aws

Guia do Desenvolvedor

Polígono de acesso AMB

Polígono de acesso AMB: Guia do Desenvolvedor

Table of Contents

O Amazon Managed Blockchain (AMB) Access Polygon está em versão prévia e está sujeito a alterações.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

O que é o Amazon Managed Blockchain (AMB) Access Polygon?

O Amazon Managed Blockchain (AMB) Access Polygon é um serviço totalmente gerenciado que ajuda você a criar aplicativos Web3 resilientes no blockchain Polygon. O AMB Access Polygon fornece acesso instantâneo e sem servidor ao blockchain Polygon.

O Polygon é uma solução de escalabilidade que usa a Máquina Virtual Ethereum (EVM) como base. O blockchain Polygon é conhecido pela alta taxa de transferência de transações e baixas taxas de transação. O blockchain Polygon usa um mecanismo de proof-of-stake consenso. O Polygon é comumente usado na criação de aplicativos descentralizados (DApps) relacionados a NFTs, jogos Web3 e casos de uso de tokenização, entre outros.

Este guia aborda como criar e gerenciar recursos de blockchain Polygon usando o Amazon Managed Blockchain (AMB) Access Polygon.

Recursos para usuários iniciantes do AMB Access Polygon

Se esta é a primeira vez que você usa o AMB Access Polygon, recomendamos que você comece lendo as seguintes seções:

- Conceitos principais: Polígono de acesso ao Amazon Managed Blockchain (AMB)
- Introdução ao Amazon Managed Blockchain (AMB) Access Polygon
- API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon

Conceitos principais: Polígono de acesso ao Amazon Managed Blockchain (AMB)

> **Note**
>
> Este guia pressupõe que você esteja familiarizado com os conceitos essenciais para o Polygon. Esses conceitos incluem staking, DApps, transações, carteiras, contratos inteligentes, Polygon (POL, anteriormente MATIC) e outros. Antes de usar o Amazon Managed Blockchain (AMB) Access Polygon, recomendamos que você revise a documentação de desenvolvimento do Polygon e a wiki do Polygon.

O Amazon Managed Blockchain (AMB) Access Polygon fornece acesso sem servidor às redes Polygon Mainnet e Polygon Mainnet, sem exigir que você provisione e gerencie qualquer infraestrutura Polygon, incluindo nós. Os nós poligonais em uma rede armazenam coletivamente o estado do blockchain Polygon, verificam as transações e participam de um consenso para alterar o estado do blockchain. Você pode usar esse serviço gerenciado para acessar as redes Polygon rapidamente e sob demanda, reduzindo seu custo geral de propriedade.

Com o AMB Access Polygon, você tem acesso às chamadas de procedimento remoto JSON (JSON-RPC). Você pode invocar Polygon JSON-RPCs para se comunicar com o blockchain Polygon por meio de nós gerenciados pelo Managed Blockchain. Você pode usar o serviço AMB Access Polygon para desenvolver e usar aplicativos descentralizados (DApps) que interagem com o blockchain Polygon. Uma parte integrante dos DApps são os contratos inteligentes. Você pode criar e implantar contratos inteligentes no blockchain Polygon usando o AMB Access Polygon. Você também pode verificar os saldos de suas carteiras, detalhes da transação, taxas estimadas e assim por diante, invocando JSON-RPCs nos endpoints AMB Access Polygon que funcionam de forma descentralizada em todos os nós que são pares da rede Polygon. Qualquer parceiro da rede Polygon pode desenvolver e implantar um contrato inteligente.

> **Important**
>
> Você é responsável por criar, manter, usar e gerenciar seus endereços Polygon. Você também é responsável pelo conteúdo dos seus endereços Polygon. AWS não é responsável por nenhuma transação implantada ou chamada usando nós Polygon no Amazon Managed Blockchain.

Considerações e limitações para usar o Amazon Managed Blockchain (AMB) Access Polygon

Ao usar o Amazon Managed Blockchain (AMB) Access Polygon, considere o seguinte:

- Redes poligonais suportadas

  O AMB Access Polygon suporta as seguintes redes públicas:

  - Mainnet — A blockchain pública Polygon protegida por proof-of-stake consenso e na qual o token Polygon (POL) é emitido e transacionado. As transações na Mainnet têm valor real (ou seja, incorrem em custos reais) e são registradas na blockchain pública.

- Redes não são mais suportadas pelo Polygon

  - Conforme comunicado pelo Polygon Labs, a rede Testnet de Mumbai será encerrada em meados de abril. De acordo com essa notícia, o AMB Access Polygon encerrou o suporte do Mumbai Testnet em 15 de abril de 2024. Recomendamos usar o Amoy Testnet para sua carga de trabalho de teste.
  - Não há suporte para redes privadas.
  - Além disso, o AMB Access Polygon não inclui suporte para a rede Polygon zKEvm.

