aws

Guida per gli sviluppatori

Poligono di accesso AMB

Poligono di accesso AMB: Guida per gli sviluppatori

Table of Contents

Amazon Managed Blockchain (AMB) Access Polygon è in versione di anteprima ed è soggetto a modifiche.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.

Cos'è Amazon Managed Blockchain (AMB) Access Polygon?

Amazon Managed Blockchain (AMB) Access Polygon è un servizio completamente gestito che ti aiuta a creare applicazioni Web3 resilienti sulla blockchain Polygon. AMB Access Polygon fornisce un accesso istantaneo e senza server alla blockchain Polygon.

Polygon è una soluzione di scalabilità che utilizza la Ethereum Virtual Machine (EVM) come base. La blockchain Polygon è nota per l'elevato throughput delle transazioni e le basse commissioni di transazione. La blockchain Polygon utilizza un meccanismo di consenso. proof-of-stake Polygon è comunemente usato nella creazione di applicazioni decentralizzate (DApp) relative, tra gli altri NFTs, ai giochi Web3 e ai casi d'uso della tokenizzazione.

Questa guida spiega come creare e gestire le risorse blockchain Polygon utilizzando Amazon Managed Blockchain (AMB) Access Polygon.

Risorse per gli utenti alle prime armi di AMB Access Polygon

Se è la prima volta che utilizzi AMB Access Polygon, ti consigliamo di iniziare leggendo le seguenti sezioni:

- Concetti chiave: Amazon Managed Blockchain (AMB) Access Polygon
- Guida introduttiva ad Amazon Managed Blockchain (AMB) Access Polygon
- API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon

Concetti chiave: Amazon Managed Blockchain (AMB) Access Polygon

> **Note**
>
> Questa guida presuppone che tu abbia familiarità con i concetti essenziali per Polygon. Questi concetti includono staking, dApp, transazioni, portafogli, contratti intelligenti, Polygon (POL, ex MATIC) e altri. Prima di utilizzare Amazon Managed Blockchain (AMB) Access Polygon, ti consigliamo di consultare la documentazione sullo sviluppo di Polygon e il wiki Polygon.

Amazon Managed Blockchain (AMB) Access Polygon ti offre l'accesso senza server alle reti Polygon Mainnet e Polygon Mainnet, senza richiedere il provisioning e la gestione di alcuna infrastruttura Polygon, inclusi i nodi. I nodi Polygon su una rete archiviano collettivamente lo stato di una blockchain Polygon, verificano le transazioni e partecipano al consenso per modificare lo stato della blockchain. Puoi utilizzare questo servizio gestito per accedere alle reti Polygon in modo rapido e su richiesta, riducendo il costo complessivo di proprietà.

Con AMB Access Polygon, hai accesso alle chiamate JSON Remote Procedure (JSON-RPC). Puoi richiamare Polygon JSON- per comunicare con la blockchain Polygon tramite nodi gestiti RPCs da Managed Blockchain. Puoi utilizzare il servizio AMB Access Polygon per sviluppare e utilizzare applicazioni decentralizzate (DApp) che interagiscono con la blockchain Polygon. Parte integrante delle dApp sono i contratti intelligenti. Puoi creare e distribuire contratti intelligenti nella blockchain Polygon utilizzando AMB Access Polygon. Puoi anche controllare i saldi dei tuoi portafogli, i dettagli delle transazioni, le commissioni stimate e così via, invocando JSON- RPCs rispetto agli endpoint AMB Access Polygon che funzionano in modo decentralizzato su tutti i nodi che sono peer della rete Polygon. Qualsiasi peer della rete Polygon può sviluppare e implementare un contratto intelligente.

> **Important**
>
> Sei responsabile della creazione, del mantenimento, dell'utilizzo e della gestione dei tuoi indirizzi Polygon. Sei anche responsabile del contenuto dei tuoi indirizzi Polygon. AWS non è responsabile per eventuali transazioni distribuite o richiamate utilizzando nodi Polygon su Amazon Managed Blockchain.

Considerazioni e limitazioni per l'utilizzo di Amazon Managed Blockchain (AMB) Access Polygon

Quando usi Amazon Managed Blockchain (AMB) Access Polygon, considera quanto segue:

- Reti Polygon supportate

  AMB Access Polygon supporta le seguenti reti pubbliche:

  - Mainnet: la blockchain pubblica Polygon protetta dal proof-of-stake consenso e sulla quale viene emesso e negoziato il token Polygon (POL). Le transazioni su Mainnet hanno un valore effettivo (ovvero comportano costi reali) e vengono registrate sulla blockchain pubblica.

- Reti non più supportate da Polygon

  - Come comunicato da Polygon Labs, la rete Mumbai Testnet tramonterà a metà aprile. In linea con questa notizia, AMB Access Polygon ha interrotto il supporto di Mumbai Testnet il 15 aprile 2024. Ti consigliamo di utilizzare Amoy Testnet per il tuo carico di lavoro di test.
  - Le reti private non sono supportate.
  - Inoltre, AMB Access Polygon non include il supporto per la rete Polygon zKEVM.

- Compatibilità con le più diffuse librerie di programmazione di terze parti

  AMB Access Polygon è compatibile con le librerie di programmazione più diffuse, come ethers.js, e consente agli sviluppatori di interagire con la blockchain Polygon utilizzando strumenti familiari per integrarsi facilmente con le implementazioni esistenti o sviluppare rapidamente nuove applicazioni.

- Regioni supportate

  Questo servizio è supportato solo nella regione Stati Uniti orientali (Virginia settentrionale).

- Service endpoints (Endpoint del servizio)

  Di seguito sono riportati gli endpoint del servizio per AMB Access Polygon. Per connettersi al servizio, è necessario utilizzare un endpoint che includa una delle regioni supportate.

  - `mainnet.polygon.managedblockchain.us-east-1.amazonaws.com`

- Lo staking non è supportato

  AMB Access Polygon non supporta i nodi di validazione Polygon (POL) per. proof-of-stake

- Firma in versione 4 delle richieste Polygon JSON-RPC

Quando effettui chiamate a Polygon JSON- RPCs su Amazon Managed Blockchain, puoi farlo tramite una connessione HTTPS autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono effettuare chiamate Polygon JSON-RPC. Per fare ciò, è necessario fornire AWS delle credenziali (un ID della chiave di accesso e una chiave di accesso segreta) con la chiamata.

