aws

開發人員指南

AMB 存取多邊形

AMB 存取多邊形: 開發人員指南

Table of Contents

Amazon Managed Blockchain（AMB）訪問多邊形處於預覽版本中，可能會發生變化。

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。

什麼是 Amazon Managed Blockchain（AMB）訪問多邊形？

Amazon Managed Blockchain（AMB）訪問多邊形是一項全受管服務，可幫助您在多邊形區塊鏈上構建具有彈性的 Web3 應用程序。AMB 訪問多邊形提供對多邊形區塊鏈的即時和無服務器訪問。

多邊形是使用以太坊虛擬機（EVM）作為基礎的擴展解決方案。多邊形區塊鏈以高交易吞吐量和低交易費用而聞名。多邊形區塊鏈使用 proof-of-stake 共識機制。多邊形通常用於構建與 NFT，Web3 遊戲和標記化用例相關的去中心化應用程序（DApps）。

本指南介紹瞭如何使用亞馬遜託管區塊鏈（AMB）訪問多邊形創建和管理多邊形區塊鏈資源。

首次 AMB 訪問多邊形用戶的資源

如果這是您第一次使用 AMB 存取多邊形，我們建議您先閱讀以下章節：

- 關鍵概念：Amazon Managed Blockchain（AMB）訪問多邊形
- 開始使用 Amazon Managed Blockchain（AMB）訪問多邊形
- 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC

關鍵概念：Amazon Managed Blockchain（AMB）訪問多邊形

> **Note**
>
> 本指南假設您熟悉 Polygon 必不可少的概念。這些概念包括放樣，DApp，交易，錢包，智能合約，Polygon（POL，以前的 MATIC）等。在使用 Amazon Managed Blockchain（AMB）訪問多邊形之前，我們建議您查看多邊形開發文檔和多邊形維基。

Amazon Managed Blockchain（AMB）訪問多邊形為您提供對多邊形主網和多邊形主網絡的無服務器訪問，而無需您佈建和管理任何多邊形基礎設施，包括節點。網絡上的多邊形節點共同存儲多邊形區塊鏈狀態，驗證交易並參與共識以改變區塊鏈狀態。您可以使用此託管服務快速，按需訪問 Polygon 網絡，從而降低整體擁有成本。

使用 AMB 存取多邊形，您可以存取 JSON 遠端程序 (JSON-RPC) 呼叫。您可以調用多邊形 JSON-RPC 通過託管區塊鏈管理的節點與多邊形區塊鏈進行通信。您可以使用 AMB 訪問多邊形服務來開發和使用與多邊形區塊鏈交互的去中心化應用程序（dApp）。DApp 的一個組成部分是智能合約。您可以使用 AMB 訪問多邊形創建智能合約並將其部署到多邊形區塊鏈中。您還可以通過對像 Polygon 網絡的所有節點以去中心化方式運行的 AMB Access Polygon 端點調用 JSON-RPC 來檢查錢包的餘額，交易詳細信息，估算費用等。任何 Polygon 網絡的同行都可以開發和部署智能合約。

> **Important**
>
> 您負責創建，維護，使用和管理您的 Polygon 地址。您還需要對您的 Polygon 地址的內容負責。 AWS 對於使用 Amazon Managed Blockchain 上的多邊形節點部署或呼叫的任何交易概不負責。

使用 Amazon Managed Blockchain (AMB) 存取多邊形的考量和限制

使用 Amazon Managed Blockchain (AMB) 存取多邊形時，請考慮下列事項：

- 支援多邊形網路

  AMB 接入多邊形支持以下公共網絡：

- 主網-通過 proof-of-stake 共識保護的公共多邊形區塊鏈，並在其上發行和交易多邊形（POL）令牌。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。

- 多邊形不再支援網路
  - 正如多邊形實驗室所傳達的那樣，孟買 Testnet 網絡將在 4 月中旬日落。根據這一消息，AMB 訪問多邊形在 2024 年 4 月 15 日結束了孟買測試網的支持。我們建議您在測試工作負載中使用淘大測試網。
  - 不支援私人網路。
  - 此外，AMB 存取多邊形不包括對多邊形 Zke VM 網路的支援。
- 與流行的第三方編程庫兼容

  AMB Access Polygon 與流行的編程庫（例如 ethers.js）兼容，使開發人員可以使用熟悉的工具與 Polygon 區塊鏈進行交互，從而輕鬆地與其現有實現集成或快速開發新的應用程序。
- 支援的區域

  此服務僅在美國東部 (維吉尼亞北部) 區域提供支援。
- 服務端點

  以下是 AMB 存取多邊形的服務端點。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.polygon.managedblockchain.us-east-1.amazonaws.com`
- 不支持放樣

  AMB 存取多邊形不支援的多邊形 (POL) 驗證程式節點。 proof-of-stake
- 簽名版本 4 簽署多邊形 JSON-RPC 請求

  在 Amazon Managed Blockchain 上對多邊形 JSON RPC 進行呼叫時，您可以透過使用簽名版本 4 簽署程序驗證的 HTTPS 連線進行呼叫。這表示 AWS 帳戶中只有經過授權的 IAM 主體可以進行多邊形 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 政策來限制對個別多邊形 JSON-RPC 的存取。
- Support 基於令牌的訪問

您也可以使用存取子權杖對多邊形網路端點進行 JSON-RPC 呼叫，作為簽章版本 4 (SIGv4) 簽署程序的便利替代方案。您必須`BILLING_TOKEN`從您建立的其中一個存取子權杖提供，並在呼叫中新增為參數。

> **Important**
>
> - 如果您優先考慮安全性和可稽核性而非便利性，請改用 Sigv4 簽署程序。
> - 您可以使用簽名版本 4（SIGv4）和基於令牌的訪問訪問多邊形 JSON RPC。但是，如果您選擇同時使用這兩種通訊協定，則會拒絕您的要求。
> - 您絕對不能在面向使用者的應用程式中嵌入存取子權杖。

- 僅支援原始交易的提交

  使用 `eth_sendrawtransaction` JSON-RPC 提交更新多邊形區塊鏈狀態的交易。

設置 Amazon Managed Blockchain（AMB）訪問多邊形

首次使用 Amazon Managed Blockchain (AMB) 存取多邊形之前，請按照本節中的步驟建立 AWS 帳戶. 下面的章節討論了如何開始使用 AMB 接入多邊形。

使用 AMB 存取多邊形的先決條件

在您第一 AWS 次使用之前，您必須擁有一個 AWS 帳戶.

