



Guida per gli sviluppatori

AMBAccedi a Polygon



AMBAccedi a Polygon: Guida per gli sviluppatori

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

.....	v
Informazioni su AMB Access Polygon	1
Risorse per gli utenti alle prime armi di AMB Access Polygon	1
Concetti chiave	2
Considerazioni e limitazioni	3
Configurazione	5
Prerequisiti per l'utilizzo di AMB Access Polygon	5
Iscriviti per AWS	5
Crea un utente IAM con le autorizzazioni appropriate	6
Installazione e configurazione dell' AWS Command Line Interface	6
Nozioni di base	7
Creazione di una policy IAM	7
Esempio di RPC per console	8
awscliEsempio RPC	9
Esempio di RPC per Node.js	10
Invia transazione	15
Leggi la transazione	17
Accesso basato su token	19
Creazione di un token Accessor per l'accesso basato su token	20
Visualizzazione dei dettagli di un token Accessor	21
Eliminazione di un token Accessor	22
JSON-RPC e API	23
Casi d'uso Polygon	35
Analizza i dati Polygon NFT	35
Supporta gli acquisti NFT	35
Crea un portafoglio Polygon	36
Il portafoglio come servizio	36
Esperienze basate su token	36
Tutorial	37
Sicurezza	38
Protezione dei dati	39
Crittografia dei dati	40
Crittografia in transito	40
Gestione dell'identità e degli accessi	40

Destinatari	41
Autenticazione con identità	41
Gestione dell'accesso con policy	45
Come funziona Amazon Managed Blockchain (AMB) Access Polygon con IAM	47
Esempi di policy basate su identità	54
Risoluzione dei problemi	59
CloudTrail registri	62
Informazioni su AMB Access Polygon in CloudTrail	62
Informazioni sulle voci dei file di registro AMB Access Polygon	63
Utilizzo CloudTrail per tracciare Polygon JSON-RPC	63
Cronologia dei documenti	66

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 a NFT, giochi Web3 e casi d'uso della tokenizzazione, tra gli altri.

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-RPC supportati 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). È possibile richiamare Polygon JSON-RPC per comunicare con la blockchain Polygon tramite nodi gestiti 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, richiamando JSON-RPC sugli 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-RPC 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'account possono effettuare chiamate Polygon JSON-RPC. AWS 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 dei client nelle applicazioni rivolte agli utenti.
- Non è possibile utilizzare le policy IAM per limitare l'accesso ai singoli JSON-RPC Polygon.

- 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-RPC 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 i servizi AWS, incluso Amazon Managed Blockchain (AMB) Access Polygon. Ti vengono addebitati solo i servizi che utilizzi.

Se ne hai un Account AWS già, 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 pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, l'utente root dell'account AWS viene creato. L'utente root dispone dell'accesso a tutte le risorse e tutti i servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso da parte dell'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-RPC 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'account possono effettuare chiamate Polygon JSON-RPC. AWS 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' AWS Management Console 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](#)

Installazione e configurazione dell' AWS Command Line Interface

Se non l'hai ancora fatto, installa l'ultima versione AWS Command Line Interface (AWS CLI) per utilizzare AWS le 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 credentials 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](#)
- [Effettua richieste di chiamata di procedura remota \(RPC\) Polygon sull'editor RPC di AMB Access utilizzando il AWS Management Console](#)
- [Effettua richieste JSON-RPC per AMB Access Polygon utilizzando il awscli AWS CLI](#)
- [Effettua richieste Polygon JSON-RPC in Node.js](#)

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_ID e AWS_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 AWS Management Console, 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 AWS Management Console

È possibile modificare, configurare e inviare chiamate di procedura remota (RPC) utilizzando AMB Access Polygon. AWS Management Console Con questi RPC, 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/](https://console.aws.amazon.com/managedblockchain/).
2. Scegli l'editor RPC.
3. Nella sezione Richiesta, scegli `POLYGON_MAINNET` come **rete Blockchain**.
4. Scegli `eth_getBlockByNumber` come metodo RPC.
5. Inserisci `latest` come **numero di blocco** 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 gli [RPC supportati 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, consulta [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'`paramsarray` 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":"0xd78301000683626f7288676f312e32312e32856c696e757800000000000000009a
  \
  423a58511085d90eaf15201a612af21ccb1e9f8350455adaba0d27eff0ecc4133e8cd255888304cc
  \
  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-RPC 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("recipient-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 seguente codice 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: 1000000000000000n,
  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.