> **Important**
>
> - Non incorporate le credenziali del client nelle applicazioni rivolte agli utenti.
> - Non è possibile utilizzare le policy IAM per limitare l'accesso ai singoli Polygon JSON-. RPCs

- Support per l'accesso basato su token

  Puoi anche utilizzare i token Accessor per effettuare chiamate JSON-RPC agli endpoint della rete Polygon come comoda alternativa al processo di firma Signature Version 4 (SigV4). È necessario fornire un elemento `BILLING_TOKEN` da uno dei token Accessor creati e aggiunti come parametro nelle chiamate.

  > **Important**
  >
  > - Se dai priorità alla sicurezza e alla verificabilità rispetto alla praticità, utilizza invece il processo di firma SigV4.
  > - Puoi accedere a Polygon JSON RPCs utilizzando Signature Version 4 (SigV4) e l'accesso basato su token. Tuttavia, se scegli di utilizzare entrambi i protocolli, la tua richiesta viene rifiutata.
  > - Non è mai necessario incorporare i token Accessor nelle applicazioni rivolte agli utenti.

- Sono supportati solo gli invii di transazioni non elaborate

  Utilizza `eth_sendrawtransaction` JSON-RPC per inviare transazioni che aggiornano lo stato della blockchain Polygon.

Configurazione di Amazon Managed Blockchain (AMB) Access Polygon

Prima di utilizzare Amazon Managed Blockchain (AMB) Access Polygon per la prima volta, segui i passaggi in questa sezione per creare un. Account AWS Il capitolo seguente illustra come iniziare a utilizzare AMB Access Polygon.

Prerequisiti per l'utilizzo di AMB Access Polygon

Prima di utilizzarlo AWS per la prima volta, è necessario disporre di un. Account AWS

Iscriviti per AWS

Quando ti registri AWS, il tuo Account AWS viene automaticamente registrato per tutti Servizi AWS, incluso Amazon Managed Blockchain (AMB) Access Polygon. Ti vengono addebitati solo i servizi che utilizzi.

Se ne hai Account AWS già uno, vai al passaggio successivo. Se non disponi di un Account AWS, utilizza la seguente procedura per crearne uno.

Per creare un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Crea un utente IAM con le autorizzazioni appropriate

Per creare e lavorare con AMB Access Polygon, devi disporre di un principale AWS Identity and Access Management (IAM) (utente o gruppo) con le autorizzazioni che consentano le azioni Managed Blockchain necessarie.

Quando effettui chiamate a Polygon JSON- RPCs su Amazon Managed Blockchain, puoi farlo tramite una connessione HTTPS autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono effettuare chiamate Polygon JSON-RPC. Per fare ciò, è necessario fornire AWS delle credenziali (un ID della chiave di accesso e una chiave di accesso segreta) con la chiamata.

Puoi anche utilizzare i token Accessor per effettuare chiamate JSON-RPC agli endpoint della rete Polygon come comoda alternativa al processo di firma Signature Version 4 (SigV4). È necessario fornire un elemento `BILLING_TOKEN` da uno dei token Accessor creati e aggiunti come parametro con le chiamate. Tuttavia, è comunque necessario l'accesso IAM per ottenere le autorizzazioni per creare token Accessor utilizzando l' Console di gestione AWS SDK, e. AWS CLI

Per informazioni su come creare un utente IAM, consulta Creazione di un utente IAM nel tuo account. AWS Per ulteriori informazioni su come allegare una politica di autorizzazioni a un utente, consulta Modifica delle autorizzazioni per un utente IAM. Per un esempio di politica di autorizzazioni che puoi utilizzare per concedere a un utente il permesso di lavorare con AMB Access Polygon, vedi. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

Installa e configura il AWS Command Line Interface

Se non l'hai ancora fatto, installa il file latest AWS Command Line Interface (AWS CLI) per utilizzare le AWS risorse di un terminale. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.

> **Note**
>
> Per l'accesso alla CLI, sono necessari un ID chiave di accesso e una chiave di accesso segreta. Utilizza credenziali temporanee al posto delle chiavi di accesso a lungo termine quando possibile. Le credenziali temporanee includono un ID della chiave di accesso, una chiave di accesso segreta e un token di sicurezza che ne indica la scadenza. Per ulteriori informazioni, consulta Using temporary credenziali with AWS resources nella IAM User Guide.

Guida introduttiva ad Amazon Managed Blockchain (AMB) Access Polygon

Inizia a usare Amazon Managed Blockchain (AMB) Access Polygon utilizzando le informazioni e le procedure in questa sezione.

Argomenti

Crea una policy IAM per accedere alla rete blockchain Polygon

Per accedere all'endpoint pubblico della rete principale Polygon per effettuare chiamate JSON-RPC, devi disporre di credenziali utente (AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY) che disponga delle autorizzazioni IAM appropriate per Amazon Managed Blockchain (AMB) Access Polygon. In un terminale su cui è AWS CLI installato, esegui il comando seguente per creare una policy IAM per accedere a entrambi gli endpoint Polygon:

```
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**
>
> L'esempio precedente ti dà accesso a tutte le reti Polygon disponibili. Per accedere a un endpoint specifico, utilizzate il seguente comando: `Action`
>
> - `"managedblockchain:InvokeRpcPolygonMainnet"`

Dopo aver creato la policy, associala al ruolo del tuo utente IAM affinché abbia effetto. Nella Console di gestione AWS, accedi al servizio IAM e collega la policy `AmazonManagedBlockchainPolygonAccess` al ruolo assegnato al tuo utente IAM.

Effettua richieste di chiamata di procedura remota (RPC) Polygon sull'editor RPC di AMB Access utilizzando il Console di gestione AWS

È possibile modificare, configurare e inviare chiamate di procedura remota (RPCs) Console di gestione AWS utilizzando AMB Access Polygon. Con questi RPCs, puoi leggere dati e scrivere transazioni sulla rete Polygon, incluso il recupero dei dati e l'invio di transazioni alla rete Polygon.

Example

L'esempio seguente mostra come ottenere informazioni sull'ultimo blocco utilizzando RPC. `eth_getBlockByNumber` Modifica le variabili evidenziate con i tuoi input o scegli uno dei metodi RPC elencati e inserisci gli input pertinenti richiesti.

1. Apri la console Managed Blockchain all'indirizzo. https://console.aws.amazon.com/managedblockchain/
2. Scegli l'editor RPC.
3. Nella sezione Richiesta, scegli *`POLYGON_MAINNET`* come. ***`Blockchain Network`***
4. Scegli *`eth_getBlockByNumber`* come metodo RPC.
5. Inserisci **`latest`** ***`Block number`***e scegli *`False`* come flag Transazione completa.
6. Quindi, scegli Invia RPC.

7. Puoi visualizzare i risultati del `latest` blocco nella sezione Risposta. È quindi possibile copiare le transazioni non elaborate complete per ulteriori analisi o utilizzarle nella logica aziendale delle applicazioni.

Per ulteriori informazioni, consulta il RPCs supporto fornito da AMB Access Polygon

Effettua richieste JSON-RPC per AMB Access Polygon utilizzando il **`awscurl`** AWS CLI

Example

Firma le richieste con le tue credenziali utente IAM utilizzando Signature Version 4 (SigV4) per effettuare richieste Polygon JSON-RPC agli endpoint AMB Access Polygon. Lo `awscurl`strumento da riga di comando può aiutarti a firmare le richieste ai servizi che utilizzano SigV4. AWS Per ulteriori informazioni, vedere awscurl README.md.

Installa `awscurl` utilizzando il metodo appropriato per il tuo sistema operativo. Su macOS, HomeBrew è l'applicazione consigliata:

```
brew install awscurl
```

Se hai già installato e configurato AWS CLI, le tue credenziali utente IAM e quelle predefinite Regione AWS sono impostate nel tuo ambiente e hai accesso a. `awscurl` Utilizzando`awscurl`, invia una richiesta alla rete principale Polygon richiamando l'RPC. `eth_getBlockByNumber` Questa chiamata accetta un parametro di stringa corrispondente al numero di blocco per il quale si desidera recuperare le informazioni.

Il comando seguente recupera i dati del blocco dalla rete principale Polygon utilizzando il numero di blocco nell'`params`array per selezionare il blocco specifico per il quale recuperare le intestazioni.

```
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**
>
> È inoltre possibile effettuare la stessa richiesta utilizzando la funzionalità di accesso basata su token AMB Access utilizzando `curl` i token. `Accessor` Per ulteriori informazioni, consulta

Creazione e gestione di token Accessor per l'accesso basato su token per effettuare richieste AMB Access Polygon.

```
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'
```

La risposta di entrambi i comandi restituisce informazioni sul blocco più recente. Vedi l'esempio seguente a scopo illustrativo:

```
{"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":[]}}
```

Effettua richieste Polygon JSON-RPC in Node.js

È possibile richiamare Polygon JSON- RPCs inviando richieste firmate utilizzando HTTPS per accedere alla rete Polygon Mainnet utilizzando il modulo https nativo in Node.js oppure è possibile

utilizzare una libreria di terze parti come AXIOS. I seguenti esempi di Node.js mostrano come effettuare richieste Polygon JSON-RPC all'endpoint AMB Access Polygon utilizzando sia l'accesso Signature Version 4 (SigV4) che quello basato su token. Il primo esempio invia una transazione da un indirizzo a un altro e il seguente esempio richiede i dettagli della transazione e le informazioni sul saldo dalla blockchain.

Example

Per eseguire questo script Node.js di esempio, applica i seguenti prerequisiti:

1. È necessario che nel computer siano installati node version manager (nvm) e Node.js. Puoi trovare le istruzioni di installazione per il tuo sistema operativo qui.
2. Usa il `node --version` comando e conferma che stai usando la versione 18 o successiva di Node. Se necessario, puoi usare il `nvm install v18.12.0` comando, seguito dal `nvm use v18.12.0` comando, per installare la versione 18, la versione LTS di Node.
3. Le variabili `AWS_ACCESS_KEY_ID` di ambiente `AWS_SECRET_ACCESS_KEY` devono contenere le credenziali associate al tuo account.

   Esporta queste variabili come stringhe sul tuo client utilizzando i seguenti comandi. Sostituisci i valori in rosso nelle stringhe seguenti con i valori appropriati del tuo account utente IAM.

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

Dopo aver completato tutti i prerequisiti, copia i seguenti file in una directory del tuo ambiente locale utilizzando il tuo editor di codice preferito:

pacchetto.json

```
{
  "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**
>
> Il codice seguente utilizza una chiave privata codificata per generare un portafoglio utilizzato da Signer solo a `Ethers.js` scopo dimostrativo. Non utilizzate questo codice in ambienti di produzione, poiché contiene fondi reali e rappresenta un rischio per la sicurezza.
> Se necessario, contatta il team del tuo account per ricevere consigli sulle best practice relative a wallet e Signer.

```
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");
```

Una volta salvati questi file nella directory, installa le dipendenze necessarie per eseguire il codice utilizzando il seguente comando:

```
npm install
```

Inviare una transazione in Node.js

L'esempio precedente invia il token Polygon Mainnet (POL) nativo da un indirizzo all'altro firmando una transazione e trasmettendola alla rete principale Polygon utilizzando AMB Access Polygon. Per fare ciò, usa lo `sendTx.js` script, che utilizza una libreria popolare per interagire con Ethereum e blockchain compatibili con Ethereum come `Ethers.js` Polygon. È necessario sostituire tre variabili nel codice evidenziate in rosso, tra cui il token Accessor `billingToken` per l'accesso basato su token, la chiave privata con cui si firma la transazione e l'indirizzo del destinatario che riceve il POL.

> **Tip**
>
> Ti consigliamo di creare una nuova chiave privata (portafoglio) per questo scopo anziché riutilizzare un portafoglio esistente per eliminare il rischio di perdere fondi. Puoi utilizzare il metodo della classe Wallet createRandom () della libreria Ethers per generare un portafoglio con cui testare. Inoltre, se è necessario richiedere POL dalla rete principale Polygon, è possibile utilizzare il faucet POL pubblico per richiederne una piccola quantità da utilizzare per i test.

Dopo aver aggiunto al codice la `billingToken` chiave privata di un wallet finanziato e l'indirizzo del destinatario, esegui il codice seguente per firmare una transazione per inviare .0001 POL dal tuo indirizzo a un altro e trasmetterla a Polygon Mainnet richiamando il `eth_sendRawTransaction` JSON-RPC utilizzando AMB Access Polygon.

