含在請求區塊中的交易雜湊清單。請參閱下列範例：

```
{"result":{"hash":"000000000000000000105bebab2f9dd16234a30950d38ec6ddc24d466e750a0",
      "confirmations":2,"height":799243,"version":664485888,"versionHex":"279b4000",
      "merkleroot":"568e79752e1921ecf40c961435abb41bc5700fe2833ecadc4abfc2f615ddc1b8",
```

```
      "time":1689684290,"mediantime":1689681317,"nonce":2091174943,"bits":"17053894",
      "difficulty":53911173001054.59,
      "chainwork":"00000000000000000000000000000000000000004f375cf72ff64e2404c1589c",
      "nTx":2135,

 "previousblockhash":"000000000000000002ffe4efe07ae74ec8b92c7696f5e12b5da506f015ba6b",

 "nextblockhash":"000000000000000000038f05ddcf3f483fdcb74f4be606c022bcb673424fa4ca"},
      "error":null,"id":"curltest"}
```

在 Node.js 中提出比特幣 JSON-RPC 請求

您可以使用 HTTPS 來存取 Bitcoin Mainnet 和 Testnet 端點，並使用 Node.js 中的原生 https 模組進行 JSON-RPC API 呼叫，或使用第三方程式庫，例如 AXIOS。下列範例示範如何對 AMB Access Bitcoin 端點提出 Bitcoin JSON-RPC 請求。

Example

若要執行此範例 Node.js 指令碼，請套用下列先決條件：

1. 您必須在機器上安裝節點版本管理員 (nvm) 和 Node.js。您可以在此處找到作業系統的安裝說明。
2. 使用 `node --version`命令並確認您正在使用 Node 第 14 版或更新版本。如果需要，您可以使用 `nvm install 14`命令，後面接著 `nvm use 14`命令來安裝 第 14 版。
3. 環境變數 `AWS_ACCESS_KEY_ID`和 `AWS_SECRET_ACCESS_KEY`必須包含與您 帳戶相關聯的登入資料。環境變數`AMB_HTTP_ENDPOINT`必須包含您的 AMB Access Bitcoin 端點。

   使用下列命令，將這些變數匯出為用戶端上的字串。將下列字串中反白顯示的值取代為 IAM 使用者帳戶的適當值。

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

完成所有先決條件後，請使用編輯器將下列`package.json`檔案和`index.js`指令碼複製到您的本機環境：

package.json

```
{
  "name": "bitcoin-rpc",
```

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

index.js

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

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


const rpcRequest = async () => {

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

```
  }

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

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

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


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

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

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


}

rpcRequest();
```

先前的範例程式碼使用 Axios 向 Bitcoin 端點提出 RPC 請求，並使用官方 AWS SDK v3 工具，以適當的 Signature 第 4 版 (SigV4) 標頭簽署這些請求。若要執行程式碼，請在與 檔案相同的目錄中開啟終端機，並執行下列動作：

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

產生的結果如下：

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

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

> **Note**
>
> 上一個指令碼中的範例請求會使用與使用 在 awscurl 中提出 AMB Access Bitcoin JSON-RPC 請求 AWS CLI範例相同的輸入參數區塊雜湊來進行`getblock`呼叫。若要進行其他呼叫，請使用不同的比特幣 JSON-RPC 修改指令碼中的`rpc`物件。您可以將主機屬性選項變更為 Bitcoin`testnet`，以在該端點上進行呼叫。

透過 使用 AMB Access Bitcoin AWS PrivateLink

AWS PrivateLink 是一項高可用性、可擴展的技術，可用來將 VPC 連線至私有 服務，就像在 VPC 中一樣。您不需要使用網際網路閘道、NAT 裝置、公有 IP 地址、 AWS Direct Connect 連線或 AWS Site-to-Site VPN 連線，即可從私有子網路與服務通訊。如需 AWS PrivateLink 或 設定的詳細資訊 AWS PrivateLink，請參閱什麼是 AWS PrivateLink？