註冊成為 AWS

當您註冊時 AWS，您的所有人 AWS 帳戶 都會自動註冊 AWS 服務，包括 Amazon Managed Blockchain（AMB）訪問多邊形。您只需針對所使用的服務付費。

如果您已 AWS 帳戶 經擁有，請轉到下一步。如果您還沒有 AWS 帳戶，請使用下列程序建立新帳戶。

若要建立 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，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

建立具有適當權限的 IAM 使用者

要創建和使用 AMB Access Polygon，您必須擁有一個 AWS Identity and Access Management（IAM）主體（用戶或組），該主體（用戶或組）具有允許必要的託管區塊鏈操作的許可。

在 Amazon Managed Blockchain 上對多邊形 JSON RPC 進行呼叫時，您可以透過使用簽名版本 4 簽署程序驗證的 HTTPS 連線進行呼叫。這表示 AWS 帳戶中只有經過授權的 IAM 主體可以進行多邊形 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)。

您也可以使用存取子權杖對多邊形網路端點進行 JSON-RPC 呼叫，作為簽章版本 4 (SIGv4) 簽署程序的便利替代方案。您必須`BILLING_TOKEN`從您建立的其中一個存取子權杖提供，並在呼叫中新增為參

數。不過，您仍然需要 IAM 存取權，才能取得使用 AWS Management Console、 AWS CLI和 SDK 建立存取子權杖的許可。

如需如何建立 IAM 使用者的詳細資訊，請參閱在您的 AWS 帳戶中建立 IAM 使用者。如需如何將許可政策附加至使用者的詳細資訊，請參閱變更 IAM 使用者的許可。如需可用來授與使用者使用 AMB 存取多邊形之權限原則的範例，請參閱Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例。

安裝及設定 AWS Command Line Interface

如果您尚未這樣做，請安裝 latest AWS Command Line Interface (AWS CLI) 以使用終端機中的 AWS 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。

開始使用 Amazon Managed Blockchain（AMB）訪問多邊形

使用本節中的資訊和程序，開始使用 Amazon Managed Blockchain (AMB) 存取多邊形。

主題

建立 IAM 政策以存取多邊形區塊鏈網路

若要存取多邊形主網的公用端點以進行 JSON-RPC 呼叫，您必須擁有具有 Amazon Managed Blockchain (AMBAWS_SECRET_ACCESS_KEY) 存取多邊形的適當 IAM 許可的使用者登入資料 (AWS_ACCESS_KEY_ID和)。在 AWS CLI 已安裝的終端機中，執行以下命令以建立 IAM 政策以存取兩個 Polygon 端點：

```
cat <<EOT > ~/amb-polygon-access-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AMBPolygonAccessPolicy",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcPolygon*"
            ],
            "Resource": "*"
        }
    ]
}
EOT
aws iam create-policy --policy-name AmazonManagedBlockchainPolygonAccess --policy-
document file://$HOME/amb-polygon-access-policy.json
```

> **Note**
>
> 上一個範例可讓您存取所有可用的 Polygon 網路。若要存取特定端點，請使用下列`Action`命令：
>
> - `"managedblockchain:InvokeRpcPolygonMainnet"`

建立政策後，將該政策附加到 IAM 使用者的角色，以使其生效。在中 AWS Management Console，導覽至 IAM 服務，並將政策附加`AmazonManagedBlockchainPolygonAccess`到指派給 IAM 使用者的角色。

在 AMB 存取 RPC 編輯器上使用 AWS Management Console

您可以在 AWS Management Console 使用 AMB 存取多邊形上編輯、設定和提交遠端程序呼叫 (RPC)。使用這些 RPC，您可以在 Polygon 網絡上讀取數據和寫入交易，包括檢索數據並將交易提交到 Polygon 網絡。

Example

下列範例顯示如何使用 `eth_getBlockByNumber` RPC 取得最新區塊的相關資訊。將反白顯示的變數變更為您自己的輸入，或選擇列出的其中一種 RPC 方法，然後輸入所需的相關輸入。

1. 在 https://console.aws.amazon.com/managedblockchain/ 開啟受管理區塊鏈主控台。
2. 選擇 RPC 編輯器。
3. 在「請求」部分中，選擇*`POLYGON_MAINNET`*作為**`#####`**。
4. 選擇*`eth_getBlockByNumber`*作為 RPC 方法。
5. 輸入**`latest`**為**`####`**，並選擇*`False`*作為完整交易旗標。
6. 然後，選擇「提交 RPC」。
7. 您會在 [回應] 區段中取得區`latest`塊的結果。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。

如需詳細資訊，請參閱 AMB 存取多邊形支援的 RPC

透過使用 **awscurl**AWS CLI

Example

使用簽名版本 4 (SIGv4) 使用您的 IAM 使用者登入資料簽署請求，以便向 AMB 存取多邊形端點發出多邊形 JSON-RPC 要求。命awscurl令行工具可以幫助您使用 Sigv4 對 AWS 服務簽署請求。如需詳細資訊，請參閱 .md。

使awscurl用適合您作業系統的方法進行安裝。在 macOS 上，建議使 HomeBrew 用以下應用程式：

```
brew install awscurl
```

如果您已安裝並設定 AWS CLI，則您的 IAM 使用者登入資料和預 AWS 區域 設值會在您的環境中設定，並可存取awscurl。使用awscurl，通過調用 RPC 向多邊形主網提交請求。eth_getBlockByNumber此呼叫接受對應於您要擷取資訊的區塊編號的字串參數。

下列命令會使用params陣列中的區塊編號來選取要擷取標頭的特定區塊，從 Polygon Mainnet 擷取區塊資料。

```
awscurl -X POST -d '{ "jsonrpc": "2.0", "id": "eth_getBlockByNumber-curltest",
 "method":"eth_getBlockByNumber", "params":["latest", false] }' --service
 managedblockchain https://mainnet.polygon.managedblockchain.us-east-1.amazonaws.com -k
```

> **Tip**
>
> 您也可以使用curl和使用令牌基於 AMB 訪問令牌的訪問功能發出相同的Accessor請求。如需詳細資訊，請參閱 為基於令牌的訪問創建和管理訪問令牌以進行 AMB 訪問多邊形請求。
>
> ```
> curl -X POST -d '{"jsonrpc":"2.0", "id": "eth_getBlockByNumber-curltest",
>  "method":"eth_getBlockByNumber", "params":["latest", false] }'
>  'https://mainnet.polygon.managedblockchain.us-east-1.amazonaws.com?
> billingtoken=your-billing-token'
> ```

