aws

開發人員指南

AMB訪問比特幣

AMB訪問比特幣: 開發人員指南

Table of Contents

什麼是 Amazon Managed Blockchain（AMB）訪問比特幣？

Amazon Managed Blockchain（AMB）訪問為您提供以太坊和比特幣的公共區塊鏈節點，您還可以使用 Hyperledger Fabric 框架創建私有區塊鏈網絡。從各種方法中選擇與公共區塊鏈互動，包括完全託管的單租戶（專用）以及對公共區塊鏈節點的無服務器多租戶 API 操作。對於存取控制很重要的使用案例，您可以從完全受管的私有區塊鏈網路中進行選擇。標準化 API 作業可讓您在完全受控的彈性基礎架構上提供即時擴充性，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：多租戶區塊鏈網絡訪問 API 操作以及專用區塊鏈節點和網絡。借助專用的區塊鏈基礎設施，您可以創建和使用公共以太坊區塊鏈節點和私有 Hyperledger Fabric 區塊鏈網絡供您自己使用。但是，基於 API 的多租戶產品（例如 AMB Access Bitcoin）由 API 層後面的一組比特幣節點組成，其中基礎區塊鏈節點基礎架構在客戶之間共享。

比特幣是一個去中心化的區塊鏈網絡，可實現以網絡本地加密貨幣比特幣（BTC）計價的安全價值 peer-to-peer 交易。比特幣網絡被個人，金融機構，金融科技公司，政府等人使用。比特幣網絡是一種交易媒介，一種投資商品，或用於刻錄數據的公開可驗證且不可變的分類帳。使用 Amazon Managed Blockchain（AMB）訪問比特幣，您可以通過區域端點訪問比特幣主網和 Testnet 網絡池，通過該端點可以寫入交易，從分類帳中讀取數據以及調用可在比特幣核心節點客戶端上提供的 JSON-RPC 請求。使用無伺服器 Bitcoin 端點，您可以專注於建置應用程式，而不必投資佈建、維護和負載平衡比特幣節點等無差異化工作。無論您是在構建比特幣錢包，建立加密貨幣交易所還是分析比特幣區塊鏈數據，您都只需使用 AMB Access 比特幣支付通過比特幣端點提出的請求費用。

您是第一次 AMB 訪問比特幣用戶嗎？

如果您是 AMB Access 比特幣的首次使用者，我們建議您先閱讀以下章節：

- 關鍵概念：Amazon Managed Blockchain（AMB）訪問比特幣
- 開始使用 Amazon Managed Blockchain（AMB）訪問比特幣
- Amazon Managed Blockchain（AMB）的比特幣使用案例訪問比特幣
- 使用 Amazon Managed Blockchain（AMB）支持的比特幣 JSON RPC 訪問比特幣

關鍵概念：Amazon Managed Blockchain（AMB）訪問比特幣

> **Note**
>
> 本指南假設您熟悉比特幣必不可少的概念。這些概念包括去中心化，節點，交易 proof-of-work，錢包，公鑰和私鑰，減半等。在使用 Amazon Managed Blockchain（AMB）訪問比特幣之前，我們建議您查看比特幣開發文檔和掌握比特幣。

Amazon Managed Blockchain（AMB）Access Bitcoin 為您提供對比特幣區塊鏈的無服務器訪問權限，而無需您佈建和管理任何比特幣基礎設施，包括節點。您可以使用此託管服務快速，隨需訪問比特幣網絡，從而降低整體擁有成本。

AMB 訪問比特幣通過運行比特幣核心客戶端的完整節點為您提供訪問比特幣網絡，並禁用了錢包功能，並支持多個 JSON 遠程過程（JSON-RPC）調用。您可以調用比特幣 JSON RPC 與託管區塊鏈管理的比特幣節點進行通信，以便與比特幣網絡進行交互。使用比特幣 JSON-RPC，您可以讀取數據和寫入交易，包括查詢數據和使用 Amazon Managed Blockchain 服務將交易提交到比特幣網絡。

> **Important**
>
> 您有責任創建，維護，使用和管理您的比特幣地址。您還需要對您的比特幣地址的內容負責。AWS 對於使用 Amazon Managed Blockchain 上的比特幣節點部署或呼叫的任何交易概不負責。

使用 Amazon Managed Blockchain（AMB）的注意事項和限制訪問比特幣

- 支持比特幣網絡

  AMB 訪問比特幣支持以下公共網絡：

  - 主網 — 通過 proof-of-work 共識保護的公共比特幣區塊鏈，並在其上發行和交易比特幣（BTC）加密貨幣。主網上的交易具有實際價值（即它們產生實際成本），並記錄在公共區塊鏈上。
  - 測試網-測試網是用於測試的替代比特幣區塊鏈。Testnet 硬幣與實際的比特幣（BTC）是分開的，並且通常沒有任何價值。

> **Note**
>
> 不支援私人網路。

- 支援的區域

  以下是此服務支援的區域：

區域名稱	代碼	區域
美國東部 (維吉尼亞北部)	IAD	us-east-1
亞太區域 (東京)	NRT	ap-northeast-1
亞太區域 (首爾)	ICN	ap-northeast-2
亞太區域 (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 訪問比特幣的服務端點。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`

- 不支援採礦

  AMB 訪問比特幣不支持比特幣（BTC）挖礦。

- 簽名版本 4 簽署比特幣 JSO-RPC 調用

  在 Amazon Managed Blockchain 上撥打比特幣 JSON RPC 時，您可以通過使用簽名版本 4 簽名過程進行身份驗證的 HTTPS 連接進行調用。這表示只有 AWS 帳戶中已授權的 IAM 主體才能進行比特幣 JSON-RPC 呼叫。若要這麼做，呼叫時必須提供 AWS 認證 (存取金鑰 ID 和秘密存取金鑰)。