您可以使用 VPC 端點 AWS PrivateLink 將 Bitcoin JSON-RPC 請求傳送到 AMB Access Bitcoin。對此私有端點的請求不會透過開放網際網路傳遞，因此您可以使用相同的 SigV4 身分驗證，直接將請求傳送至 Bitcoin 端點。如需詳細資訊，請參閱透過 存取 AWS 服務 AWS PrivateLink。

對於服務名稱，請在AWS 服務欄中尋找 Amazon Managed Blockchain。如需詳細資訊，請參閱 AWS 整合的 服務 AWS PrivateLink。端點的服務名稱將採用下列格式：`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*。

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

使用 Amazon Managed Blockchain (AMB) Access Bitcoin 的比特幣使用案例

本主題提供 AMB Access Bitcoin 使用案例清單

主題

建置 Bitcoin (BTC) 錢包以傳送和接收 BTC

BTC 是比特幣網路上的原生加密貨幣，是網路安全模型的重要元件。它也可以做為商品和交換媒介，由機構、企業和個人廣泛使用。因此，許多錢包應用程式依賴比特幣節點與比特幣區塊鏈互動。這些應用程式會計算一組指定地址的未使用輸出 (UTXOs) 餘額、簽署交易並傳送至比特幣網路，以及擷取歷史交易的資料。

以下是 Amazon Managed Blockchain (AMB) Access Bitcoin 支援用於 BTC 錢包交易的一些 Bitcoin JSON-RPCs 範例：

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

如需詳細資訊，請參閱支援的 JSON-RPCs。

分析比特幣區塊鏈上的活動

您可以使用 `getchaintxstats` JSON-RPC 方法分析比特幣區塊鏈上的交易活動量。此 JSON-RPC 可讓您存取指標，例如每秒平均交易速率、總交易計數、區塊計數等。您也可以將區塊編號的時段或區塊雜湊定義為分隔符號，以視需要計算網路中特定區塊集的這些統計資料。

如需詳細資訊，請參閱支援的 JSON-RPCs。

驗證使用比特幣金鑰對簽署的訊息

比特幣錢包具有私有金鑰和構成金鑰對的公有金鑰。這些金鑰用於簽署交易，並做為區塊鏈上的使用者身分。公有金鑰用於建立地址，這是標準化的英數字元識別符（長度為 27 到 34 個字元）。這些地址用於接收 BTC 輸出並處理交易或訊息。

使用比特幣錢包，使用者也可以以密碼編譯方式簽署和驗證訊息。此程序通常用於證明特定錢包地址及其相關聯 BTC 的擁有權。透過使用`verifymessage`比特幣 JSON-RPC，您可以檢查由另一個錢包簽署的訊息的真實性和有效性。具體而言，Bitcoin 節點可用來驗證訊息是否已使用與簽章訊息本身內提供的公有金鑰衍生地址對應的私有金鑰簽署。

如需詳細資訊，請參閱支援的 JSON-RPCs。

檢查比特幣集區

許多應用程式需要存取 Mmpool，以追蹤待處理交易、取得所有待處理交易的清單，或了解交易的來源。為此，有比特幣 JSON-RPCs，例如 `getmempoolancestors`、 `getmempoolentry`和 `getrawmempool` 支援此活動。這些比特幣 JSON-RPCs可協助應用程式從集區取得所需的資訊。

Amazon Managed Blockchain (AMB) Access Bitcoin 也支援 `testmempoolaccept` Bitcoin JSON-RPCs，可讓您驗證交易是否符合通訊協定規則，並在提交之前由節點接受。直接提交交易至比特幣區塊鏈的錢包、交換和任何其他實體都會使用這些比特幣 JSON-RPCs。