Leggete 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'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 `fissinull`, 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-RPC supportati su AMB Access Polygon, puoi modificare gli esempi e scrivere altro codice per creare le tue applicazioni su Polygon utilizzando questo servizio. Per un elenco completo dei JSON-RPC supportati su AMB Access Polygon, consulta. [API Blockchain gestita e JSON-RPC supportati 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-RPC 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-RPC supportati con AMB Access Polygon](#)

È possibile creare e gestire i token Accessor utilizzando. AWS Management Console 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 SDK. AWS Management Console AWS CLI

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 AWS Management Console

1. [Apri la console Managed Blockchain all'indirizzo https://console.aws.amazon.com/managedblockchain/](https://console.aws.amazon.com/managedblockchain/).
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": "jZ1P80UI-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 AWS Management Console

1. Apri la console Managed Blockchain all'[indirizzo https://console.aws.amazon.com/managedblockchain/](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": "jZlP80UI-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 AWS Management Console

1. Apri la console Managed Blockchain all'[indirizzo https://console.aws.amazon.com/managedblockchain/](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-RPC supportati 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 dei Polygon JSON-RPC supportati da AMB Access Polygon. Ogni JSON-RPC supportato ha una breve descrizione del suo utilizzo. Utilizzi Polygon JSON-RPC 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-RPC 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'account possono effettuare chiamate Polygon JSON-RPC. AWS 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. AWS Support Per contattare AWS Support, 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	<u>Restituisce un valore intero per il valore attualmente configurato introdotto in Chain Id EIP-155.</u> Restituisce None se non è disponibile. Chain Id	
	ETH_EstimateGas	Stima e restituisce il gas necessario per una transazione senza	

Categoria	JSON-RPC	Descrizione	Considerazioni
		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_get Hash BlockBy	Restituisce informazioni sul blocco specificato utilizzando l'hash del blocco.	
	eth_get Numero BlockBy	Restituisce informazioni sul blocco specificato utilizzando il numero di blocco.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_getBlockReceipts	Restituisce le ricevute relative al blocco specificato utilizzando il numero di blocco.	
	eth_getBlockTransactionCountByHash	Restituisce il numero di transazioni nel blocco specificato utilizzando l'hash del blocco.	
	eth_getBlockTransactionCountByNumber	Restituisce il numero di transazioni nel blocco specificato utilizzando il numero di blocco.	
	ETH_getCode	Restituisce il codice all'indirizzo 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 <code>eth_getLogs</code> 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_getRawTransactionByHash	Restituisce la forma grezza della transazione specificata da <code>transaction_hash</code>	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_get StorageAt	Restituisce il valore della posizione di archiviazione specificata per l'indirizzo di account e l'identificatore di blocco specificati.	
	eth_get TransactionBy BlockHash AndIndex	Restituisce informazioni su una transazione utilizzando l'hash di blocco specificato e la posizione dell'indice delle transazioni.	
	eth_get TransactionBy BlockNumber AndIndex	Restituisce informazioni su una transazione utilizzando il numero di blocco e la posizione dell'indice della transazione specificati.	
	eth_get Hash TransactionBy	Restituisce informazioni sulla transazione con l'hash della transazione specificato.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_get TransactionCount	Restituisce il numero di transazioni inviate dall'indirizzo e dall'identificatore di blocco specificati.	
	eth_get TransactionReceipt	Restituisce la ricevuta della transazione utilizzando l'hash della transazione specificato.	
	eth_get UncleBy BlockHash AndIndex	Restituisce informazioni sul blocco uncle specificato utilizzando l'hash del blocco e la posizione dell'indice uncle.	
	eth_get UncleBy BlockNumber AndIndex	Restituisce informazioni sul blocco uncle specificato utilizzando il numero di blocco e la posizione dell'indice uncle.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_getHashUncleCountByBlock	Restituisce il numero di conteggi nello zio specificato utilizzando l'hash uncle.	
	eth_getNumeroUncleCountByBlock	Restituisce il numero di conteggi nello zio specificato utilizzando il numero dello zio.	
	eth_maxPriorityFeePerGas	Restituisce la tariffa per benzina, che è una stima di quanto puoi pagare come commissione prioritaria, o «mancia», per includere una transazione nel blocco corrente.	In genere si utilizza il valore restituito da questo metodo per impostare la maxFeePerGas transazione successiva che si sta inviando.
	ETH_ProtocolVersion	Restituisce la versione corrente del protocollo Ethereum.	

Categoria	JSON-RPC	Descrizione	Considerazioni
	eth_send RawTransaction	Crea una nuova transazione di chiamata tramite messaggio o una creazione di 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	Hash debug_trace BlockBy	Restituisce il possibile numero di risultati di tracciamento eseguendo tutte le transazioni nel blocco specificato dall'hash del blocco con un tracer (è richiesta la modalità di tracciamento).	
	Numero debug_trace BlockBy	Restituisce il risultato di tracciamento eseguendo tutte le transazioni nel blocco specificato dal numero con un tracciant e (è richiesta la modalità di tracciamento).	