> **Important**
>
> - 請勿在使用者對應的應用程式中內嵌用戶端認證
> - 您無法使用 IAM 政策來限制對個別比特幣 JSON RPC 的存取。

- 僅支援原始交易的提交

  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

  您可以配置 CloudTrail 為記錄您的比特幣 JSON-RPC。如需詳細資訊，請參閱 日誌記錄 Amazon Managed Blockchain（AMB）通過使用訪問比特幣事件 AWS CloudTrail

設置 Amazon Managed Blockchain（AMB）訪問比特幣

在您第一次使用 Amazon Managed Blockchain（AMB）訪問比特幣之前，請按照本節中的步驟創建 AWS 帳戶。下面的章節討論了如何開始使用AMB訪問比特幣。

先決條件和考量事項

使用前 AWS 第一次，你必須有一個 AWS 帳戶.

註冊成為 AWS

當您註冊 AWS，您的 AWS 帳戶 已自動為所有人註冊 AWS 服務，包括 Amazon Managed Blockchain（AMB）訪問比特幣。您只需針對所使用的服務付費。

如果您有 AWS 帳戶 已經轉到下一步。如果您沒有 AWS 帳戶，請使用下列程序來建立一個。

若要建立 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個 AWS 帳戶，一個 AWS 帳戶根使用者已建立。根使用者可以存取所有 AWS 服務 和帳戶中的資源。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。

建立具有適當權限的IAM使用者

要創建並AMB使用訪問比特幣，您必須擁有一個 AWS Identity and Access Management （IAM）具有允許必要託管區塊鏈操作的權限的主體（用戶或組）。

只有IAM校長可以使比特幣 JSON-RPC 電話。RPCs在 Amazon Managed Blockchain 上撥打比JSON特幣時，您可以通過使用簽名版本 4 簽名過程進行身份驗證的HTTPS連接進行調用。這表示只有授權的IAM主參與者 AWS 帳戶可以使比特幣 JSON-RPC 電話。若要執行此作業， AWS 呼叫時必須提供憑據（訪問密鑰 ID 和秘密訪問密鑰）。

如需如何建立IAM使用者的詳細資訊，請參閱在 IAM AWS 帳戶。如需如何將權限原則附加至使用者的相關資訊，請參閱變更IAM使用者的權限。有關權限策略的示例，您可以使用該策略向用戶授予AMB訪問比特幣的權限，請參閱Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣。

安裝和配置 AWS Command Line Interface

如果您尚未這樣做，請安裝最新版本 AWS 要使用的命令行界面（CLI）AWS 來自終端的資源。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI.

> **Note**
>
> 要CLI訪問，您需要一個訪問密鑰 ID 和秘密訪問密鑰。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，請參閱搭配使用臨時認證AWS 《IAM使用者指南》中的資源。

開始使用 Amazon Managed Blockchain（AMB）訪問比特幣

使用本節中的 step-by-step 教學課程，了解如何使用 Amazon Managed Blockchain (AMB) 存取比特幣來執行任務。這些範例會要求您完成某些先決條件。如果您是 AMB Access Bitcoin 的新手，請查看本指南的「設置」部分，以確保您已完成這些先決條件。如需詳細資訊，請參閱設置 Amazon Managed Blockchain（AMB）訪問比特幣。

主題

創建訪問比特幣的IAM策略 JSON-RPCs

為了訪問比特幣主網和 Testnet 進JSON行RPC呼叫的公共端點，您必須擁有具有 Amazon Managed Blockchain（KEY）訪問比特幣的適當IAM許可的用戶憑據（AWS_ACCESSKEYAWS_SECRETACCESS_ ID 和 _ _AMB）。在終端 AWS CLI 安裝後，運行以下命令以創建一個IAM策略以訪問兩個比特幣端點：

```
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**
>
> 前面的例子使您可以訪問比特幣主網和 Testnet。若要存取特定端點，請使用下列`Action`命令：
>
> - `"managedblockchain:InvokeRpcBitcoinMainnet"`
> - `"managedblockchain:InvokeRpcBitcoinTestnet"`

建立原則後，請將該原則附加至IAM使用者的角色，以使其生效。在 AWS Management Console，瀏覽至IAM服務，並將原則附加`AmazonManagedBlockchainBitcoinAccess`至指派給IAM使用者的角色。如需詳細資訊，請參閱建立角色和指派給IAM使用者。

在 AMB Access RPC 編輯器上使比特幣遠端程序呼叫 (RPC) 請求 AWS Management Console

您可以在上編輯和提交遠端程序呼叫 (RPCs) AWS Management Console 使用AMB訪問。有了這些RPCs，您可以在比特幣網絡上讀取數據，寫入和提交交易。

Example

下列範例會示範如何取得有關的資訊。 `blockhash` `getBlock` RPC以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. 開啟受管理區塊鏈主控台，位於https://console.aws.amazon.com/managedblockchain/。
2. 選擇RPC編輯器。
3. 在「請求」部分中，選擇*`BITCOIN_MAINNET`*作為區塊鏈網絡。
4. 選擇*`getblock`*作為RPC方法。
5. 輸入*`00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09`*為「封鎖」編號，然後選擇*`0`*作為詳細資訊。
6. 然後選擇 Submit (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供進一步分析，或在應用程式的商務邏輯中使用。

有關更多信息，請參閱AMB訪問比特幣的RPCs支持

使AMB訪問比特幣 JSON-通過使用 awscurl 中的RPC請求 AWS CLI

Example

通過使用簽名版本 4（SIGv4）使用您的用IAM戶憑據簽名簽署請求，以使比特幣 JSON-RPC 調用 AMB訪問比特幣端點。awscurl 命令行工具可以幫助您將請求簽名 AWS 使用 Sigv4 的服務。如需詳細資訊，請參閱 awscurl .md README。

使用適合您的作業系統的方法來安裝 awscurl。在 macOS 上，建議使 HomeBrew用以下應用程式：