如需詳細資訊，請參閱支援的 JSON-RPCs。

支援搭配 Amazon Managed Blockchain (AMB) Access Bitcoin 的 Bitcoin JSON-RPCs

本主題提供受管 Blockchain 支援的 Bitcoin JSON-RPCs 的清單和參考。每個支援的 JSON-RPC 都有其使用的簡短描述。

> **Note**
>
> - 您可以使用 Signature 第 4 版 (SigV4) 簽署程序來驗證受管 Blockchain 上的 Bitcoin JSON-RPCs。這表示只有 AWS 帳戶中的授權 IAM 主體可以使用比特幣 JSON-RPCs 與其互動。隨 呼叫提供 AWS 登入資料 （ 存取金鑰 ID 和私密存取金鑰 ）。
> - 如果您的 HTTP 回應大於 10 MB，您會收到錯誤。若要修正此問題，您必須將壓縮標頭設定為 `Accept-Encoding:gzip`。然後，用戶端收到的壓縮回應包含下列標頭： `Content-Type: application/json`和 `Content-Encoding: gzip`。
> - Amazon Managed Blockchain (AMB) Access Bitcoin 會針對格式不正確的 JSON-RPC 請求產生 400 錯誤。
> - 使用 `sendrawtransaction` JSON-RPC 提交更新比特幣區塊鏈狀態的交易。
> - AMB Access Bitcoin 預設請求限制為每秒 100 個請求 (RPS)`NETWORK_TYPE`，每個 AWS 區域每個 。
>
>   若要提高配額，您必須聯絡 AWS 支援。若要聯絡 AWS 支援，請登入AWS 支援中心主控台。選擇建立案例。選擇技術。選擇受管區塊鏈做為您的服務。選擇 Access：Bitcoin 作為您的類別，選擇一般指引作為您的嚴重性。在描述文字方塊中輸入 RPC Quota 做為主旨，並列出每個區域每個比特幣網路 RPS 中適用您需求的配額限制。提交您的案例。

支援的 JSON-RPCs

AMB Access Bitcoin 支援下列 Bitcoin JSON-RPCs。每個支援的呼叫都有其使用的簡短描述。

類別	JSON-RPC	描述
區塊鏈 RPCs	getbestblockhash	傳回最有效、經過完整驗證鏈中最佳 （ 提示 ） 區塊的雜湊。

類別	JSON-RPC	描述
	getblock	如果詳細度為 0，則 會針對區塊「雜湊」傳回序列化的十六進位編碼資料字串。如果詳細資訊為 1，則 會傳回物件，其中包含區塊「雜湊」的相關資訊。如果詳細資訊為 2，則 會傳回物件，其中包含區塊「雜湊」的相關資訊，以及每筆交易的相關資訊。如果詳細資訊為 3，則 會傳回物件，其中包含區塊「雜湊」的相關資訊，以及每個交易的相關資訊，包括輸入prevout的資訊。
	getblockchaininfo	傳回物件，其中包含區塊鏈處理的各種狀態資訊。
	getblockcount	傳回最有效、經過完整驗證的鏈結高度。geneis區塊的高度為 0。
	getblockfilter	使用區塊雜湊擷取特定區塊的 BIP 157 內容篩選條件。
	getblockhash	在提供的高度傳回 best-block-chain 中的區塊雜湊。
	getblockheader	如果詳細資訊為 false， 會傳回區塊標頭「hash」的序列化十六進位編碼資料字串。如果詳細內容為 true， 會傳回 物件，其中包含 blockheader ‘hash’ 的相關資訊。
	getblockstats	指定時段的每個區塊統計資料的運算。所有數量都是 satoshis。它不適用於某些具有剔除的高度。
	getchaintips	傳回區塊樹狀結構中所有已知提示的相關資訊，包括主鏈和孤立分支。
	getchaintxstats	運算鏈結中交易總數和速率的統計資料。
	getdifficulty	傳回proof-of-work困難度，做為最低困難度的倍數。

類別	JSON-RPC	描述
	getmempoolancestors	如果 txid 位於集區中，則 會傳回所有集區內上階。
	getmempooldescendants	如果 txid 位於集區中，則 會傳回所有集區內子系。
	getmempoolentry	傳回指定交易的集區資料。
	getmempoolinfo	傳回 TX 記憶體集區作用中狀態的詳細資訊。
	getrawmempool	以字串交易 IDs的 JSON 陣列傳回記憶體集區中的所有交易 IDs。 **Note** 不支援 `verbose = true`。
	gettxout	傳回有關未花費交易輸出的詳細資訊。
	gettxoutproof	傳回以十六進位編碼的證明，指出「txid」包含在區塊中。
原始交易 RPCs	createrawtransaction	建立花費指定輸入的交易，並建立新的輸出。
	解碼交易	傳回代表序列化、十六進位編碼交易的 JSON 物件。
	描述符	解碼十六進位編碼指令碼。
	getrawtransaction	傳回原始交易資料。
	sendrawtransaction	將原始交易（序列化、十六進位編碼）提交至本機節點和網路。
	testmempoolaccept	傳回 mempool 接受測試的結果，指出 mempool 是否接受原始交易（序列化、十六進位編碼）。這會檢查交易是否違反共識或政策規則。