任一指令的回應都會傳回有關最新區塊的資訊。有關說明目的，請參閱以下示例：

```
{"error":null,"id":"eth_getBlockByNumber-curltest","jsonrpc":"1.0",
      "result":{"baseFeePerGas":"0x873bf591e","difficulty":"0x18",
```

```
      "extraData":"0xd78301000683626f7288676f312e32312e32856c696e757800000000000000000009a
\
      423a58511085d90eaf15201a612af21ccbf1e9f8350455adaba0d27eff0ecc4133e8cd255888304cc
\
      67176a33b451277c2c3c1a6a6482d2ec25ee1573e8ba000",
      "gasLimit":"0x1c9c380","gasUsed":"0x14ca04d",
      "hash":"0x1ee390533a3abc3c8e1306cc1690a1d28d913d27b437c74c761e1a49********;",
      "nonce":"0x0000000000000000","number":"0x2f0ec4d",

 "parentHash":"0x27d47bc2c47a6d329eb8aa62c1353f60e138fb0c596e3e8e9425de163afd6dec",

 "receiptsRoot":"0x394da96025e51cc69bbe3644bc4e1302942c2a6ca6bf0cf241a5724c74c063fd",

 "sha3Uncles":"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
      "size":"0xbd6b",
      "stateRoot":"0x7ca9363cfe9baf4d1c0dca3159461b2cca8604394e69b30af05d7d5c1beea6c3",
      "timestamp":"0x653ff542",
      "totalDifficulty":"0x33eb01dd","transactions":[...],

 "transactionsRoot":"0xda1602c66ffd746dd470e90a47488114a9d00f600ab598466ecc0f3340b24e0c",
      "uncles":[]}}
```

在 Node.js 中製作多邊形 JSON 請求

您可以通過使用 HTTPS 提交簽名的請求來使用 Node.js 中的本機 https 模塊訪問多邊形主網絡來調用多邊形 JSON-RPC，或者您可以使用第三方庫，例如 AXIOS。下列 Node.js 範例說明如何使用簽章版本 4 (SIGv4) 和基於權杖的存取，向 AMB 存取多邊形端點發出多邊形 JSON-RPC 要求。第一個示例將交易從一個地址發送到另一個地址，下面的示例從區塊鏈請求交易詳細信息和餘額信息。

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 18 或更高版本。如果需要，您可以使用`nvm install v18.12.0`命令，然後使用`nvm use v18.12.0`命令來安裝節點的 LTS 版本 18 版本。
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。

   使用下列命令將這些變數匯出為用戶端上的字串。將下列字串中的紅色值取代為 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"
```

完成所有必要條件之後，請使用偏好的程式碼編輯器，將下列檔案複製到本機環境中的目錄中：

包裝

```
{
  "name": "polygon-rpc",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "ethers": "^6.8.1",
    "@aws-crypto/sha256-js": "^5.2.0",
    "@aws-sdk/credential-provider-node": "^3.360.0",
    "@aws-sdk/protocol-http": "^3.357.0",
    "@aws-sdk/signature-v4": "^3.357.0",
    "axios": "^1.6.2"
  }
}
```

dispatch-evm-rpc.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 (rpcEndpoint, rpc) => {

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

  // 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: url,
      data: req.body,
    });
    return response.data;
  } catch (error) {
    console.error("Something went wrong: ", error);
  }
};

module.exports = { rpcRequest: rpcRequest };
```

sendTx.js

> **Warning**
>
> 下面的代碼使用硬編碼的私鑰來生成一個錢包簽名者使Ethers.js用僅用於演示。請勿在生產環境中使用此代碼，因為它具有真正的資金並帶來安全風險。
> 如有需要，請聯絡您的帳戶團隊，以提供有關錢包和簽署者最佳做法的建議。

```
const ethers = require("ethers");

//set AMB Access Polygon endpoint using token based access (TBA)
let token = "your-billing-token"
let url = `https://mainnet.polygon.managedblockchain.us-east-1.amazonaws.com?
billingtoken=${token}`;

//prevent batch RPCs
let options = {
  batchMaxCount: 1,
};

//create JSON RPC provider with AMB Access endpoint and options
let provider = new ethers.JsonRpcProvider(url, null, options);

let sendTx = async (to) => {
  //create an instance of the Wallet class with a private key
  //DO NOT USE A WALLET YOU USE ON MAINNET, NEVER USE A RAW PRIVATE KEY IN PROD
  let pk = "wallet-private-key";
  let signer = new ethers.Wallet(pk, provider);

  //use this wallet to send a transaction of POL from one address to another
  const tx = await signer.sendTransaction({
    to: to,
    value: ethers.parseUnits("0.0001", "ether"),
  });

  console.log(tx);
};

sendTx("recipent-address");
```

readTx.js

```
let rpcRequest = require("./dispatch-evm-rpc").rpcRequest;
let ethers = require("ethers");

let getTxDetails = async (txHash) => {
  //set url to a Signature Version 4 endpoint for AMB Access
  let url = "https://mainnet.polygon.managedblockchain.us-east-1.amazonaws.com";

  //set RPC request body to get transaction details
  let getTransactionByHash = {
    id: "1",
    jsonrpc: "2.0",
    method: "eth_getTransactionByHash",
    params: [txHash],
  };

  //make RPC request for transaction details
  let txDetails = await rpcRequest(url, getTransactionByHash);

  //set RPC request body to get recipient user balance
  let getBalance = {
    id: "2",
    jsonrpc: "2.0",
    method: "eth_getBalance",
    params: [txDetails.result.to, "latest"],
  };

  //make RPC request for recipient user balance
  let recipientBalance = await rpcRequest(url, getBalance);

  console.log("TX DETAILS: ", txDetails.result, "BALANCE: ",
 ethers.formatEther(recipientBalance.result));
};

getTxDetails("your-transaction-id");
```

將這些檔案儲存到目錄後，請使用下列命令安裝執行程式碼所需的相依性：

```
npm install
```

在 Node.js 中傳送交易

前面的示例通過簽署事務並使用 AMB 訪問多邊形將其廣播到多邊形主網從一個地址發送本地多邊形主網（POL）到另一個地址。為此，請使用腳本，該sendTx.js腳本使用了一個流行的庫Ethers.js，用於與以太坊和以太坊兼容的區塊鏈（如 Polygon）進行交互。您需要替換以紅色突出顯示的代碼中的三個變量，包括基於令牌的訪問令牌的訪問令牌，用於簽署事務的私鑰以及接收 POL 的收件人的地址。billingToken

> **Tip**
>
> 我們建議您為此創建一個新的私鑰（錢包），而不是重複使用現有錢包以消除資金損失的風險。您可以使用以太函式庫的錢包類別方法 createranDOM () 來產生要測試的錢包。此外，如果您需要從多邊形主網請求 POL，則可以使用公共 POL 水龍頭請求少量用於測試。