```
brew install awscurl
```

如果您已經安裝並配置 AWS CLI，您的IAM用戶憑據和默認AWS區域在您的環境中設置，並可以訪問 awscurl。使用 awscurl，通過調用. getblock RPC 此調用接受對應於您要檢索信息的塊哈希的字符串參數。

下列指令會使用params陣列中的區塊雜湊來選取要擷取標頭的特定區塊，從 Bitcoin 主網擷取區塊標頭資料。此範例使用us-east-1端點。您可以將其替換為您喜歡的比特幣 JSON-RPC 和 AWS 亞馬遜託管區塊鏈（AMB）支持的區域訪問比特幣。此外，您可以通過testnet 在命令中替換mainnet來對 Testnet 網絡而不是主網發出請求。

```
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
```

結果包括來自塊標題的詳細信息以及請求塊中包含的事務哈希列表。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":"0000000000000000000000000000000000000004f375cf72ff64e2404c1589c",
      "nTx":2135,

 "previousblockhash":"00000000000000000002ffe4efe07ae74ec8b92c7696f5e12b5da506f015ba6b",
```

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

製作比特幣 JSON-在 Node.js 中RPC請求

您可以通過使用HTTPS訪問比特幣主網和 Testnet 端點，並通過使用 Node.js 中的本機 https 模塊進JSON行RPCAPI調用來提交已簽名的請求，或者您可以使用第三方庫，例如. AXIOS 下面的例子演示了如何使一個比特幣 JSON-RPC 請求AMB訪問比特幣端點。

Example

若要執行此範例 Node.js 指令碼，請套用下列先決條件：

1. 您的電腦上必須安裝節點版本管理員 (nvm) 和 Node.js。您可以在這裡找到作業系統的安裝說明。
2. 使用指`node --version`令並確認您使用的是節點版本 14 或更高版本。如果需要，您可以使用`nvm install 14`命令，然後使用`nvm use 14`命令來安裝版本 14。
3. 環境變數`AWS_ACCESS_KEY_ID`和`AWS_SECRET_ACCESS_KEY`必須包含與您的帳戶相關聯的認證。環境變量`AMB_HTTP_ENDPOINT`必須包含您的AMB訪問比特幣端點。

   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使用者帳戶中的適當值。

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

完成所有必要條件後，請使用編輯器將下列`package.json`檔案和`index.js`指令碼複製到本機環境中：

包裝

```
{
  "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();
```

前面的示例代碼使用 Axios 向 Bitcoin 端點發出RPC請求，並使用官方的簽名版本 4（Sigv4）標頭對這些請求進行簽名 AWS SDKV3 工具。若要執行程式碼，請在與檔案相同的目錄中開啟終端機，然後執行下列命令：