類別	JSON-RPC	描述
Util RPCs	createmultisig	建立具有 n 個必要 m 金鑰簽章的多簽章地址。
	estimatesmartfee	盡可能估計交易開始確認 conf_target 區塊所需的每 KB 約略費用，並傳回預估有效區塊的數量。使用虛擬交易大小，如 BIP 141 所定義（寬度資料折扣）。
	validateaddress	傳回指定比特幣地址的相關資訊。
	驗證訊息	驗證已簽章的訊息。

Amazon Managed Blockchain (AMB) Access Bitcoin 中的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型將此描述為雲端安全性和雲端安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon Managed Blockchain (AMB) Access Bitcoin 的合規計劃，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

為了提供資料保護、身分驗證和存取控制，Amazon Managed Blockchain 會使用 AWS Managed Blockchain 中執行的開放原始碼架構的功能。

本文件可協助您了解如何在使用 AMB Access Bitcoin 時套用共同責任模型。下列主題說明如何設定 AMB Access Bitcoin 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AMB Access Bitcoin 資源。

主題

- Amazon Managed Blockchain (AMB) Access Bitcoin 中的資料保護
- Amazon Managed Blockchain (AMB) Access Bitcoin 的身分和存取管理

Amazon Managed Blockchain (AMB) Access Bitcoin 中的資料保護

AWS 共同責任模型適用於 Amazon Managed Blockchain (AMB) Access Bitcoin 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 AMB Access Bitcoin 或其他 AWS 服務 使用主控台 AWS CLI、API 或 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

資料加密

資料加密有助於防止未經授權的使用者從區塊鏈網路和相關聯的資料儲存系統讀取資料。這包括在網路移動時可能攔截的資料，稱為傳輸中的資料。

傳輸中加密

根據預設，受管區塊鏈會使用 HTTPS/TLS 連線來加密從執行 AWS CLI 至 AWS 服務端點的用戶端電腦傳輸的所有資料。

您不須採取任何行動即可啟用 HTTPS/TLS。除非您使用 AWS CLI 命令明確停用個別命令的`--no-verify-ssl`命令，否則一律會啟用。

Amazon Managed Blockchain (AMB) Access Bitcoin 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用 AMB Access Bitcoin 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

目標對象

如何使用 AWS Identity and Access Management (IAM) 會因您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Amazon Managed Blockchain (AMB) Access Bitcoin 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。

- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Managed Blockchain (AMB) Access Bitcoin 如何與 IAM 搭配使用

在您使用 IAM 管理 AMB Access Bitcoin 的存取權之前，請先了解哪些 IAM 功能可與 AMB Access Bitcoin 搭配使用。

您可以搭配 Amazon Managed Blockchain (AMB) Access Bitcoin 使用的 IAM 功能

IAM 功能	AMB Access Bitcoin 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	否
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	否
主體許可	否
服務角色	否
服務連結角色	否

若要全面了解 AMB Access Bitcoin 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

AMB Access Bitcoin 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

AMB Access Bitcoin 的身分型政策範例

若要檢視 AMB Access Bitcoin 身分型政策的範例，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例。

AMB Access Bitcoin 內的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

AMB Access Bitcoin 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 AMB Access Bitcoin 動作清單，請參閱《服務授權參考》中的 Amazon Managed Blockchain (AMB) Access Bitcoin 定義的動作。