一旦您billingToken有了資金錢包的私鑰，並將收件人的地址添加到代碼中，您可以運行以下代碼來簽署 .0001 POL 的交易，以從您的地址發送到另一個地址並將其廣播到使用 AMB 訪問多邊形調用 eth_sendRawTransaction JSON-RPC 的多邊形主網。

```
node sendTx.js
```

接收回的回應類似下列：

```
TransactionResponse {
provider: JsonRpcProvider {},
blockNumber: null,
blockHash: null,
index: undefined,
hash: '0x8d7538b4841261c5120c0a4dd66359e8ee189e7d1d34ac646a1d9923********',
type: 2,
to: '0xd2bb4f4f1BdC4CB54f715C249Fc5a991********',
from: '0xcf2C679AC6cb7de09Bf6BB6042ecCF05********',
nonce: 2,
gasLimit: 21000n,
gasPrice: undefined,
maxPriorityFeePerGas: 16569518669n,
maxFeePerGas: 16569518685n,
data: '0x',
value: 100000000000000n,
chainId: 80001n,
```

```
signature: Signature {
r: "0x1b90ad9e9e4e005904562d50e904f9db10430a18b45931c059960ede337238ee",
s: "0x7df3c930a964fd07fed4a59f60b4ee896ffc7df4ea41b0facfe82b470db448b7",
yParity: 0,
networkV: null
},
accessList: []
}
```

回應構成交易收據。儲存屬性的值hash。這是您剛提交到區塊鏈的交易標識符。您可以在讀取交易範例中使用此屬性，以從多邊形主網取得有關此交易的其他詳細資訊。

請注意，blockNumber和blockHash正null在回應中。這是因為交易尚未記錄在 Polygon 網路上的一個區塊中。請注意，這些值會在稍後定義，您可能會在下一節要求交易詳細資訊時看到這些值。

在 Node.js 中讀取交易

在本節中，您要求先前提交的交易詳細信息，並使用 AMB Access Polygon 向多邊形主網讀取請求來檢索收件人地址的 POL 餘額。在readTx.js檔案中，取代標示*your-transaction-id*為hash您在上一節執行程式碼時所儲存的回應中所儲存的變數。

此代碼使用一個實用程序dispatch-evm-rpc.js，該實用程序使用 AWS SDK 中必需的簽名版本 4（Sigv4）模塊對 AMB 訪問多邊形簽名 HTTPS 請求，並使用廣泛使用的 HTTP 客戶端 AXIOS 發送請求。

接收回的回應類似下列：

```
TX DETAILS: {
blockHash: '0x59433e0096c783acab0659175460bb3c919545ac14e737d7465b3ddc********',
blockNumber: '0x28b4059',
from: '0xcf2c679ac6cb7de09bf6bb6042eccf05b7fa1394',
gas: '0x5208',
gasPrice: '0x3db9eca5d',
maxPriorityFeePerGas: '0x3db9eca4d',
maxFeePerGas: '0x3db9eca5d',
hash: '0x8d7538b4841261c5120c0a4dd66359e8ee189e7d1d34ac646a1d9923********',
input: '0x',
nonce: '0x2',
to: '0xd2bb4f4f1bdc4cb54f715c249fc5a991********',
transactionIndex: '0x0',
value: '0x5af3107a4000',
type: '0x2',
```

```
accessList: [],
chainId: '0x13881',
v: '0x0',
r: '0x1b90ad9e9e4e005904562d50e904f9db10430a18b45931c059960ede337238ee',
s: '0x7df3c930a964fd07fed4a59f60b4ee896ffc7df4ea41b0facfe82b470db448b7'
} BALANCE: 0.0003
```

響應表示交易詳細信息。請注意，`blockHash`和現`blockNumber`在可能已定義。這表示交易已記錄在區塊中。如果這些值仍然存在`null`，請等待幾分鐘，然後再次執行程式碼以檢查您的交易是否已包含在區塊中。最後，收件者地址餘額（0x110d9316ec000）的十六進制表示使用以太網的方法轉換為十進制，該`formatEther()`方法將十六進制轉換為十進制，並將小數位移動 18（10 ^ 18），以獲得 POL 中的真正平衡。

> **Tip**
>
> 雖然前面的程式碼範例說明如何使用 Node.js、乙醚和 Axios 來利用 AMB 存取多邊形上支援的 JSON RPC，但您可以修改範例，並撰寫其他程式碼，以便使用此服務在多邊形上建置您的應用程式。如需 AMB 存取多邊形上受支援 JSON RPC 的完整清單，請參閱。受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC

為基於令牌的訪問創建和管理訪問令牌以進行 AMB 訪問多邊形請求

您也可以使用存取子權杖對多邊形網路端點進行 JSON-RPC 呼叫，作為簽章版本 4 (SIGv4) 簽署程序的便利替代方案。您必須BILLING_TOKEN從您建立的其中一個存取子權杖提供，並在呼叫中新增為參數。

> **Important**
>
> - 如果您優先考慮安全性和可稽核性而非便利性，請改用 Sigv4 簽署程序。
> - 您可以使用簽名版本 4（SIGv4）和基於令牌的訪問訪問多邊形 JSON RPC。但是，如果您選擇同時使用這兩種通訊協定，則會拒絕您的要求。
> - 您絕對不能在面向使用者的應用程式中嵌入存取子權杖。

在主控台中，[權杖存取子] 頁面會顯示所有存取子權杖的清單，您可以用來從用戶端上的程式碼進行 AMB 存取多邊形 JSON-RPC 呼叫。 AWS 帳戶

如需 AMB 存取多邊形 JSON-RPC 要求的詳細資訊，請參閱。受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC

您可以使用建立和管理存取子權杖。 AWS Management Console您也可以使用下列 API 作業建立和管理存取子權杖：CreateAccessor GetAccessor、ListAccessors、和 DeleteAccessor。A BILLING_TOKEN 是存取子的屬性。此BILLING_TOKEN屬性用於跟踪您的訪問器和計費 AMB 訪問多邊形 JSO-RPC 請求從您的. AWS 帳戶

與建立和管理存取子權杖相關的所有 API 動作也可透過 AWS Management Console AWS CLI、和 SDK 取得。

為基於令牌的訪問創建訪問令牌

您可以建立存取子權杖，並使用它在您的. AWS 帳戶

創建一個訪問器令牌來使 AMB 訪問多邊形 JSO-RPC 請求使用 AWS Management Console

1. 在 https://console.aws.amazon.com/managedblockchain/ 開啟受管理區塊鏈主控台。

2. 選擇權杖存取器。
3. 選擇 [建立存取子]。
4. 選擇有效的多邊形區塊鏈網絡。
5. 選用，為您的存取子新增標籤。
6. 選擇建立存取子以建立新的存取子 Token。