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

產生的結果如下所示：

```
{"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要求會使用與範使AMB訪問比特幣 JSON-通過使用 awscurl 中的RPC請求 AWS CLI例相同的輸入參數區塊雜湊進行`getblock`呼叫。要進行其他調用，用不同的 Bitcoin 修改腳本中的`rpc`對象 JSON-RPC。您可以將主機屬性選項更改為 Bitcoin `testnet` 以在該端點上撥打電話。

使用AMB訪問比特幣 AWS PrivateLink

AWS PrivateLink 是一種高可用性、可擴展的技術，您可以使用它來私下連接VPC到服務，就像它們在您的VPC. 您不必使用互聯網閘道，NAT設備，公共 IP 地址， AWS 直接 Connect 連接，或 AWS 站點對站點VPN連接，可從您的私有子網路與服務進行通訊。如需關於 AWS PrivateLink 或設置 AWS PrivateLink，請參閱什麼是 AWS PrivateLink?

您可以發送比特幣 JSON-AMB 訪問比特幣的RPC請求 AWS PrivateLink 通過使用VPC端點。對此私有端點的請求不會通過開放的互聯網傳遞，因此您可以使用相同的 Sigv4 身份驗證將請求直接發送到 Bitcoin 端點。如需詳細資訊，請參閱存取 AWS 通過服務 AWS PrivateLink.

對於服務名稱，請查找 Amazon Managed Blockchain AWS 服務列。如需詳細資訊，請參閱 AWS 與之整合的服務 AWS PrivateLink。 端點的服務名稱將採用下列格`com.amazonaws.`*`AWS-REGION`*`.managedblockchain.bitcoin.`*`NETWORK-TYPE`*式：

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

Amazon Managed Blockchain（AMB）的比特幣使用案例訪問比特幣

本主題提供了 AMB 訪問比特幣用例列表

主題

建立一個比特幣（BTC）錢包以發送和接收 BTC

BTC 是比特幣網絡上的本地加密貨幣，是網絡安全模型的重要組成部分。它還充當商品和交易媒介，被機構，企業和個人廣泛使用。因此，許多錢包應用程序依靠比特幣節點與比特幣區塊鏈進行交互。這些應用程序計算一組給定地址的未使用輸出（UTXOS）的餘額，簽名並將交易發送到比特幣網絡，並檢索有關歷史交易的數據。

以下是 Amazon Managed Blockchain（AMB）訪問比特幣支持 BTC 錢包交易的一些比特幣 JSON RPC 的示例：

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

如需詳細資訊，請參閱 支持 JSON-接收。

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 允許您訪問指標，例如每秒平均交易速率，總交易計數，塊數等。如有需要，您也可以將區塊編號或區塊雜湊視窗定義為分隔符號，以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 支持 JSON-接收。

驗證使用比特幣 key pair 簽名的消息

比特幣錢包有一個私鑰和一個組成密鑰對的公鑰。這些密鑰用於簽署交易並充當區塊鏈上的用戶身份。公鑰用於創建地址，這些地址是標準化的字母數字標識符（長度為 27 到 34 個字符）。這些地址用於接收 BTC 輸出並處理交易或消息。

使用比特幣錢包，用戶還可以加密簽名和驗證消息。此過程通常用於證明特定錢包地址以及與之相關聯的 BTC 的所有權。通過使用`verifymessage`比特幣 JSON-RPC，您可以檢查另一個錢包簽名的消息的真實性和有效性。具體來說，Bitcoin 節點可以用來驗證消息是否已使用與簽名消息本身中提供的公鑰派生地址相對應的私鑰進行簽名。

如需詳細資訊，請參閱 支持 JSON-接收。

檢查比特幣內存池

許多應用程序需要訪問 mempool 來跟踪待處理的事務，獲取所有待處理事務的列表，或者找出事務來自哪裡。要做到這一點，有比特幣 JSON-RPC 一樣 `getmempoolancestorsgetmempoolentry`，並且支持`getrawmempool`此活動。這些比特幣 JSON-RPC 幫助應用程序從內存池中獲取所需的信息。

Amazon Managed Blockchain（AMB）訪問比特幣還支持`testmempoolaccept`比特幣 JSON RPC，它允許您驗證交易是否符合協議規則，並且在提交之前被節點接受。錢包，交易所以及直接向比特幣區塊鏈提交交易的任何其他實體都使用這些比特幣 JSON-RPC。

如需更多詳細資訊，請參閱 支持 JSON-接收。

使用 Amazon Managed Blockchain（AMB）支持的比特幣 JSON RPC 訪問比特幣

本主題提供託管區塊鏈支持的比特幣 JSON RPC 的列表和引用。每個支持的 JSON-RPC 都有其使用的簡要說明。

Note

- 您可以使用簽名版本 4（SIGv4）簽名過程在託管區塊鏈上對比特幣 JSON-RPC 進行身份驗證。這意味著只有 AWS 帳戶中獲得授權的 IAM 主體才能使用比特幣 JSON RPC 與其互動。在呼叫中提供 AWS 憑據（訪問密鑰 ID 和秘密訪問密鑰）。
- 如果您的 HTTP 回應大於 10 MB，您將會收到錯誤訊息。若要更正此問題，您必須將壓縮標頭設定為`Accept-Encoding:gzip`。您的用戶端接收到的壓縮回應包含下列標頭：`Content-Type: application/json`和`Content-Encoding: gzip`。
- 亞馬 Amazon Managed Blockchain（AMB）訪問比特幣會針對格式錯誤的 JSO-RPC 請求生成 400 個錯誤。
- 使用 `sendrawtransaction` JSON-RPC 提交更新比特幣區塊鏈狀態的交易。
- AMB 訪問比特幣的默認請求限制為每秒 100 個請求（RPS）`NETWORK_TYPE`，每 AWS 個區域。

  若要增加配額，您必須聯絡AWS 支援人員。若要聯絡 S AWS upport，請登入AWS 支援中心主控台。選擇建立案例。選擇 [技術]。選擇託管區塊鏈作為您的服務。選擇訪問：比特幣作為您的類別，並選擇一般指導作為嚴重程度。輸入 RPC 配額作為主旨，並在說明文字方塊中列出適用於您需求的配額限制，以每個區域每個比特幣網路的 RPS 列出。提交您的案例。

支持 JSON-接收

AMB 訪問比特幣支持以下比特幣 JSON-RPC。每個支援的呼叫都有其使用方式的簡短說明。

類別	JS-RPC	描述
區塊鏈 RPC	獲得最佳塊鏈	傳回工作最完整驗證鏈中最佳 (tip) 區塊的雜湊值。

類別	JS-RPC	描述
	獲取塊	如果詳細程度為 0，則會傳回區塊「雜湊」序列化、十六進位編碼資料的字串。如果詳細程度為 1，則返回一個包含有關塊「哈希」信息的對象。如果詳細程度為 2，則返回一個 Object，其中包含有關塊「哈希」和每個事務的信息。如果詳細程度為 3，則返回一個 Object，其中包含有關塊「哈希」的信息以及每個事務的信息，包括輸入`prevout`信息。
	獲取塊鏈信息	返回包含有關區塊鏈處理的各種狀態信息的對象。
	獲取塊計數	傳回最多工作且經過完整驗證的鏈結的高度。創世紀塊的高度為 0。
	獲取塊過濾器	使用區塊雜湊擷取特定區塊的 BIP 157 內容篩選器。
	獲取塊卡什	在 best-block-chain 提供的高度返回塊的哈希值。
	。頭部。	如果詳細為 false，則返回一個字符串，該字符串被序列化，用於塊頭「哈希」的十六進制編碼數據。如果詳細為 true，則返回一個包含有關塊頭「哈希」信息的對象。
	獲取塊狀態	計算給定窗口的每個塊統計信息。所有金額都以薩托希斯為單位。它不適用於修剪的一些高度。
	獲取鏈技巧	傳回有關圖塊樹中所有已知提示的資訊，包括主鏈和孤立分支。
	獲取鏈接	計算鏈結中交易總數和比率的統計資料。
	獲得困難	以最小 proof-of-work 難度的倍數傳回難度。
	得到內存池祖先	如果 txid 在內存池中，則返回所有內存池祖先。