AMB Access Bitcoin 中的政策動作在動作之前使用下列字首：

```
managedblockchain:
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 InvokeRpcBitcoin 文字的所有動作，請包含以下動作：

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

若要檢視 AMB Access Bitcoin 身分型政策的範例，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例。

AMB Access Bitcoin 的政策資源

支援政策資源：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看 AMB Access Bitcoin 資源類型及其 ARNs的清單，請參閱《服務授權參考》中的 Amazon Managed Blockchain (AMB) Access Bitcoin 定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 定義的動作。

若要檢視 AMB Access Bitcoin 身分型政策的範例，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例。

AMB Access Bitcoin 的政策條件索引鍵

支援服務特定政策條件金鑰：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 AMB Access Bitcoin 條件金鑰清單，請參閱《服務授權參考》中的 Amazon Managed Blockchain (AMB) Access Bitcoin 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 定義的動作。

若要檢視 AMB Access Bitcoin 身分型政策的範例，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例。

AMB Access Bitcoin 中的 ACLs

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 搭配 AMB Access Bitcoin

支援 ABAC (政策中的標籤)：否

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 AMB Access Bitcoin 使用臨時登入資料

支援臨時登入資料：否

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

AMB Access Bitcoin 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：否

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 請求 AWS 服務 向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

AMB Access Bitcoin 的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 AMB Access Bitcoin 功能。只有在 AMB Access Bitcoin 提供指引時，才能編輯服務角色。

AMB Access Bitcoin 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon Managed Blockchain (AMB) Access Bitcoin 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AMB Access Bitcoin 資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 AMB Access Bitcoin 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 Amazon Managed Blockchain (AMB) Access Bitcoin 的動作、資源和條件金鑰。

主題

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AMB Access Bitcoin 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。

- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 AMB Access Bitcoin 主控台

若要存取 Amazon Managed Blockchain (AMB) Access Bitcoin 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 AMB Access Bitcoin 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用 AMB Access Bitcoin 主控台，請將 AMB Access Bitcoin *ConsoleAccess*或*ReadOnly* AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

存取比特幣網路

> **Note**
>
> 為了存取 Bitcoin 的公`testnet`有端點`mainnet`和進行 JSON-RPC 呼叫，您需要具有 AMB Access Bitcoin 適當 IAM 許可的使用者登入資料 (`AWS_ACCESS_KEY_ID` 和 `AWS_SECRET_ACCESS_KEY`)。

Example存取所有比特幣網路的 IAM 政策

此範例會授予 IAM 使用者 AWS 帳戶 存取所有 Bitcoin 網路的權限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AccessAllBitcoinNetworks",
            "Effect": "Allow",
```

```
            "Action": [
                "managedblockchain:InvokeRpcBitcoin*"
            ],
            "Resource": "*"
        }
    ]
}
```

Example存取 Bitcoin Testnet 網路的 IAM 政策

此範例會授予您 AWS 帳戶 存取 Bitcoin `testnet` 網路的 IAM 使用者。

JSON

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

對 Amazon Managed Blockchain (AMB) Access Bitcoin 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AMB Access Bitcoin 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 AMB Access Bitcoin 中執行動作
- 我未獲得執行 iam:PassRole 的授權

- 我想要允許 以外的人員 AWS 帳戶 存取我的 AMB Access Bitcoin 資源

我無權在 AMB Access Bitcoin 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 managedblockchain::*GetWidget* 許可時發生。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 managedblockchain::*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞給 AMB Access Bitcoin。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM marymajor 使用者嘗試使用主控台在 AMB Access Bitcoin 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 AMB Access Bitcoin 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 AMB Access Bitcoin 是否支援這些功能，請參閱 Amazon Managed Blockchain (AMB) Access Bitcoin 如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

使用 記錄 Amazon Managed Blockchain (AMB) 存取比特幣事件 AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Bitcoin 不支援管理事件。

Amazon Managed Blockchain 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或 Managed Blockchain 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將受管區塊鏈的 AMB Access Bitcoin 端點叫用者擷取為資料平面事件。

如果您建立已正確設定且訂閱接收所需資料平面事件的線索，您可以接收 AMB Access Bitcoin 相關 CloudTrail 事件持續交付至 Amazon S3 儲存貯體。您可以使用 CloudTrail 收集的資訊，判斷已向其中一個 AMB Access Bitcoin 端點提出請求、請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 AMB Access Bitcoin 資訊