創建一個訪問器令牌來使 AMB 訪問多邊形 JSO-RPC 請求使用 AWS CLI

```
aws managedblockchain create-accessor --accessor-type BILLING_TOKEN --network-type
 POLYGON_MAINNET
```

上一個命令會傳回`AccessorId`與`BillingToken`，如下列範例所示。

```
{
"AccessorId": "ac-NGQ6QNKXLNEBXD3UI6********",
"NetworkType": "POLYGON_MAINNET",
"BillingToken": "jZlP8OUI-PcQSKINyX9euJJDC5-IcW9e-n********"
}
```

在您的回應中的關鍵要素是`BillingToken`. 您可以使用此屬性來進行 AMB 存取多邊形 JSON-RPC 呼叫。出於安全原因，示例中的某些值已被混淆，但將完全出現在實際響應中。

> **Note**
>
> 運行操作後，託管區塊鏈為您佈建並配置令牌。這個過程的長度取決於許多變量。

檢視存取子權杖詳細資訊

您可以檢視您 AWS 帳戶 擁有的每個存取子權杖的屬性。例如，您可以檢視存取子 ID 或存取子的 Amazon 資源名稱 (ARN)。您還可以查看狀態、類型、創建日期和`BillingToken`。

若要使用檢視存取子權杖的資訊 AWS Management Console

1. 在 https://console.aws.amazon.com/managedblockchain/ 開啟受管理區塊鏈主控台。
2. 在瀏覽窗格中，選擇權杖存取器。
3. 從清單中選擇權杖的存取子 ID。

彈出令牌詳細信息頁面。您可以在此頁面檢視權杖的屬性。

若要使用檢視存取子權杖的資訊 AWS CLI

執行下列命令以檢視存取子權杖的詳細資料。`--accessor-id`以您的存取子 ID 取代的值。

```
aws managedblockchain get-accessor --accessor-id ac-NGQ6QNKXLNEBXD3UI6********
```

會傳回`BillingToken`和其他索引鍵屬性，如下列範例所示。出於安全原因，示例中的某些值已被混淆，但完全出現在實際響應中。

```
{
  "Accessor": {
  "Id": "ac-NGQ6QNKXLNEBXD3UI6********",
  "Type": "BILLING_TOKEN",
  "BillingToken": "jZlP8OUI-PcQSKINyX9euJJDC5-IcW9e-n********",
  "Status": "AVAILABLE",
  "NetworkType": "POLYGON_MAINNET"
  "CreationDate": "2022-01-04T23:09:47.750Z",
  "Arn": "arn:aws:managedblockchain:us-east-1:666666666666:accessors/ac-
NGQ6QNKXLNEBXD3UI6********"
  }
}
```

刪除存取子權杖

當您刪除存取子權杖時，權杖會從狀態變更`AVAILABLE`為狀`PENDING_DELETION`態。您無法在`PENDING_DELETION`狀態中使用存取子權杖。

若要使用刪除存取子權杖 AWS Management Console

1. 在 https://console.aws.amazon.com/managedblockchain/ 開啟受管理區塊鏈主控台。
2. 在瀏覽窗格中，選擇權杖存取器。
3. 從清單中選取您想要的存取子權杖。
4. 選擇刪除。
5. 確認您的選擇。

您將返回帶有已刪除的訪問器令牌的令牌訪問器頁面。頁面會顯示`PENDING_DELETION`狀態。

若要使用刪除存取子權杖 AWS CLI

下列範例顯示如何刪除權杖。使用delete-accessor指令刪除權杖。--accessor-id使用您的存取子 ID 設定的值。

使用 CLI 刪除存取子權杖 AWS

```
aws managedblockchain delete-accessor --accessor-id ac-NGQ6QNKXLNEBXD3UI6********
```

如果此命令運行成功，則不會返回任何消息。

受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC

Amazon Managed Blockchain 提供 API 操作，用於為 AMB 訪問多邊形創建和管理令牌訪問器。如需詳細資訊，請參閱受管理區塊鏈 API 參考指南。

下列主題提供 AMB 存取多邊形支援的多邊形 JSON RPC 的清單與參考。每個支持的 JSON-RPC 都有其使用的簡要說明。您可以使用 Polygon JSON-RPC 查詢和獲取智能合約數據，獲取交易詳細信息，提交交易以及其他實用程序，例如在交易上運行跟踪和估算費用。

AMB 訪問多邊形支持以下 JSO-RPC 方法。每個支援的 JSON-RPC 都有其公用程式及其預設要求配額的類別和簡短描述。將 JSON-RPC 方法與 Amazon Managed Blockchain 搭配使用的獨特考量，會在適用的情況下指出。

> **Note**
>
> - 不支援任何未列出的方法。
> - 在 Amazon Managed Blockchain 上對多邊形 JSON RPC 進行呼叫時，您可以透過使用簽名版本 4 簽署程序驗證的 HTTPS 連線進行呼叫。這表示 AWS 帳戶中只有經過授權的 IAM 主體可以進行多邊形 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)。
> - 您也可以使用基於令牌的訪問作為簽名版本 4（SIGv4）簽名過程的便捷替代方法。如果您優先考慮安全性和可稽核性而非便利性，請改用 Sigv4 簽署程序。但是，如果您同時使用 Sigv4 和基於令牌的訪問，則您的請求將無法正常工作。
> - 此預覽的 Amazon Managed Blockchain (AMB) 存取多邊形不支援 JSON-RPC 批次請求。
> - 下表中的配額欄會列出每個 JSON-RPC 的配額。每個 JSON-RPC 在每個多邊形網絡（主網）每個區域的每秒請求數（RPS）中設置配額。
>
>   為了增加您的配額，您必須聯繫 AWS Support。若要聯絡 AWS Support，請登入AWS Support Center Console。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：多邊形作為您的類別，並選擇一般指導作為嚴重性。在 [說明] 文字方塊中輸入 RPC 配額，並在 [說明] 文字方塊清單中輸入 JSON-RPC 以及適用於您需求的配額限制 (以每個區域每個多邊形網路的 RPS 為單位)。提交您的案例。