```
node sendTx.js
```

La risposta ricevuta è simile alla seguente:

```
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: []
}
```

La risposta costituisce la ricevuta della transazione. Salva il valore della proprietà`hash`. Questo è l'identificatore della transazione che hai appena inviato alla blockchain. Si utilizza questa proprietà nell'esempio di transazione di lettura per ottenere ulteriori dettagli su questa transazione dalla rete principale Polygon.

Nota che i `blockNumber` e `blockHash` sono `null` nella risposta. Questo perché la transazione non è stata ancora registrata in un blocco sulla rete Polygon. Tieni presente che questi valori vengono definiti in seguito e potresti vederli quando richiedi i dettagli della transazione nella sezione seguente.

Leggi una transazione in Node.js

In questa sezione, richiedi i dettagli della transazione per la transazione inviata in precedenza e recuperi il saldo POL per l'indirizzo del destinatario utilizzando le richieste di lettura alla rete principale Polygon utilizzando AMB Access Polygon. Nel `readTx.js` file, sostituisci la variabile etichettata *`your-transaction-id`* con quella salvata dalla risposta durante l'`hash`esecuzione del codice nella sezione precedente.

Questo codice utilizza un'utilità che firma le richieste HTTPS ad AMB Access Polygon con i moduli Signature Version 4 (SigV4) richiesti dall' AWS SDK e invia le richieste utilizzando il client HTTP ampiamente utilizzato, AXIOS. `dispatch-evm-rpc.js`

La risposta ricevuta è simile alla seguente:

```
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
```

La risposta rappresenta i dettagli della transazione. Nota che ora `blockNumber` sono probabilmente definiti gli `blockHash` e. Ciò indica che la transazione è stata registrata in un blocco. Se questi valori sono fissi`null`, attendi qualche minuto, quindi esegui nuovamente il codice per verificare se la transazione è stata inclusa in un blocco. Infine, la rappresentazione esadecimale del saldo dell'indirizzo del destinatario (0x110d9316ec000) viene convertita in decimale utilizzando il `formatEther()` metodo di Ethers, che converte l'esadecimale in decimale e sposta le posizioni decimali di 18 (10^18) per fornire il vero equilibrio in POL.

> **Tip**
>
> Sebbene gli esempi di codice precedenti illustrino come utilizzare Node.js, Ethers e Axios per utilizzare alcuni dei JSON- RPCs su AMB Access Polygon supportati, puoi modificare gli esempi e scrivere altro codice per creare le tue applicazioni su Polygon utilizzando questo servizio. Per un elenco completo dei formati JSON- supportati su AMB Access Polygon, consulta. RPCs API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon

Creazione e gestione di token Accessor per l'accesso basato su token per effettuare richieste AMB Access Polygon

Puoi anche utilizzare i token Accessor per effettuare chiamate JSON-RPC agli endpoint della rete Polygon come comoda alternativa al processo di firma Signature Version 4 (SigV4). È necessario fornire un elemento `BILLING_TOKEN` da uno dei token Accessor creati e aggiunti come parametro con le chiamate.

> **Important**
>
> - Se dai priorità alla sicurezza e alla verificabilità rispetto alla praticità, utilizza invece il processo di firma SigV4.
> - Puoi accedere a Polygon JSON, RPCs utilizzando Signature Version 4 (SigV4) e l'accesso basato su token. Tuttavia, se scegli di utilizzare entrambi i protocolli, la tua richiesta viene rifiutata.
> - Non è mai necessario incorporare i token Accessor nelle applicazioni rivolte agli utenti.

Nella console, la pagina Token Accessors mostra un elenco di tutti i token Accessor che è possibile utilizzare per effettuare chiamate JSON-RPC AMB Access Polygon dal codice from su un client. Account AWS

Per ulteriori informazioni sulle richieste JSON-RPC di AMB Access Polygon, vedere. API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon

È possibile creare e gestire i token Accessor utilizzando. Console di gestione AWS Puoi anche creare e gestire i token Accessor utilizzando le seguenti operazioni API:`CreateAccessor`,, `GetAccessor` e. `ListAccessors` `DeleteAccessor` A `BILLING_TOKEN` è una proprietà di Accessor. Questa `BILLING_TOKEN` proprietà viene utilizzata per tracciare il tuo Accessor e per fatturare le richieste JSON-RPC di AMB Access Polygon effettuate dal tuo. Account AWS

Tutte le azioni API relative alla creazione e alla gestione dei token Accessor sono disponibili anche tramite, e. Console di gestione AWS AWS CLI SDKs

Creazione di un token Accessor per l'accesso basato su token

Puoi creare un token Accessor e utilizzarlo per effettuare chiamate API AMB Access Polygon su qualsiasi nodo AMB Access Polygon del tuo. Account AWS

Crea un token Accessor per effettuare richieste AMB Access Polygon JSON-RPC utilizzando il Console di gestione AWS

1. Apri la console https://console.aws.amazon.com/managedblockchain/Managed Blockchain all'indirizzo.
2. Scegli Token Accessors.
3. Scegli Create Accessor.
4. Scegli una rete blockchain Polygon valida.
5. Facoltativo, aggiungi tag per il tuo Accessor.
6. Scegli Crea Accessor per creare un nuovo token Accessor.

Crea un token Accessor per effettuare richieste AMB Access Polygon JSON-RPC utilizzando il AWS CLI

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

Il comando precedente restituisce `AccessorId` insieme a, come illustrato nell'esempio seguente`BillingToken`.

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

L'elemento chiave della tua risposta è il`BillingToken`. È possibile utilizzare questa proprietà per effettuare chiamate JSON-RPC a AMB Access Polygon. Alcuni valori dell'esempio sono stati offuscati per motivi di sicurezza, ma appariranno completamente nelle risposte effettive.

> **Note**
>
> Dopo l'esecuzione dell'operazione, Managed Blockchain effettua il provisioning e configura il token per te. La durata di questo processo dipende da molte variabili.

Visualizzazione dei dettagli di un token Accessor

Puoi visualizzare le proprietà di ogni token Accessor che possiedi Account AWS . Ad esempio, puoi visualizzare l'Accessor ID o l'Amazon Resource Name (ARN) dell'Accessor. Puoi anche visualizzare lo stato, il tipo, la data di creazione e il. `BillingToken`

Per visualizzare le informazioni di un token Accessor utilizzando il Console di gestione AWS

1. Apri la console Managed Blockchain all'indirizzo https://console.aws.amazon.com/managedblockchain/.
2. Nel riquadro di navigazione, scegli Token Accessors.
3. Scegli l'ID di accesso del token dall'elenco.

Viene visualizzata la pagina dei dettagli del token. Da questa pagina è possibile visualizzare le proprietà del token.

Per visualizzare le informazioni di un token Accessor utilizzando il AWS CLI

Esegui il comando seguente per visualizzare i dettagli di un token Accessor. Sostituisci i valori di `--accessor-id` con il tuo ID di accesso.

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

Le `BillingToken` e altre proprietà chiave vengono restituite come illustrato nell'esempio seguente. Alcuni valori dell'esempio sono stati offuscati per motivi di sicurezza, ma appaiono completamente nelle risposte effettive.