Categoria	JSON-RPC	Descrizione	Considerazioni
	debug_traceCall	Restituisce il numero di possibili risultati di tracciamento eseguendo una chiamata eth nel contesto dell'esecuzione del blocco specificato (è richiesta la modalità Trace).	
	Debug_traceTransaction	Restituisce tutte le tracce di una determinata transazione (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 tracciamento eseguendo una chiamata eth nel contesto dell'esecuzione del blocco specificato (è richiesta la modalità Trace).	
	trace_transaction	Restituisce tutte le tracce di una determinata transazione (è richiesta la modalità di tracciamento).	
Pool Tx	txpool_content	Restituisce tutte le transazioni in sospeso e in coda.	
	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).	

Categoria	JSON-RPC	Descrizione	Considerazioni
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 a NFT, giochi Web3 e casi d'uso della tokenizzazione, tra gli altri. 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](#)
- [Supporta gli acquisti NFT](#)
- [Crea un portafoglio Polygon](#)
- [Il portafoglio come servizio](#)
- [Esperienze basate su token](#)

Analizza i dati Polygon NFT

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

Per ulteriori informazioni, consulta [API Blockchain gestita e JSON-RPC supportati 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 un regolamento rapido per tutte le parti interessate coinvolte.

Per ulteriori informazioni, consulta [API Blockchain gestita e JSON-RPC supportati 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-RPC supportati 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 i Polygon JSON-RPC supportati.

Per ulteriori informazioni, consulta [API Blockchain gestita e JSON-RPC supportati 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, devi leggere la blockchain per determinare la proprietà NFT dell'indirizzo di un utente.

Per ulteriori informazioni, consulta [API Blockchain gestita e JSON-RPC supportati 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](#)
- [Gestione delle identità e degli accessi per Amazon Managed Blockchain \(AMB\) Access Polygon](#)

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 AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o 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.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- 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 FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere [Federal Information Processing Standard \(\) 140-3. FIPS](#)

Ti consigliamo vivamente 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 AWS servizi utilizzando la console,, 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel 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 TLS connessione HTTPS/per crittografare tutti i dati trasmessi da un computer client che esegue gli endpoint dei AWS CLI due servizi. AWS

Non è necessario 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 `--no-verify-ssl` comando.

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

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

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona Amazon Managed Blockchain \(AMB\) Access Polygon con IAM](#)
- [Esempi di policy basate sull'identità per Amazon Managed Blockchain \(AMB\) Access Polygon](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain \(AMB\) Access Polygon](#)

Destinatari

Il modo in cui si usa AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AMB Access Polygon.

Utente del servizio: se utilizzi il servizio AMB Access Polygon per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di AMB Access Polygon per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in AMB Access Polygon, vedi. [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Managed Blockchain \(AMB\) Access Polygon](#)

Amministratore del servizio: se sei responsabile delle risorse di AMB Access Polygon presso la tua azienda, probabilmente hai pieno accesso ad Access Polygon. AMB È tuo compito determinare a quali funzionalità e risorse di AMB Access Polygon devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM AMB Access Polygon, consulta. [Come funziona Amazon Managed Blockchain \(AMB\) Access Polygon con IAM](#)

IAM amministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso ad AMB Access Polygon. Per visualizzare esempi di policy basate sull'identità di AMB Access Polygon che puoi utilizzare in, vedi. IAM [Esempi di policy basate sull'identità per Amazon Managed Blockchain \(\) AMB Access Polygon](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi utilizzando le tue credenziali di identità. AWS È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Firmare AWS API le richieste nella Guida per l'IAMutente](#).

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente](#) e [Utilizzo dell'autenticazione a più fattori \(MFA\) AWS nella Guida per l'IAMutente](#).

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per

informazioni su IAM Identity Center, vedi [Cos'è IAM Identity Center?](#) nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un IAM utente \(anziché un ruolo\)](#) nella Guida per l'IAMutente.

IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console [cambiando ruolo](#). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Utilizzo IAM dei ruoli](#) nella Guida per l'IAMutente.

IAMI ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni

sui ruoli per la federazione, vedere [Creazione di un ruolo per un provider di identità di terze parti](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in IAM. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente IAM](#)
- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- Sessioni di accesso inoltrato (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).
- Ruolo di servizio: un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente](#).
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un AWS servizio. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida](#) per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta [Quando creare un IAM ruolo \(anziché un utente\)](#) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy

definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scelta tra politiche gestite e politiche in linea nella Guida](#) per l'IAM utente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o AWS servizi.