類別	JS-RPC	描述
	得到內存池後代	如果 txid 在內存池中，則返回所有內存池後代。
	獲取內存池條目	返回給定事務的內存池數據。
	元素池	返回 TX 內存池的活動狀態的詳細信息。
	儲存池	返回內存池中的所有事務 ID 作為字符串事務 ID 的 JSON 數組。 Note 不支援 `verbose = true`。
	收入輸出	傳回未使用交易輸出的詳細資訊。
	防止吸收	傳回區塊中包含「txid」的十六進位編碼證明。
罗交易 RPC	創建交易	創建支出給定輸入並創建新輸出的交易。
	解碼器交易	傳回代表序列化、十六進位編碼交易的 JSON 物件。
	解碼	解碼一個十六進制編碼的腳本。
	二次交易	返回原始交易數據。
	感應交易	提交原始事務（序列化，十六進制編碼）到本地節點和網絡。
	測試池接受	返回 mempool 驗收測試的結果，指示原始事務（序列化，十六進制編碼）是否會被 mempool 接受。這會檢查交易是否違反一致或策略規則。
使用 RPC	創建多重簽名	創建一個多簽名地址，其中需要 m 個密鑰的 n 個簽名。

類別	JS-RPC	描述
	估計費	如果可能，估計交易在 conf_target 區塊內開始確認所需的每千位元組大約費用，並傳回估計有效的區塊數。使用 BIP 141 (見證資料折扣) 中所定義的虛擬交易大小。
	驗證地址	返回有關給定的比特幣地址的信息。
	驗證消息	驗證已簽署的郵件。

Amazon Managed Blockchain（AMB）中的安全性訪問比特幣

雲安全性 AWS 是最高優先級的。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同的責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。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) 存取比特幣的合規計劃，請參閱合規計劃範圍內的AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 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 使用 AWS 受管區塊鏈中執行的開放原始碼架構的功能和功能。

本文檔幫助您了解如何在使用 AMB Access 比特幣時應用共同責任模型。以下主題向您展示如何配置 AMB Access 比特幣以滿足您的安全性和合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AMB Access 比特幣資源。

主題

- Amazon Managed Blockchain 中的資料保護 (AMB) 存取比特幣
- 亞馬遜託管區塊鏈的身份和訪問管理（AMB）訪問比特幣

Amazon Managed Blockchain 中的資料保護 (AMB) 存取比特幣

所以此 AWS 共同責任模型適用於 Amazon Managed Blockchain (AMB) 存取比特幣中的資料保護。如本模型所述， AWS 負責保護運行所有的全球基礎設施 AWS 雲端。 您有責任維持對託管在此基礎結構上的內容的控制權。您也必須負責安全性設定與管理工作 AWS 服務 你使用. 如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱 AWS 共同責任模型和 GDPR博客文章 AWS 安全部落格。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM)。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：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。 如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱使用 CloudTrail 系統線 AWS CloudTrail 用戶指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 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。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，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AMB使用訪問比特幣或其他工作 AWS 服務 使用控制台API， AWS CLI，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URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

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資料儲存系統讀取資料。這包括在網路傳輸時可能遭到攔截的資料，稱為傳輸中的資料。

傳輸中加密

默認情況下，託管區塊鏈使用HTTPS/TLS連接來加密從運行該計算機的客戶端計算機傳輸的所有數據 AWS CLI 至 AWS 服務端點。

你不需要做任何事情來啟用HTTPS/的使用TLS。除非您為個人明確禁用它，否則它始終處於啟用狀態 AWS CLI 使用指令`--no-verify-ssl`執行指令。

亞馬遜託管區塊鏈的身份和訪問管理（AMB）訪問比特幣

AWS Identity and Access Management (IAM) 是 AWS 服務 協助系統管理員安全地控制存取 AWS 的費用。IAM管理員控制誰可以進行身份驗證（登錄）和授權（有權限）使用 AMB Access Bitcoin 資源。IAM是一個 AWS 服務 您可以免費使用。

主題

物件

您如何使用 AWS Identity and Access Management （IAM）不同，這取決於你在AMB訪問比特幣做的工作。

服務使用者 — 如果您使用 AMB Access Bitcoin 服務完成工作，則您的管理員會為您提供所需的憑據和權限。當您使用更多 AMB Access Bitcoin 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存AMB取比特幣中的某項功能，請參閱疑難排解 Amazon Managed Blockchain (AMB) 存取比特幣身分和存取。

服務管理員 — 如果您負責AMB訪問公司的比特幣資源，則可能擁有訪問比特幣的完全AMB訪問權限。您的工作就是確定您的服務用戶應該AMB訪問哪些 Access Bitcoin 功能和資源。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。要了解有關貴公司如何IAM與 AMB Access 比特幣一起使用的更多信息，請參閱亞馬遜託管區塊鏈（AMB）訪問比特幣如何與 IAM。

IAM管理員 — 如果您是管理IAM員，您可能想了解如何編寫政策來管理 AMB Access Bitcoin 的存取權限的詳細資訊。若要檢視您可以在中使用的AMB存取 Bitcoin 身分型政策範例IAM，請參閱。Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣

使用身分驗證

驗證是您登入的方式 AWS 使用您的身份證明。您必須經過驗證 (登入 AWS) 作為 AWS 帳戶根使用者，以IAM使用者身分或假定IAM角色。

您可以登入 AWS 使用透過身分識別來源提供的認證做為聯合身分識別。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您存取 AWS 通過使用聯合，您間接擔任一個角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱如何登入您的 AWS 帳戶 中的 AWS 登入 使用者指南。