```
{
  "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********"
  }
}
```

Eliminazione di un token Accessor

Quando si elimina un token Accessor, il token cambia dallo stato `AVAILABLE` a. `PENDING_DELETION` Non è possibile utilizzare un token Accessor con lo `PENDING_DELETION` stato.

Per eliminare un token Accessor utilizzando il Console di gestione AWS

1. Apri la console Managed Blockchain all'indirizzo https://console.aws.amazon.com/managedblockchain/.
2. Nel riquadro di navigazione, scegli Token Accessors.
3. Seleziona il token Accessor che desideri dall'elenco.
4. Scegli Elimina.
5. Conferma la tua scelta.

Verrai reindirizzato alla pagina Tokens Accessors con il token Accessor eliminato. La pagina mostra lo stato. `PENDING_DELETION`

Per eliminare un token Accessor utilizzando il AWS CLI

L'esempio seguente mostra come eliminare un token. Utilizzate il `delete-accessor` comando per eliminare un token. Imposta il valore di `--accessor-id` con il tuo ID di accesso.

Eliminazione di un token Accessor utilizzando la CLI AWS

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

Se questo comando viene eseguito correttamente, non viene restituito alcun messaggio.

API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon

Amazon Managed Blockchain fornisce operazioni API per la creazione e la gestione degli accessor di token per AMB Access Polygon. Per ulteriori informazioni, consulta la Managed Blockchain API Reference Guide.

L'argomento seguente fornisce un elenco e un riferimento del Polygon JSON, supportato da AMB Access RPCs Polygon. Ogni JSON-RPC supportato ha una breve descrizione del suo utilizzo. Si utilizza Polygon JSON- RPCs per interrogare e ottenere dati sugli smart contract, ottenere dettagli sulle transazioni, inviare transazioni e altre utilità come tracciare le transazioni e stimare le commissioni.

AMB Access Polygon supporta i seguenti metodi JSON-RPC. Ogni JSON-RPC supportato ha una categoria e una breve descrizione della sua utilità e delle sue quote di richiesta predefinite. Laddove applicabile, vengono indicate considerazioni esclusive per l'utilizzo del metodo JSON-RPC con Amazon Managed Blockchain.

Note

- Tutti i metodi che non sono elencati non sono supportati.
- Quando effettui chiamate a Polygon JSON- RPCs su Amazon Managed Blockchain, puoi farlo tramite una connessione HTTPS autenticata utilizzando il processo di firma Signature Version 4. Ciò significa che solo i principali IAM autorizzati presenti nell' AWS account possono effettuare chiamate Polygon JSON-RPC. Per fare ciò, è necessario fornire AWS delle credenziali (un ID della chiave di accesso e una chiave di accesso segreta) con la chiamata.
- È inoltre possibile utilizzare l'accesso basato su token come comoda alternativa al processo di firma Signature Version 4 (SigV4). Se dai priorità alla sicurezza e alla verificabilità rispetto alla praticità, utilizza invece il processo di firma SigV4. Tuttavia, se utilizzi sia l'accesso SigV4 che quello basato su token, le tue richieste non funzioneranno.
- Le richieste batch JSON-RPC non sono supportate su Amazon Managed Blockchain (AMB) Access Polygon per questa anteprima.

- La colonna Quotas nella tabella seguente elenca la quota per ogni JSON-RPC. Le quote sono impostate in richieste al secondo (RPS) per regione per rete Polygon (Mainnet) per ogni JSON-RPC.

  Per aumentare la tua quota, devi contattare. Supporto Per contattare Supporto, accedi a AWS Support Center Console. Scegli Crea caso. Scegli Tecnico. Scegli Managed Blockchain come servizio. Scegli Access:Polygon come categoria e Guida generale come severità. Inserisci la quota RPC come oggetto e nella casella di testo Descrizione elenca il JSON-RPC e i limiti di quota applicabili alle tue esigenze in RPS per rete Polygon per regione. Invia il tuo caso.

Categoria	JSON-RPC	Descrizione	Considerazioni
Ethereum	ETH_BlockNumber	Restituisce il numero del blocco più recente.	
	eth_call	Esegue immediatamente una nuova chiamata di messaggio senza creare una transazione sulla blockchain.	`eth_call`consuma 0 gas, ma ha un parametro di gas per i messaggi che lo richiedono.
	ETH_ChainID	Restituisce un valore intero per il valore attualmente configurato introdotto in `Chain Id` EIP-155. Restituisce `None` se non è disponibile. `Chain Id`	

Categoria	JSON-RPC	Descrizione	Considerazioni
	ETH_EstimateGas	Stima e restituisce il gas necessario per una transazione senza aggiungere la transazione alla blockchain.	
	ETH_feeHistory	Restituisce una raccolta di informazioni storiche sul gas.	
	ETH_GasPrice	Restituisce il prezzo corrente del gas in Wei.	
	ETH_GetBalance	Restituisce il saldo di un conto per l'indirizzo di account e l'identificatore di blocco specificati.	
	eth_ Hash getBlockBy	Restituisce informazioni sul blocco specificato utilizzando l'hash del blocco.	
	eth_ Numero getBlockBy	Restituisce informazioni sul blocco specificato utilizzando il numero di blocco.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_ getBlockReceipts	Restituisce le ricevute relative al blocco specifica to utilizzando il numero di blocco.	
	eth_ getBlockTransaction CountByHash	Restituisce il numero di transazioni nel blocco specificato utilizzando l'hash del blocco.	
	eth_ getBlockTransaction CountByNu mber	Restituisce il numero di transazioni nel blocco specifica to utilizzando il numero di blocco.	
	ETH_getCode	Restituisce il codice all'indir izzo dell'account e all'identificatore di blocco specificati.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	ETH_GetLogs	Restituisce un array di tutti i log per un oggetto filtro specificato.	È possibile effettuare `eth_getlogs` richieste su qualsiasi intervallo di blocchi con un intervallo di blocchi di 1.000 blocchi per impostazione predefinita quando viene fornito un indirizzo di contratto. I contratti ad alta attività possono essere limitati a intervalli di blocchi più piccoli. Se non viene fornito alcun indirizzo contrattuale, l'intervallo di blocchi sarà 8.
	eth_ getRawTransaction ByHash	Restituisce la forma grezza della transazione specificata da. `transaction_hash`	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_ getStorageAt	Restituisce il valore della posizione di archiviazione specificata per l'indirizzo di account e l'identif icatore di blocco specificati.	
	eth_ getTransactionBy BlockHash AndIndex	Restituisce informazioni su una transazione utilizzando l'hash di blocco specifica to e la posizione dell'indice delle transazioni.	
	eth_ getTransactionBy BlockNumb erAndIndex	Restituisce informazioni su una transazio ne utilizzando il numero di blocco e la posizione dell'indice della transazione specificati.	
	eth_ Hash getTransactionBy	Restituisce informazioni sulla transazio ne con l'hash della transazione specificato.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_ getTransactionCount	Restituisce il numero di transazioni inviate dall'indirizzo e dall'identificatore di blocco specificati.	
	eth_ getTransactionReceipt	Restituisce la ricezione della transazione utilizzando l'hash della transazione specificato.	
	eth_ getUncleBy BlockHashAndIndex	Restituisce informazioni sul blocco uncle specificato utilizzando l'hash del blocco e la posizione dell'indi ce uncle.	
	eth_ getUncleBy BlockNumberAndIndex	Restituisce informazioni sul blocco uncle specificato utilizzan do il numero di blocco e la posizione dell'indi ce uncle.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_ getUncleCount ByBlockHash	Restituisce il numero di conteggi nello zio specificato utilizzando l'hash uncle.	
	eth_ getUncleCount ByBlockNumber	Restituisce il numero di conteggi nello zio specifica to utilizzando il numero dello zio.	
	eth_ maxPriorityFee PerGas	Restituisce la tariffa per benzina, che è una stima di quanto puoi pagare come commissio ne prioritaria, o «mancia», per includere una transazione nel blocco corrente.	In genere si utilizza il valore restituito da questo metodo per impostare la `maxFeePer Gas` transazione successiva che si sta inviando.
	ETH_ProtocolVersion	Restituisce la versione corrente del protocollo Ethereum.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_ sendRawTransaction	Crea una nuova transazione di chiamata via messaggio o la creazione di un contratto per le transazioni firmate.	Managed Blockchain supporta solo transazioni non elaborate . È necessario creare e firmare le transazioni prima di inviarle.
Esegui il debug	debug_ traceBlockBy Hash	Restituisce il possibile numero di risultati di tracciamento eseguendo tutte le transazioni nel blocco specifica to dall'hash del blocco con un tracer (è richiesta la modalità di tracciamento).	