類別	JS-RPC	描述	考量事項
以太坊	以太區塊編號	返回最近的塊的數量。	
	民俗呼叫	立即執行新的訊息呼叫，而無需在區塊鏈上建立交易。	`eth_call`消耗 0 個氣體，但對於需要它的消息有一個 gas 參數。
	ETH_CHAIN	返回 EIP-155 中引入的當前配置`Chain Id`值的整數值。`None`如果沒有可用`Chain Id`，則返回。	
	估算	估算並返回交易所需的氣體，而無需將交易添加到區塊鏈中。	
	ETH_ 費用歷史	傳回歷史氣體資訊的集合。	
	以太坊汽油價格	返回魏每個天然氣的當前價格。	
	ETH_ 獲取平衡	傳回指定帳戶地址和區塊識別碼的帳戶餘額。	
	以太獲取哈希 BlockBy	返回有關使用塊哈希指定的塊的信息。	

類別	JS-RPC	描述	考量事項
	以太獲取號碼 BlockBy	返回有關使用塊號指定的塊的信息。	
	ET_GET BlockReceipts	傳回有關使用區塊編號指定區塊的收據。	
	以太獲取哈希 BlockTransaction CountBy	返回使用塊哈希指定的塊中的事務數。	
	以太獲取號碼 BlockTransaction CountBy	返回使用塊號指定的塊中的事務數。	
	乙太獲取代碼	返回指定帳戶地址和塊標識符處的代碼。	
	ETH_ 獲取日誌	傳回指定篩選器物件的所有記錄檔陣列。	當提供合約地址時，您可以在`eth_getlogs` 預設為 1K 區塊範圍的任何區塊範圍內提出請求。活性高的合約可能限制在較小的區塊範圍內。如果沒有提供合約地址，區塊範圍將是 8。
	ET_GET RawTransaction ByHash	傳回指定之交易的原始形式`transaction_hash` 。	

類別	JS-RPC	描述	考量事項
	ET_GET StorageAt	針對指定的帳戶位址和區塊識別碼，傳回指定儲存位置的值。	
	ET_GET TransactionBy BlockHash AndIndex	返回有關使用指定塊哈希和事務索引位置的事務信息。	
	ET_GET TransactionBy BlockNumber AndIndex	傳回使用指定區塊編號與交易索引位置之交易的相關資訊。	
	以太獲取哈希 TransactionBy	返回有關具有指定事務哈希事務的信息。	
	ET_GET TransactionCount	返回從指定地址和塊標識符發送的交易數。	
	ET_GET TransactionReceipt	返回使用指定的事務哈希交易的接收。	
	ET_GET UncleBy BlockHash AndIndex	返回有關使用塊哈希和叔叔索引位置指定叔叔塊的信息。	
	ET_GET UncleBy BlockNumber AndIndex	返回有關使用塊號和叔叔索引位置指定叔叔塊的信息。	

類別	JS-RPC	描述	考量事項
	以太獲取哈希 UncleCount ByBlock	返回使用叔叔哈希指定的叔叔的計數數。	
	以太獲取號碼 UncleCount ByBlock	返回使用叔叔號指定的叔叔計數的數量。	
	乙太最大 PriorityFee PerGas	返回每個氣體的費用，該費用是您可以支付多少優先費用或「小費」，以獲取當前區塊中包含的交易。	一般而言，您可以使用此方法傳回的值，`maxFeePerGas` 在您要提交的後續交易中設定。
	乙种协议	返回當前的以太坊協議版本。	
	乙太發送 RawTransaction	為已簽署的交易建立新的訊息呼叫交易或建立合約。	託管區塊鏈僅支持原始交易。在傳送交易之前，您必須先建立並簽署交易。
偵錯	調試跟踪哈希 BlockBy	透過使用追蹤器執行區塊雜湊所指定區塊中的所有交易，傳回可能的追蹤結果編號 (需要追蹤模式)。	

類別	JS-RPC	描述	考量事項
	除錯追蹤編BlockBy號	通過使用跟踪器執行由數字指定的塊中的所有事務返回跟踪結果（需要跟踪模式）。	
	偵錯追蹤 (Call)	在指定區塊執行的內容中執行 eth 呼叫，傳回可能的追蹤結果數目 (需要追蹤模式)。	
	除錯追蹤交易	傳回指定交易的所有追蹤 (需要追蹤模式)。	
淨	網版	返回當前網絡 ID。	
追蹤	追蹤區塊	返回包含在塊中的所有事務的所有調用操作碼的完整堆棧跟踪。	
	跟踪調用	在指定區塊執行的內容中執行 eth 呼叫，傳回可能的追蹤結果數目 (需要追蹤模式)。	
	追蹤交易	傳回指定交易的所有追蹤 (需要追蹤模式)。	
德克薩斯池	異常池內容	傳回所有擱置中和佇列中的交易。	

類別	JS-RPC	描述	考量事項
	流通池狀態	提供目前擱置中包含在下一個區塊中的所有交易計數，以及排入佇列 (僅排程供 future 執行) 的交易計數。	
Web	Web3_ 客戶端版	返回當前客戶端版本。	

Amazon Managed Blockchain (AMB) 存取多邊形的多邊形使用案例

多邊形區塊鏈通常用於構建與 NFT，Web3 遊戲和令牌化用例相關的去中心化應用程序（DApps）。本主題提供您可以使用 Amazon Managed Blockchain (AMB) 存取多邊形實作的一些使用案例清單。

主題

分析多邊形 NFT 資料

您可以收集有關 Polygon NFT 的資料，包括指定期間內的傳輸事件和 NFT 中繼資料等資訊。然後，您可以分析此資料，以獲得深入分析，例如哪些 NFT 正在趨勢分析，或者哪些使用者最常與特定集合互動。

如需詳細資訊，請參閱 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC。

Support NFT 購買

您可以使用 AMB Access Polygon 使用初始鑄幣，允許列表或二級市場提交交易以進行 NFT 購買。然後，結合其他 AWS 服務，您可以允許使用信用卡進行購買，接受菲亞特或加密貨幣，並為所有涉及的利益相關者快速結算。

如需詳細資訊，請參閱 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC。

創建一個多邊形錢包

您可以使用 AMB Access Polygon 來服務數字資產錢包的關鍵功能，例如從區塊鏈上的智能合約中讀取用戶令牌餘額或將簽名的交易廣播到區塊鏈。

如需詳細資訊，請參閱 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC。

錢包即服務

您可以使用 AMB Access Polygon 開發支持常見錢包交易 wallet-as-a-service 所需的操作，例如使用支持的 Polygon JSON-RPC 檢查餘額，資產轉移，資產發送和費用估算。

如需詳細資訊，請參閱 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC。

令牌門控體驗

您可以使用 AMB 訪問多邊形為用戶構建令牌門控體驗。例如，您可以有條件地僅向特定 NFT 的擁有者提供對某個內容的存取權。為此，您必須閱讀區塊鏈以確定用戶地址的 NFT 所有權。