如果您訪問 AWS 編程方式， AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果你不使用 AWS 工具，您必須自己簽署請求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱簽署AWS API《IAM用戶指南》中的請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如 AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。要了解更多信息，請參閱中的多因素身份驗證 AWS IAM Identity Center 用戶指南和使用多因素身份驗證（MFA）AWS (在 IAM 使用者指南中)

AWS 帳戶 根使用者

當你創建一個 AWS 帳戶時，您會從一個擁有完整存取權限的登入身分開始 AWS 服務 和帳戶中的資源。這個身份被稱為 AWS 帳戶 root 使用者，並透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要管理員存取權的使用者) 使用與身分識別提供者的同盟來存取 AWS 服務 通過使用臨時憑據。

聯合身分是來自您企業使用者目錄的使用者、Web 身分識別提供者、 AWS Directory Service、身分識別中心目錄或存取的任何使用者 AWS 服務 使用透過身分識別來源提供的認證。同盟身分存取時 AWS 帳戶，他們假定角色，並且角色提供臨時認證。

對於集中式存取管理，我們建議您使用 AWS IAM Identity Center。 您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在您的所有身分識別來源中使用 AWS 帳戶 和應用程序。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在 AWS IAM Identity Center 使用者指南。

IAM 使用者和群組

用IAM戶是您的身份 AWS 帳戶 具有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您的身份 AWS 帳戶 具有特定權限。它類似於用IAM戶，但不與特定人員相關聯。您可以暫時IAM擔任 AWS Management Console 通過切換角色。您可以通過調用一個角色 AWS CLI 或 AWS API操作或通過使用自定義URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關權限集的資訊，請參閱 AWS IAM Identity Center 使用者指南。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，有一些 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 一些 AWS 服務 使用其他中的功能 AWS 服務。 例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色在 AWS，您被視為校長。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS使用主體呼叫 AWS 服務，結合請求 AWS 服務 向下游服務提出請求。FAS只有當服務收到需要與其他人互動的請求時才會發出請求 AWS 服務 或要完成的資源。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱建立角色以將權限委派給 AWS 服務 (在 IAM 使用者指南中)

- 服務連結角色 — 服務連結角色是連結至 AWS 服務。 服務可以扮演角色代表您執行動作。服務連結角色會顯示在您的 AWS 帳戶 並由服務擁有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行並製作的應用程式的臨時登入資料 AWS CLI 或 AWS API請求。這比在EC2實例中存儲訪問密鑰更好。若要指派 AWS EC2執行個體的角色並讓它可供其所有應用程式使用，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以控制存取 AWS 藉由建立原則並將其附加至 AWS 身分識別或資源。原則是中的物件 AWS 當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數策略都存儲在 AWS 作為JSON文件。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該策略的使用者可以從 AWS Management Console，該 AWS CLI，或 AWS API.

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的多個使用者、群組和角色 AWS 帳戶。 受管政策包

括 AWS 受管理的政策和客戶管理的政策。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務.

資源型政策是位於該服務中的內嵌政策。你不能使用 AWS 在以資源為基礎的策略IAM中受管理的策略。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3， AWS WAF和 Amazon VPC 是支持的服務的例子ACLs。若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略（SCPs）— SCPs 是指定中組織或組織單位（OU）的最大權限的JSON策略 AWS Organizations. AWS Organizations 是一種用於分組和集中管理多個服務 AWS 帳戶 您的企業擁有。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者。 如需有關 Organizations 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作

階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何 AWS 決定當涉及多個原則類型時是否允許要求，請參閱《IAM使用指南》中的「原則評估邏輯」。

亞馬遜託管區塊鏈（AMB）訪問比特幣如何與 IAM

在您用IAM來管理訪問比特幣的AMB訪問之前，請了解哪些IAM功能可以與 AMB Access 比特幣一起使用。

IAM您可以與 Amazon Managed Blockchain 一起使用的功能（AMB）訪問比特幣

IAM特徵	AMB訪問比特幣支持
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
ACLs	否
ABAC(策略中的標籤)	否
暫時性憑證	否
主體許可	否
服務角色	否
服務連結角色	否

要獲得如何AMB訪問比特幣和其他的高層次視圖 AWS 服務適用於大多數IAM功能，請參閱 AWS《IAM使用者指南》IAM中使用的服務。

訪問比特幣的基於身份的AMB政策

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

訪問比特幣的基於身份的政策示例 AMB

若要檢視AMB存取以比特幣身分識別為基礎的政策範例，請參閱。Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣

AMB訪問比特幣中基於資源的策略

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務.

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者與資源不同時 AWS 帳戶，受信任帳戶中的IAM系統管理員也必須授與主參與者實體 (使用者或角色) 存取資源的權限。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

AMB訪問比特幣的政策行動

支援政策動作：是

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的名稱相同 AWS API操作。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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存取比特幣動作清單，請參閱服務授權參考中的 Amazon 受管區塊鏈定義的動作 (AMB) 存取比特幣。

AMB訪問比特幣中的策略操作在操作之前使用以下前綴：