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

Elenchi di controllo degli accessi () 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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità

(utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP Limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [le politiche di sessione](#) nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAM utente.

Come funziona Amazon Managed Blockchain (AMB) Access Polygon con IAM

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

IAMfunzionalità che puoi usare con Amazon Managed Blockchain (AMB) Access Polygon

IAMcaratteristica	AMBAccedi al supporto Polygon
Policy basate su identità	Si
Policy basate su risorse	No
Azioni di policy	Si
Risorse relative alle policy	No
Chiavi di condizione delle policy	No
ACLs	No
ABAC(tag nelle politiche)	No
Credenziali temporanee	No
Autorizzazioni del principale	No
● Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale del funzionamento di AMB Access Polygon e altri AWS servizi con la maggior parte delle IAM funzionalità, consulta [AWS i servizi che funzionano con IAM](#) nella Guida per l'IAMutente.

Politiche basate sull'identità per Access Polygon AMB

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un utente, un gruppo di utenti o un IAM ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il [riferimento agli elementi IAM JSON della politica](#) nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Access Polygon AMB

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 Access Polygon AMB

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti JSON politici allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione [Cross Account Resource Access IAM nella](#) Guida IAM per l'utente.

Azioni politiche per AMB Access Polygon

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'Actionelemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di 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 Access Polygon AMB

Supporta risorse politiche: No

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, 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 le caratteristiche ARN di ogni risorsa, consulta [Azioni definite da 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 Access Polygon AMB

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi 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.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica OR. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il

suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'IAMutente.

Per visualizzare un elenco delle chiavi di condizione di 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](#)

ACLsAMBin Access Polygon

Supporti ACLs: no

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

ABACcon Access Polygon AMB

Supporti ABAC (tag nelle politiche): No

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo di ABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABAC è utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, vedere [Cos'è? ABAC](#) nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazione ABAC, consulta [Utilizzare il controllo di accesso basato sugli attributi \(ABAC\)](#) nella Guida per l'IAM utente.

Utilizzo di credenziali temporanee con Access Polygon AMB

Supporta credenziali temporanee: No

Alcune AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione [AWS servizi relativa alla funzionalità IAM nella Guida](#) per l'IAM utente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta [Passare a un ruolo \(console\)](#) nella Guida per l'IAM utente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere [Credenziali di sicurezza temporanee](#) in IAM.

Autorizzazioni principali multiservizio per Access Polygon AMB

Supporta sessioni di accesso diretto (FAS): No

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

Ruoli di servizio per AMB Access Polygon

Supporta i ruoli di servizio: No

Un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente](#).

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 Access Polygon AMB

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

[Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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 Access Polygon. AMB Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempio JSON, consulta [Creazione di IAM politiche](#) nella Guida per l'IAMutente.

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 AMB le risorse Access Polygon nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche 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 ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono

utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.

- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere [Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM](#)
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta [Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.](#)

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.](#)

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 il o il. AWS CLI AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione 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 *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta [Aggiungere autorizzazioni a un utente nella Guida per l'utente. IAM](#)

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le

autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI
AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Accesso alle reti Polygon

Note

Per accedere agli endpoint pubblici di Polygon mainnet ed mainnet effettuare JSON RPC chiamate, avrai bisogno di credenziali utente

(AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY) che dispongano delle autorizzazioni appropriate per Access Polygon. IAM AMB

Example IAMPolitica di accesso a tutte le reti Polygon

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

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

Example IAMPolitica di accesso alla rete Polygon Mainnet

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

```
{
  "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 Access Polygon AMB](#)
- [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 Access Polygon AMB

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

```
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 assistenza, contatta l'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'azione `iam:PassRole`, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad AMB Access Polygon.

Alcuni AWS servizi consentono di passare 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.

L'errore di esempio seguente si verifica quando un IAM utente 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 passare 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 AWS amministratore. 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 concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AMB Access Polygon supporta queste funzionalità, consulta [Come funziona Amazon Managed Blockchain \(AMB\) Access Polygon con IAM](#)
- Per sapere come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida](#) per l'IAMutente. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.

- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM 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 AWS servizi 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-RPC](#)
- [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 AWS servizio

Per ulteriori informazioni, vedete l'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-RPC

Puoi utilizzarlo 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 esplicitamente 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. AWS Management Console AWS CLI Per ulteriori informazioni, consulta [Registrazione degli eventi utilizzando selettori avanzati](#) nella Guida per l'utente. AWS CloudTrail

Per registrare gli eventi relativi ai dati in un percorso, utilizzate l'operazione [put-event-selectors](#) dopo aver creato l'itinerario. Utilizzate l'`--advanced-event-selector` 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-selector` 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": "ARO554U062RJ7KSB7FAX: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