如需更多詳細資訊，請參閱 受管理的區塊鏈 API 和支持 AMB 訪問多邊形的 JSON-RPC。

Amazon Managed Blockchain（AMB）訪問多邊形的教程

本節中突出顯示的以下教程是社區文章，其中提供了逐步解 AWS re:Post 說，以幫助您學習如何使用 AMB Access Polygon 在 Polygon 區塊鏈上執行一些常見任務。

- 使用 AMB 存取多邊形和 web3.js 傳送交易
- 使用 AMB 接入多邊形和安全帽點火部署智能合約
- 與智能合約交互
- 使用 AMB Access 多邊形和鏈鏈數據源檢索當前鏈下價格數據
- 使用 AMB 訪問分析多邊形主網上的 ERC-20 令牌數據

Amazon Managed Blockchain（AMB）訪問多邊形中的安全性

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 與您之間共同承擔的責任。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) 存取多邊形的合規計劃，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。

本文檔可幫助您了解如何在使用 AMB 訪問多邊形時應用共享責任模型。下列主題說明如何設定 AMB 存取多邊形，以符合您的安全性和合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監視和保護您的 AMB Access Polygon 資源。

主題

- Amazon Managed Blockchain (AMB) 存取多邊形中的資料保護
- 亞馬遜託管區塊鏈（AMB）的身份和訪問管理多邊形

Amazon Managed Blockchain (AMB) 存取多邊形中的資料保護

AWS 共同責任模型適用於 Amazon Managed Blockchain (AMB) 存取多邊形中的資料保護。如此模型中所述， AWS 負責保護執行所有 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，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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 資源進行通訊。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。
- 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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) 140-2 概觀。

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。這包括當您使用控制台，API 或 AWS SDK AWS 服務 使用 AMB 訪問多邊形或其他方式時。 AWS CLI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 連接來加密從運行到 AWS 服務端點的客戶端計算機傳輸的所有數據。 AWS CLI

您不須採取任何行動即可啟用 HTTPS/TLS。除非您使用該命令為單個 AWS CLI 命令明確禁用它，否則它始終處於啟用`--no-verify-ssl`狀態。

亞馬遜託管區塊鏈（AMB）的身份和訪問管理多邊形

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 AMB Access Polygon 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

根據您在 AMB 存取多邊形中所做的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 AMB Access Polygon 服務來完成工作，則管理員會為您提供所需的認證和權限。當您使用更多 AMB 存取多邊形圖徵來完成工作時，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。如果您無法存取 AMB 存取多邊形中的圖徵，請參閱疑難排解 Amazon Managed Blockchain (AMB) 存取多邊形身分和存取。

服務管理員 — 如果您負責公司的 AMB 訪問多邊形資源，則可能擁有對 AMB 訪問多邊形的完全訪問權限。確定您的服務使用者應該存取哪些 AMB Access 多邊形功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何將 IAM 與 AMB 存取多邊形搭配使用，請參閱亞馬遜託管區塊鏈（AMB）訪問多邊形如何與 IAM 配合使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 AMB 存取多邊形的存取權限的詳細資訊。若要檢視可在 IAM 中使用的範例 AMB 存取多邊形以身分識別為基礎的政策，請參閱。Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

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。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 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。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可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。如需這些任務的完整清單，了解需以根使用者登入的任務，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

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，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，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。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 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

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。如需進一步了解，請參閱IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 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。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 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）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (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 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。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 服務服務。

- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請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該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 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。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

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。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

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 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理

的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 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。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。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 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。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 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 使用者指南中的工作階段政策。

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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

亞馬遜託管區塊鏈（AMB）訪問多邊形如何與 IAM 配合使用

在您使用 IAM 管理 AMB 存取多邊形的存取權限之前，請先了解哪些 IAM 功能可與 AMB 存取多邊形搭配使用。

您可以搭配 Amazon Managed Blockchain (AMB) 存取多邊形使用的 IAM 功能

IAM 功能	AMB 存取多邊形支援
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

若要取得 AMB 存取多邊形和其他 AWS 服務 如何使用大多數 IAM 功能的高階檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

AMB 存取多邊形的身分型原則

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。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。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 存取多邊形的基於身分識別的原則範例

若要檢視 AMB 存取多邊形身分型原則的範例，請參閱。Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例

AMB 存取多邊形中以資源為基礎的政策

支援以資源基礎的政策	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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。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 使用者指南中的 IAM 中的跨帳戶資源存取。

AMB 存取多邊形的原則動作

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哪些內容。也就是說，哪個主體在什麼条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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。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 存取多邊形動作清單，請參閱服務授權參考中的 Amazon 受管區塊鏈 (AMB) 存取多邊形定義的動作。

AMB 存取多邊形中的原則動作會在動作前使用下列前置詞：

```
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 `InvokeRpcPolygon` 文字的所有動作，請包含以下動作：

```
"Action": "managedblockchain::InvokeRpcPolygon*"
```

若要檢視 AMB 存取多邊形身分型原則的範例，請參閱。Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例

AMB 存取多邊形的政策資源

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哪些內容。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。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。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 存取多邊形資源類型及其 ARN 的清單，請參閱服務授權參考中的 Amazon 受管區塊鏈 (AMB) 存取多邊形定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon 受管區塊鏈 (AMB) 存取多邊形定義的動作。

若要檢視 AMB 存取多邊形身分型原則的範例，請參閱。Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例

AMB 存取多邊形的原則條件金鑰

支援服務特定政策條件金鑰	否

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 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，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 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。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 AMB 存取多邊形條件金鑰清單，請參閱服務授權參考中的 Amazon Managed Blockchain (AMB) 存取多邊形的條件金鑰。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 (AMB) 存取多邊形定義的動作。

若要檢視 AMB 存取多邊形身分型原則的範例，請參閱。Amazon Managed Blockchain (AMB) 存取多邊形的身分型政策範例

AMB 存取多邊形中的 ACL

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 與 AMB 接入多邊形

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，可根據屬性來定義許可。在中 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) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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 使用者指南中的什麼是 ABAC?。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 存取多邊形使用臨時登入資料

支援臨時憑證	否

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。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。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。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 中的暫時性安全憑證。

AMB 存取多邊形的跨服務主體權限

支援轉寄存取工作階段 (FAS)	否

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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 存取多邊形的服務角色

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 服務服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 AMB 存取多邊形功能。只有當 AMB 存取多邊形提供指引時，才編輯服務角色。

AMB 存取多邊形的服務連結角色

支援服務連結角色。	否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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) 存取多邊形的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AMB 存取多邊形資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要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。

有關 AMB Access Polygon 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon Managed Blockchain (AMB) 存取多邊形的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 AMB 存取多邊形主控台
- 允許使用者檢視他們自己的許可
- 存取多邊形網路

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除 AMB Access Polygon 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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS 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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 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 存取多邊形主控台

若要存取 Amazon Managed Blockchain (AMB) 存取多邊形主控台，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檢視有關 AMB 存取多邊形資源的詳細資 AWS 帳戶料。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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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 Polygon 主控台，請同時將 AMB 存取多邊形*ConsoleAccess*或*ReadOnly* AWS 受管理的原則附加至實體。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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
        }
    ]
}
```