```
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存取以比特幣身分識別為基礎的政策範例，請參閱。Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣

AMB訪問比特幣的政策資源

支援政策資源：否

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 AMB Access Bitcoin 資源類型及其清單ARNs，請參閱服務授權參考資料中的 Amazon 受管區塊鏈定義的資源 (AMB) 存取比特幣。若要了解您可以針對每個資源指定哪些動作，請參閱 Amazon 受管區塊鏈定義ARN的動作 (AMB) 存取比特幣。

若要檢視AMB存取以比特幣身分識別為基礎的政策範例，請參閱。Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣

AMB存取比特幣的政策條件金鑰

支援服務特定政策條件金鑰：否

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。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。

如果您在一個語句中指定多個Condition元素，或在單個Condition元素中指定多個鍵， AWS 使用邏輯AND操作評估它們。如果您為單個條件鍵指定多個值， AWS 使用邏輯OR運算評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看全部 AWS 全域條件索引鍵，請參閱 AWS《IAM使用指南》中的整體條件前後關聯鍵字。

若要查看AMB存取比特幣條件金鑰清單，請參閱服務授權參考中的 Amazon Managed Blockchain 的條件金鑰 (AMB) 存取比特幣。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon 受管區塊鏈定義的動作 (AMB) 存取比特幣。

若要檢視AMB存取以比特幣身分識別為基礎的政策範例，請參閱。Amazon Managed Blockchain（AMB）基於身份的政策示例訪問比特幣

ACLs在AMB訪問比特幣

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與AMB訪問比特幣

支援 ABAC (策略中的標籤): 否

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。In (入) AWS，這些屬性稱為標籤。您可以將標籤附加到IAM實體 (使用者或角色) 以及許多實體 AWS 的費用。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

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。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM〉。

使用臨時憑據AMB訪問比特幣

支持臨時憑據：否

一些 AWS 服務 使用臨時憑據登錄時不起作用。有關其他信息，包括哪些 AWS 服務 使用臨時憑證，請參閱 AWS 服務 在《IAM使用者指南》IAM中使用。

如果您登入，則使用臨時登入資料 AWS Management Console 使用除了使用者名稱和密碼之外的任何方法。例如，當您訪問時 AWS 使用貴公司的單一登入 (SSO) 連結，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用手動建立臨時認證 AWS CLI 或 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS. 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。

存取比特幣的跨服務主體AMB權限

支持轉發訪問會話（FAS）：否

當您使用使用IAM者或角色執行動作 AWS，您被視為校長。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS使用主體呼叫 AWS 服務，結合請求 AWS 服務 向下游服務提出請求。FAS只有當服務收到需要與其他人互動的請求時才會發出請求 AWS 服務 或要完成的資源。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

AMB訪問比特幣的服務角色

支援服務角色：否

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱建立角色以將權限委派給 AWS 服務 (在 IAM 使用者指南中)

> **Warning**
>
> 變更服務角色的權限可能會中斷AMB存取比特幣功能。只有在AMB訪問比特幣提供指導時才編輯服務角色。

訪問比特幣的服務鏈AMB接角色

支援服務連結角色：否

服務連結角色是一種服務角色類型，連結至 AWS 服務。 服務可以扮演角色代表您執行動作。服務連結角色會顯示在您的 AWS 帳戶 並由服務擁有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需建立或管理服務連結角色的詳細資訊，請參閱 AWS 與之合作的服務IAM。在表格中尋找服務，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）基於身份的政策示例訪問比特幣

默認情況下，用戶和角色沒有創建或修改AMB訪問比特幣資源的權限。他們也無法執行任務使用 AWS Management Console, AWS Command Line Interface (AWS CLI)，或 AWS API。若要授與使用者對

所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

有關 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格式，請參閱 Amazon Managed Blockchain 的動作、資源和條件金鑰 (AMB) 存取服務授權參考中的比特幣。ARNs

主題

- 政策最佳實務
- 使用AMB訪問比特幣控制台
- 允許使用者檢視他們自己的許可
- 訪問比特幣網絡

政策最佳實務

基於身份的政策決定了某人是否可以創建，訪問或刪除AMB訪問您帳戶中的比特幣資源。這些動作可能會為您帶來成本 AWS 帳戶。 建立或編輯以身分識別為基礎的原則時，請遵循下列準則和建議：

- 開始使用 AWS 受管原則並朝著最低權限權限移轉 — 若要開始授與使用者和工作負載的權限，請使用 AWS 授與許多常見使用案例權限的受管理策略。他們是可用的 AWS 帳戶。 我們建議您透過定義來進一步減少使用權限 AWS 針對您的使用案例特定的客戶管理政策。如需詳細資訊，請參閱 AWS 受管理的策略或 AWS 《使用者指南》 中針對工作職能的IAM管理策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。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。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。如果服務動作是透過特定使用條件，您也可以使用條件來授與對服務動作的存取權 AWS 服務，例如， AWS CloudFormation。 如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。

- 需要多重要素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟MFA以獲得額外的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

使用AMB訪問比特幣控制台

若要存取 Amazon Managed Blockchain (AMB) 存取比特幣主控台，您必須擁有最低限度的許可集。這些權限必須允許您列出並查看有關AMB訪問比特幣資源的詳細信息 AWS 帳戶。 如果您建立的以身分識別為基礎的原則比所需的最低權限更嚴格，則控制台將無法如預期用於具有該原則的實體 (使用者或角色) 運作。

您不需要針對只撥打電話的使用者允許最低主控台權限 AWS CLI 或 AWS API。相反地，只允許存取符合他們嘗試執行之API作業的動作。

為了確保用戶和角色仍然可以使用 AMB Access 比特幣控制台，還可以附加AMB訪問比特幣*ConsoleAccess*或 *ReadOnly* AWS 對實體的管理策略。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上完成此動作的權限，或以程式設計方式使用 AWS CLI 或 AWS API.