	numero debug_ traceBlockBy	Restituisce il risultato di tracciamento eseguendo tutte le transazioni nel blocco specificato dal numero con un tracer (è richiesta la modalità di tracciamento).	

Categoria	JSON-RPC	Descrizione	Considerazioni
	debug_traceCall	Restituisce il numero di possibili risultati di tracciame nto eseguendo una chiamata eth nel contesto dell'esecuzione del blocco specifica to (è richiesta la modalità Trace).	
	Debug_traceTransaction	Restituisce tutte le tracce di una determina ta transazio ne (è richiesta la modalità di tracciamento).	
Rete	net_version	Restituisce l'ID di rete corrente.	
Traccia	trace_block	Restituisce una traccia completa dello stack di tutti gli opcode richiamati di tutte le transazioni incluse in un blocco.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	trace_call	Restituisce il numero di possibili risultati di tracciame nto eseguendo una chiamata eth nel contesto dell'esecuzione del blocco specifica to (è richiesta la modalità di tracciamento).	
	trace_transaction	Restituisce tutte le tracce di una determina ta transazio ne (è richiesta la modalità di tracciamento).	
Pool Tx	txpool_content	Restituisce tutte le transazioni in sospeso e in coda.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	txpool_status	Fornisce un conteggio di tutte le transazioni attualmente in attesa di inclusion e nei blocchi successivi e di quelle in coda (pianificate solo per l'esecuzione futura).	
App	Web3_Client Version	Restituisce la versione corrente del client.	

Casi d'uso Polygon con Amazon Managed Blockchain (AMB) Access Polygon

La blockchain Polygon è comunemente usata nella creazione di applicazioni decentralizzate (DApp) relative, tra gli altri NFTs, ai giochi Web3 e ai casi d'uso della tokenizzazione. Questo argomento fornisce un elenco di alcuni casi d'uso che puoi implementare utilizzando Amazon Managed Blockchain (AMB) Access Polygon.

Argomenti

Analizza i dati Polygon NFT

Puoi raccogliere dati su Polygon NFTs, incluse informazioni come eventi di trasferimento e metadati NFT per un periodo specifico. Puoi quindi analizzare questi dati per ottenere informazioni quali NFTs sono di tendenza o quali utenti interagiscono più frequentemente con una determinata raccolta.

Per ulteriori informazioni, consulta API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon.

Supporta gli acquisti NFT

Puoi utilizzare AMB Access Polygon per inviare transazioni per acquisti NFT utilizzando Initial Mint, Allowlist o sul mercato secondario. Utilizzando una combinazione di altri AWS servizi, puoi quindi consentire gli acquisti utilizzando carte di credito, accettando Fiat o criptovalute, con una rapida liquidazione per tutte le parti interessate coinvolte.

Per ulteriori informazioni, consulta API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon.

Crea un portafoglio Polygon

Puoi utilizzare AMB Access Polygon per svolgere funzioni fondamentali dei portafogli di risorse digitali, come leggere i saldi dei token degli utenti dai contratti intelligenti sulla blockchain o trasmettere transazioni firmate sulla blockchain.

Per ulteriori informazioni, consulta API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon.

Il portafoglio come servizio

Puoi utilizzare AMB Access Polygon per sviluppare un sistema operativo wallet-as-a-service necessario a supportare le transazioni di portafoglio più comuni come il controllo del saldo, il trasferimento di asset, l'invio di asset e la stima delle commissioni, utilizzando il Polygon JSON-supportato. RPCs

Per ulteriori informazioni, consulta API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon.

Esperienze basate su token

Puoi utilizzare AMB Access Polygon per creare esperienze basate su token per i tuoi utenti. Ad esempio, puoi fornire in modo condizionale l'accesso a un contenuto solo ai proprietari di uno specifico NFT. A tal fine, è necessario leggere la blockchain per determinare la proprietà NFT dell'indirizzo di un utente.

Per ulteriori informazioni, consulta API Blockchain gestita e JSON, RPCs supportate con AMB Access Polygon.

Tutorial per Amazon Managed Blockchain (AMB) Access Polygon

I seguenti tutorial evidenziati in questa sezione sono articoli della community AWS re:Post che forniscono procedure dettagliate per aiutarti a imparare come eseguire alcune attività comuni sulla blockchain Polygon utilizzando AMB Access Polygon.

- Invio di transazioni utilizzando AMB Access Polygon e web3.js
- Implementa un contratto intelligente utilizzando AMB Access Polygon e Hardhat Ignition
- Interazione con un contratto intelligente
- Recupera i dati correnti sui prezzi off-chain utilizzando i feed di dati AMB Access Polygon e Chainlink
- Analizza i dati dei token ERC-20 su Polygon Mainnet con AMB Access

Sicurezza in Amazon Managed Blockchain (AMB) Access Polygon

La sicurezza del cloud ha la massima priorità AWS . In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa lo descrive sia come sicurezza del cloud che come sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per informazioni sui programmi di conformità che si applicano ad Amazon Managed Blockchain (AMB) Access Polygon, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Per fornire protezione dei dati, autenticazione e controllo degli accessi, Amazon Managed Blockchain utilizza AWS le caratteristiche e le caratteristiche del framework open source in esecuzione in Managed Blockchain.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AMB Access Polygon. I seguenti argomenti mostrano come configurare AMB Access Polygon per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse AMB Access Polygon.

Argomenti

Protezione dei dati in Amazon Managed Blockchain (AMB) Access Polygon

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in Amazon Managed Blockchain (AMB) Access Polygon. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AMB Access Polygon o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un

server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

La crittografia dei dati aiuta a impedire agli utenti non autorizzati di leggere i dati da una rete blockchain e dai sistemi di archiviazione dati associati. Ciò include i dati che potrebbero essere intercettati mentre viaggiano nella rete, noti come dati in transito.

Crittografia in transito

Per impostazione predefinita, Managed Blockchain utilizza una connessione HTTPS/TLS per crittografare tutti i dati trasmessi da un computer client che esegue gli endpoint dei due servizi. AWS CLI AWS

Non devi fare nulla per abilitare l'uso di HTTPS/TLS. È sempre abilitato a meno che non lo disabiliti esplicitamente per un singolo AWS CLI comando utilizzando il comando. `--no-verify-ssl`

Gestione delle identità e degli accessi per Amazon Managed Blockchain (AMB) Access Polygon

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse AMB Access Polygon. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Polygon)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta In che modo Amazon Managed Blockchain (AMB) Access Polygon funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

In che modo Amazon Managed Blockchain (AMB) Access Polygon funziona con IAM

Prima di utilizzare IAM per gestire l'accesso ad AMB Access Polygon, scopri quali funzionalità IAM sono disponibili per l'uso con AMB Access Polygon.

Funzionalità IAM che puoi utilizzare con Amazon Managed Blockchain (AMB) Access Polygon

Funzionalità IAM	Supporto per AMB Access Polygon
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	No
ACLs	No

Funzionalità IAM	Supporto per AMB Access Polygon
ABAC (tag nelle policy)	No
Credenziali temporanee	No
Autorizzazioni del principale	No
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come AMB Access Polygon e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, consulta i AWS servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AMB Access Polygon

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di policy basate sull'identità per AMB Access Polygon

Per visualizzare esempi di politiche basate sull'identità di AMB Access Polygon, vedere. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

Politiche basate sulle risorse all'interno di AMB Access Polygon

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per AMB Access Polygon

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni AMB Access Polygon, consulta Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon nel Service Authorization Reference.

Le azioni politiche in AMB Access Polygon utilizzano il seguente prefisso prima dell'azione:

```
managedblockchain:
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `InvokeRpcPolygon`, includi la seguente azione:

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

Per visualizzare esempi di politiche basate sull'identità di AMB Access Polygon, vedere. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

Risorse politiche per AMB Access Polygon

Supporta le risorse di policy: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse AMB Access Polygon e relativi ARNs, consulta Resources Defined by Amazon Managed Blockchain (AMB) Access Polygon nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon.

Per visualizzare esempi di politiche basate sull'identità di AMB Access Polygon, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

Chiavi relative alle condizioni delle policy per AMB Access Polygon

Supporta le chiavi di condizione delle policy specifiche del servizio: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per

visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione AMB Access Polygon, consulta Condition Keys for Amazon Managed Blockchain (AMB) Access Polygon nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon.

Per visualizzare esempi di politiche basate sull'identità di AMB Access Polygon, consulta. Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

ACLs in AMB Access Polygon

Supporti: No ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AMB Access Polygon

Supporta ABAC (tag nelle policy): No

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AMB Access Polygon

Supporta credenziali temporanee: No

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per AMB Access Polygon

Supporta l'inoltro delle sessioni di accesso (FAS): no

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AMB Access Polygon

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di AMB Access Polygon. Modifica i ruoli di servizio solo quando AMB Access Polygon fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per AMB Access Polygon

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono

visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon Managed Blockchain (AMB) Access Polygon

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse AMB Access Polygon. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da AMB Access Polygon, incluso il formato di ARNs per ogni tipo di risorsa, consulta Actions, Resources and Condition Keys for Amazon Managed Blockchain (AMB) Access Polygon nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console AMB Access Polygon
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accesso alle reti Polygon

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse AMB Access Polygon nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono

le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console AMB Access Polygon

Per accedere alla console Amazon Managed Blockchain (AMB) Access Polygon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse AMB Access Polygon presenti nel tuo. Account AWS Se crei una policy basata

sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l'API. AWS CLI AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console AMB Access Polygon, collega anche AMB Access Polygon *ConsoleAccess* o la policy gestita alle entità. *ReadOnly* AWS Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

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

Accesso alle reti Polygon

> **Note**
>
> Per accedere agli endpoint pubblici di Polygon `mainnet` ed effettuare chiamate JSON-RPC, avrai bisogno `mainnet` di credenziali utente (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) che dispongano delle autorizzazioni IAM appropriate per AMB Access Polygon.