存取多邊形網路

> **Note**
>
> 若要存取多邊形的公用端點mainnet並mainnet進行 JSON-RPC 呼叫，您將需要具有 AMB 存取多邊形適當 IAM 許可的使用者登入資料 (AWS_ACCESS_KEY_ID和AWS_SECRET_ACCESS_KEY)。

Example 存取所有多邊形網路的 IAM 政策

此範例授予 IAM 使用者存 AWS 帳戶 取所有 Polygon 網路。

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

Example 訪問多邊形主網絡的 IAM 政策

此範例授予 IAM 使用者存 AWS 帳戶 取多邊形主網路。

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

```
    ]
}
```

疑難排解 Amazon Managed Blockchain (AMB) 存取多邊形身分和存取

使用下列資訊可協助您診斷和修正使用 AMB 存取多邊形和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 AMB 訪問多邊形中執行操作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 AMB 訪問多邊形資源

我沒有授權在 AMB 訪問多邊形中執行操作

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。

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 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞給 AMB Access Polygon。

有些 AWS 服務 允許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 使用者marymajor嘗試使用主控台在 AMB 存取多邊形中執行動作時，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 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 AMB 訪問多邊形資源

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：

- 若要瞭解 AMB 存取多邊形是否支援這些功能，請參閱亞馬遜託管區塊鏈（AMB）訪問多邊形如何與 IAM 配合使用。
- 若要了解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中的另一個您擁有 AWS 帳戶 的 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 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)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

日誌記錄 Amazon Managed Blockchain（AMB）通過使用訪問多邊形事件 AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain（AMB）訪問多邊形不支持管理事件。

Amazon Managed Blockchain 可在其上執行 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 捕獲調用管理區塊鏈的 AMB Access 多邊形端點作為數據平面事件的人員。

如果您建立已訂閱接收所需資料平面事件的正確設定追蹤，您可以接收 AMB Access Polygon 相關 CloudTrail 事件的持續傳遞至 S3 儲存貯體。使用收集的資訊 CloudTrail，您可以判斷是否向其中一個 AMB Access Polygon 端點提出要求、要求來自的 IP 位址、提出要求的時間，以及其他其他詳細資料。

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

AMB 存取多邊形資訊 CloudTrail

CloudTrail 在您創建它 AWS 帳戶 時啟用它。但是，您必須設定資料平面事件，以檢視誰呼叫 AMB 存取多邊形端點。

對於您的事件的持續記錄 AWS 帳戶，包括 AMB 訪問多邊形的事件，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔傳遞至 S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分割區中所有受支援區域的事件，並將日誌檔傳送到您指定的 S3 儲存貯體。此外，您還可以設定 other AWS 服務 以進一步分析並對 CloudTrail 記錄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 於跟踪多邊形 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 日誌文件和從多個帳戶接收 CloudTrail 日誌文件

透過分析資 CloudTrail 料事件，您可以監視呼叫 AMB 存取多邊形端點的使用者。

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：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由另一個人提出 AWS 服務

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

瞭解 AMB 存取多邊形記錄檔項目

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 Polygon 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 於跟踪多邊形 JSON-RPC

您可以使用 CloudTrail 來追蹤帳戶中呼叫 AMB 存取多邊形端點的使用者，以及叫用哪些 JSON-RPC 做為資料事件。根據預設，當您建立追蹤時，不會記錄資料事件。若要記錄呼叫 AMB Access Polygon 端點作為資 CloudTrail 料事件的使用者，您必須明確地將要收集活動的支援資源或資源類型新增至追蹤。AMB 存取多邊形支援使用 AWS Management Console、 AWS CLI和 SDK 新增資料事件。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

若要記錄追蹤中的資料事件，請在建立追蹤後使用放置事件選取器作業。使用`--advanced-event-selectors`此選項可指定`AWS::ManagedBlockchain::Network`資源類型，以便開始記錄資料事件，以判斷呼叫 AMB Access Polygon 端點的人員。

Example 您帳戶所有 AMB 存取多邊形端點要求的資料事件記錄項目

下列範例示範如何使用此`put-event-selectors`作業記錄您帳戶的所有 AMB Access Polygon 端點要求，以便在`us-east-1`區域`my-polygon-trail`中追蹤。

```
aws cloudtrail put-event-selectors \

--region us-east-1 \
--trail-name my-polygon-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。您可以判斷是否對其中一個 AMB 存取多邊形端點、要求來自的 IP 位址、提出要求的時間和其他其他詳細資料發出 Polygon JSON-RPC 要求。下列範例中的某些值基於安全性考量而被模糊化，但完全出現在實際的記錄項目中。

```
{
        "eventVersion": "1.09",
        "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": "gettxout",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "111.222.333.444",
        "userAgent": "python-requests/2.28.1",
        "errorCode": "-",
        "errorMessage": "-",
        "requestParameters": {
            "jsonrpc": "2.0",
            "method": "gettxout",
            "params": [],
            "id": 1
        },
        "responseElements": null,
        "requestID": "DRznHHEj********",
        "eventID": "baeb232d-2c6b-46cd-992c-0e40********",
```

```
        "readOnly": true,
        "resources": [{
            "type": "AWS::ManagedBlockchain::Network",
            "ARN": "arn:aws:managedblockchain:::networks/n-polygon-mainnet"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data"
}
```

AMB 存取多邊形使用者指南的文件歷程

下表說明 AMB 存取多邊形的文件版本。

變更	描述	日期
更新了 JSON-RPC 的配額	AMB 存取多邊形支援每個支援的 JSON-RPC 的配額已更新。	2024年4月12日
終止對孟買測試網絡的支持	AMB 訪問多邊形在 2024 年 4 月 15 日結束了孟買測試網的支持。	2024年4月10日
自學課程主題的新增	AMB 存取 AWS RE: POST 的「社群文章」區段中的多邊形教學課程。	2024年4月9日
公開預覽	Amazon Managed Blockchain（AMB）訪問多邊形服務的公開預覽版。	2023年11月24日