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

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

訪問比特幣網絡

> **Note**
>
> 為了訪問比特幣的公共端點`mainnet`並`testnet`進行 JSON-RPC 呼叫，您將需要具有 AMB Access Bitcoin IAM 權限的用戶憑據（`AWS_ACCESS_KEY_ID`和`AWS_SECRET_ACCESS_KEY`）。

Example IAM訪問所有比特幣網絡的政策

此範例會授予您的IAM使用者 AWS 帳戶 訪問所有的比特幣網絡。

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

```
}
```

Example IAM訪問比特幣測試網絡的策略

此範例會授予您的IAM使用者 AWS 帳戶 訪問比特幣testnet網絡。

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

疑難排解 Amazon Managed Blockchain (AMB) 存取比特幣身分和存取

使用以下信息來幫助您診斷和修復使用 AMB Access Bitcoin 和時可能遇到的常見問題IAM。

主題

- 我沒有授權在AMB訪問比特幣中執行操作
- 我沒有授權執行 iam：PassRole
- 我想讓我以外的人 AWS 帳戶 訪問我的AMB訪問比特幣資源

我沒有授權在AMB訪問比特幣中執行操作

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。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的managedblockchain::*GetWidget*權限時，就會發生下列範例錯誤。

```
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。

我沒有授權執行 iam：PassRole

如果您收到錯誤訊息，指出您未獲授權執行iam:PassRole動作，則必須更新您的政策以允許您將角色傳遞給 AMB Access Bitcoin。

一些 AWS 服務 可讓您將現有角色傳遞至該服務，而非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。

當名為的使用IAM者marymajor嘗試使用主控台在 AMB Access Bitcoin 中執行動作時，就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 沒有將角色傳遞至該服務的許可。

```
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。

我想讓我以外的人 AWS 帳戶 訪問我的AMB訪問比特幣資源

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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 要了解 AMB Access 比特幣是否支持這些功能，請參閱亞馬遜託管區塊鏈（AMB）訪問比特幣如何與 IAM。
- 了解如何提供對您資源的存取權 AWS 帳戶 您擁有的，請參閱為其他IAM使用者提供存取權AWS 帳戶 您在IAM用戶指南中擁有的。
- 瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱提供存取權限AWS 帳戶 由IAM用戶指南中的第三方擁有。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權(身分聯合)。

- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

日誌記錄 Amazon Managed Blockchain（AMB）通過使用訪問比特幣事件 AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain（AMB）訪問比特幣不支持管理事件。

Amazon Managed Blockchain 與服務整合在一起 AWS CloudTrail，該服務可提供受管區塊鏈中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 捕獲為託管區塊鏈調用 AMB Access 比特幣端點作為數據平面事件的人員。

如果您建立已訂閱以接收所需資料平面事件的正確設定追蹤，您可以接收 AMB Access Bitcoin 相關 CloudTrail 事件的持續傳遞到 Amazon S3 儲存貯體。使用收集的信息 CloudTrail，您可以確定是否向其中一個 AMB Access Bitcoin 端點提出請求，請求來自的 IP 地址，提出請求的時間以及其他其他詳細信息。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

AMB 訪問比特幣信息 CloudTrail

AWS CloudTrail 默認情況下，當您創建 AWS 帳戶. 但是，要查看誰調用了 AMB Access 比特幣端點，您必須配置 CloudTrail 以記錄數據平面事件。

要保留您的事件的持續記錄 AWS 帳戶，包括 AMB Access Bitcoin 的數據平面事件，您必須創建一個跟踪。跟踪使日誌文件 CloudTrail 交付到 Amazon S3 存儲桶。依預設，當您在中建立系統線時 AWS Management Console，系統線會套用至所有系統線 AWS 區域。追蹤記錄來自 AWS 分區中所有受支援區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務以進一步分析此資料，並對 CloudTrail 記錄檔中收集的事件資料採取行動。如需詳細資訊，請參閱下列內容：

- 用 CloudTrail 來跟踪比特幣 JSON-RPC
- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

通過分析數 CloudTrail 據事件，您可以監控調用 AMB Access 比特幣端點的人員。

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：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 要求是使用角色或同盟使用者的暫時安全性登入資料來提出。
- 請求是否由其他 AWS 服務提出。

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

了解 AMB 訪問比特幣日誌文件條目

對於資料平面事件，追蹤是一種組態，可讓事件以日誌檔的形式傳遞至指定的 S3 儲存貯體。每個 CloudTrail 記錄檔都包含一或多個記錄項目，這些記錄項目代表來自任何來源的單一要求。這些項目提供有關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**
>
> CloudTrail 日誌文件中的數據事件不是 AMB Access 比特幣 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

用 CloudTrail 來跟踪比特幣 JSON-RPC

您可以使用 CloudTrail 來追蹤您帳戶中的使用者呼叫 AMB Access 比特幣端點，以及調用了哪些 JSON-RPC 作為資料事件。根據預設，當您建立追蹤時，不會記錄資料事件。要記錄誰將 AMB Access Bitcoin 端點調用為 CloudTrail 數據事件，您必須明確地將支持的資源或資源類型添加到跟踪中。Amazon Managed Blockchain 支援使用 AWS Management Console、 AWS SDK 和 AWS CLI. 如需詳細資訊，請參閱《使用指南》中的使用進階選取器記錄事件。AWS CloudTrail

若要在追蹤中記錄資料事件，請在建立追蹤後使用該put-event-selectors作業。使用選`--advanced-event-selectors`項指定`AWS::ManagedBlockchain::Network`資源類型，以便開始記錄資料事件，以判斷誰叫用 AMB Access Bitcoin 端點。

Example 您帳戶所有 AMB Access 比特幣端點請求的數據事件日誌條目

以下示例演示瞭如何使用該`put-event-selectors`操作來記錄您帳戶的所有 AMB Access Bitcoin 端點請求，以了解該`us-east-1`地區`my-bitcoin-trail`中的跟踪。

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

訂閱之後，您可以追蹤 S3 儲存貯體中連線至上個範例中指定之追蹤的使用情況。

下列結果顯示所收集之資訊的資 CloudTrail 料事件記錄項目 CloudTrail。您可以確定是否向其中一個 AMB Access Bitcoin 端點提出了比特幣 JSON-RPC 請求，請求來自的 IP 地址，提出請求的時間以及其他其他詳細信息。

```
{
        "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。