Example Policy IAM per accedere a tutte le reti Polygon

Questo esempio concede a un utente IAM l' Account AWS accesso a tutte le reti Polygon.

JSON

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

Example Policy IAM per accedere alla rete Polygon Mainnet

Questo esempio concede a un utente IAM l' Account AWS accesso alla rete Polygon Mainnet.

JSON

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

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain (AMB) Access Polygon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AMB Access Polygon e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in AMB Access Polygon
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AMB Access Polygon

Non sono autorizzato a eseguire un'azione in AMB Access Polygon

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `managedblockchain::`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `managedblockchain::`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad AMB Access Polygon.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AMB Access Polygon. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AMB Access Polygon

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AMB Access Polygon supporta queste funzionalità, consulta. In che modo Amazon Managed Blockchain (AMB) Access Polygon funziona con IAM
- Per scoprire come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in Account AWS un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Registrazione degli eventi di Amazon Managed Blockchain (AMB) Access Polygon utilizzando AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Polygon non supporta gli eventi di gestione.

Amazon Managed Blockchain funziona su AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Managed Blockchain. CloudTrail registra chi ha richiamato gli endpoint AMB Access Polygon per Managed Blockchain come eventi del piano dati.

Se si crea un percorso correttamente configurato e sottoscritto per ricevere gli eventi del piano dati desiderati, è possibile ricevere la consegna continua degli eventi relativi ad AMB Access Polygon a un bucket S3. CloudTrail Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare se è stata effettuata una richiesta a uno degli endpoint AMB Access Polygon, l'indirizzo IP da cui proviene la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'utente.AWS CloudTrail

Informazioni su AMB Access Polygon in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando lo crei. Tuttavia, è necessario configurare gli eventi del piano dati per visualizzare chi ha richiamato gli endpoint AMB Access Polygon.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per AMB Access Polygon, crea un percorso. Un trail consente di inviare file di registro CloudTrail a un bucket S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi da tutte le regioni supportate nella AWS partizione e consegna i file di registro al bucket S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzarli ulteriormente e agire in base ai dati degli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Utilizzo CloudTrail per tracciare Polygon JSON- RPCs
- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati

- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Analizzando gli eventi CloudTrail relativi ai dati, è possibile monitorare chi ha richiamato gli endpoint AMB Access Polygon.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o (IAM) AWS Identity and Access Management
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato
- Se la richiesta è stata effettuata da un altro Servizio AWS

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro AMB Access Polygon

Per gli eventi del piano dati, un trail è una configurazione che consente la consegna di eventi come file di registro a un bucket S3 specificato. Ogni file di CloudTrail registro contiene una o più voci di registro che rappresentano una singola richiesta proveniente da qualsiasi fonte. Queste voci forniscono dettagli sull'azione richiesta, tra cui la data e l'ora dell'azione e gli eventuali parametri di richiesta associati.

> **Note**
>
> CloudTrail gli eventi di dati nei file di registro non sono una traccia stack ordinata delle chiamate API AMB Access Polygon, quindi non vengono visualizzati in un ordine specifico.

Utilizzo CloudTrail per tracciare Polygon JSON- RPCs

Puoi usarlo CloudTrail per tracciare chi nel tuo account ha richiamato gli endpoint AMB Access Polygon e quale JSON-RPC è stato richiamato come eventi relativi ai dati. Per impostazione

predefinita, quando crei un percorso, gli eventi relativi ai dati non vengono registrati. Per registrare chi ha richiamato gli endpoint AMB Access Polygon come eventi CloudTrail relativi ai dati, è necessario aggiungere in modo esplicito le risorse o i tipi di risorse supportati per i quali si desidera raccogliere attività in un percorso. AMB Access Polygon supporta l'aggiunta di eventi di dati utilizzando, e SDK. Console di gestione AWS AWS CLIPer ulteriori informazioni, consulta Registrare gli eventi utilizzando selettori avanzati nella Guida per l'utente.AWS CloudTrail

Per registrare gli eventi relativi ai dati in un percorso, utilizzate l'put-event-selectorsoperazione dopo aver creato il percorso. Utilizzate l'`--advanced-event-selectors`opzione per specificare i tipi di `AWS::ManagedBlockchain::Network` risorse per iniziare a registrare gli eventi relativi ai dati per determinare chi ha richiamato gli endpoint AMB Access Polygon.

Example Registrazione nel registro degli eventi relativi ai dati di tutte le richieste relative agli endpoint AMB Access Polygon del tuo account

L'esempio seguente mostra come utilizzare l'`put-event-selectors`operazione per registrare tutte le richieste degli endpoint AMB Access Polygon dell'account per il percorso nella regione. `my-polygon-trail` `us-east-1`

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

Dopo la sottoscrizione, puoi tenere traccia dell'utilizzo nel bucket S3 collegato al trail specificato nell'esempio precedente.

Il risultato seguente mostra una voce del registro degli eventi di CloudTrail dati con le informazioni raccolte da. CloudTrail È possibile determinare se è stata effettuata una richiesta Polygon JSON-RPC a uno degli endpoint AMB Access Polygon, l'indirizzo IP da cui proviene la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli aggiuntivi. Alcuni valori dell'esempio seguente sono stati offuscati per motivi di sicurezza, ma appaiono completamente nelle voci di registro effettive.

```
{
```

```
        "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"
}
```

Cronologia dei documenti per la AMB Access Polygon User Guide

La tabella seguente descrive le versioni della documentazione per AMB Access Polygon.

Modifica	Descrizione	Data
Quote aggiornate per JSON-RPC	Le quote supportate da AMB Access Polygon per ogni JSON-RPC supportato vengono aggiornate.	12 aprile 2024
Fine del supporto per la rete di testnet di Mumbai	AMB Access Polygon ha interrotto il supporto della testnet di Mumbai il 15 aprile 2024.	10 aprile 2024
Aggiunta dell'argomento Tutorial	Tutorial AMB Access Polygon dalla sezione Articoli della community di AWS re:POST.	9 aprile 2024
Anteprima pubblica	Versione di anteprima pubblica del servizio Amazon Managed Blockchain (AMB) Access Polygon.	24 novembre 2023