AWS CloudTrail 當您建立 時，預設會啟用 AWS 帳戶。不過，若要查看誰叫用 AMB Access Bitcoin 端點，您必須設定 CloudTrail 來記錄資料平面事件。

若要在 中持續記錄事件 AWS 帳戶，包括 AMB Access Bitcoin 的資料平面事件，您必須建立追蹤。線索可讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在 中建立線索時 AWS 管理主控台，線索會套用至所有 AWS 區域。線索會記錄 AWS 分割區中所有支援區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務進一步分析此資料，並對 CloudTrail 日誌中收集的資料採取行動。如需詳細資訊，請參閱下列內容：

- 使用 CloudTrail 追蹤比特幣 JSON-RPCs
- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

透過分析 CloudTrail 資料事件，您可以監控誰叫用 AMB Access Bitcoin 端點。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 是否使用角色或聯合身分使用者的臨時安全登入資料提出請求。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 AMB Access Bitcoin 日誌檔案項目

對於資料平面事件，線索是一種組態，可讓事件做為日誌檔案交付至指定的 S3 儲存貯體。每個 CloudTrail 日誌檔案都包含一或多個日誌項目，代表來自任何來源的單一請求。這些項目提供請求動作的詳細資訊，包括動作的日期和時間，以及任何相關聯的請求參數。

> **Note**
>
> 日誌檔案中的 CloudTrail 資料事件不是 AMB Access Bitcoin API 呼叫的排序堆疊追蹤，因此不會以任何特定順序顯示。

使用 CloudTrail 追蹤比特幣 JSON-RPCs

您可以使用 CloudTrail 來追蹤帳戶中誰叫用 AMB Access Bitcoin 端點，以及叫用哪些 JSON-RPC 做為資料事件。根據預設，當您建立線索時，不會記錄資料事件。若要將叫用 AMB Access Bitcoin 端點的人員記錄為 CloudTrail 資料事件，您必須明確新增要收集活動的資源或資源類型至線索。Amazon Managed Blockchain 支援使用 、 AWS 管理主控台 AWS SDK 和 新增資料事件 AWS CLI。如需詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用進階選擇器記錄事件。

若要在線索中記錄資料事件，請在建立線索後使用 put-event-selectors 操作。使用 `--advanced-event-selectors`選項指定`AWS::ManagedBlockchain::Network`資源類型，以開始記錄資料事件，以判斷誰叫用 AMB Access Bitcoin 端點。

Example您帳戶的所有 AMB Access Bitcoin 端點請求的資料事件日誌項目

下列範例示範如何使用 `put-event-selectors`操作，記錄您帳戶的所有 AMB Access Bitcoin 端點`my-bitcoin-trail`對 `us-east-1` 區域中線索的請求。

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

訂閱後，您可以在連線至先前範例中所指定線索的 S3 儲存貯體中追蹤用量。

下列結果顯示 CloudTrail 所收集的資訊的 CloudTrail 資料事件日誌項目。您可以判斷 Bitcoin JSON-RPC 請求是對其中一個 AMB Access Bitcoin 端點提出、請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA554UO62RJ7KSB7FAX:777777777777",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/777777777777",
            "accountId": "111122223333"
        },
        "eventTime": "2023-04-12T19:00:22Z",
        "eventSource": "managedblockchain.amazonaws.com",
        "eventName": "getblock",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "111.222.333.444",
        "userAgent": "python-requests/2.28.1",
        "errorCode": "-",
        "errorMessage": "-",
        "requestParameters": {
            "jsonrpc": "2.0",
            "method": "getblock",
            "params": [],
            "id": 1
        },
        "responseElements": null,
        "requestID": "DRznHHEjIAMFSzA=",
        "eventID": "baeb232d-2c6b-46cd-992c-0e4033aace86",
        "readOnly": true,
        "resources": [{
```

```
            "type": "AWS::ManagedBlockchain::Network",
            "ARN": "arn:aws:managedblockchain:::networks/n-bitcoin-mainnet"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data"
}
```

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。