- Compatibilidade com bibliotecas populares de programação de terceiros

  O AMB Access Polygon é compatível com bibliotecas de programação populares, como ethers.js, permitindo que os desenvolvedores interajam com o blockchain Polygon usando ferramentas familiares para se integrarem facilmente às implementações existentes ou desenvolverem novos aplicativos rapidamente.

- Supported Regions (Regiões compatíveis)

  Esse serviço é suportado somente na região Leste dos EUA (Norte da Virgínia).

- Service endpoints (Endpoints de serviço)

  A seguir estão os endpoints de serviço do AMB Access Polygon. Para se conectar ao serviço, você deve usar um endpoint que inclua uma das regiões suportadas.

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

- Estaqueamento não suportado

  O AMB Access Polygon não suporta nós validadores Polygon (POL) para. proof-of-stake

- Assinatura Versão 4: assinatura de solicitações Polygon JSON-RPC

  Ao fazer chamadas para o Polygon JSON-RPCs no Amazon Managed Blockchain, você pode fazer isso por meio de uma conexão HTTPS autenticada usando o processo de assinatura Signature Version 4. Isso significa que somente diretores autorizados do IAM na AWS conta podem fazer chamadas Polygon JSON-RPC. Para fazer isso, AWS as credenciais (uma ID da chave de acesso e uma chave de acesso secreta) devem ser fornecidas com a chamada.

  > ⚠ Important
  >
  > - Não incorpore credenciais do cliente em aplicativos voltados para o usuário.
  > - Você não pode usar políticas do IAM para restringir o acesso a JSON-RPCs individuais do Polygon.

- Support para acesso baseado em token

  Você também pode usar tokens Accessor para fazer chamadas JSON-RPC para os endpoints da rede Polygon como uma alternativa conveniente ao processo de assinatura Signature Version 4 (SigV4). Você deve fornecer `BILLING_TOKEN` a de um dos tokens do Accessor que você cria e adiciona como parâmetro às suas chamadas.

  > ⚠ Important
  >
  > - Se você priorizar a segurança e a auditabilidade em vez da conveniência, use o processo de assinatura SigV4 em vez disso.
  > - Você pode acessar os Polygon JSON-RPCs usando o Signature Version 4 (SigV4) e o acesso baseado em token. No entanto, se você optar por usar os dois protocolos, sua solicitação será rejeitada.
  > - Você nunca deve incorporar tokens de acesso em aplicativos voltados para o usuário.

- Somente envios de transações brutas são aceitos

  Use o `eth_sendrawtransaction` JSON-RPC para enviar transações que atualizam o estado do blockchain Polygon.

Configurando o polígono de acesso do Amazon Managed Blockchain (AMB)

Antes de usar o Amazon Managed Blockchain (AMB) Access Polygon pela primeira vez, siga as etapas nesta seção para criar um. Conta da AWS O capítulo a seguir discute como começar a usar o AMB Access Polygon.

Pré-requisitos para usar o AMB Access Polygon

Antes de usar AWS pela primeira vez, você deve ter um Conta da AWS.

Inscreva-se para AWS

Quando você se inscreve AWS, você Conta da AWS é automaticamente inscrito em todos Serviços da AWS, incluindo o Amazon Managed Blockchain (AMB) Access Polygon. Você será cobrado apenas pelos serviços que usar.

Se você Conta da AWS já tem um, vá para a próxima etapa. Se você não tem uma Conta da AWS, siga o procedimento abaixo para criar uma.

Para criar um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Crie um usuário do IAM com as permissões apropriadas

Para criar e trabalhar com o AMB Access Polygon, você deve ter um diretor AWS Identity and Access Management (IAM) (usuário ou grupo) com permissões que permitam as ações necessárias do Managed Blockchain.

Ao fazer chamadas para o Polygon JSON-RPCs no Amazon Managed Blockchain, você pode fazer isso por meio de uma conexão HTTPS autenticada usando o processo de assinatura Signature Version 4. Isso significa que somente diretores autorizados do IAM na AWS conta podem fazer chamadas Polygon JSON-RPC. Para fazer isso, AWS as credenciais (uma ID da chave de acesso e uma chave de acesso secreta) devem ser fornecidas com a chamada.

Você também pode usar tokens Accessor para fazer chamadas JSON-RPC para os endpoints da rede Polygon como uma alternativa conveniente ao processo de assinatura Signature Version 4 (SigV4). Você deve fornecer `BILLING_TOKEN` a de um dos tokens do Accessor que você cria e adiciona como parâmetro às suas chamadas. No entanto, você ainda precisa ter acesso ao IAM para obter permissões para criar tokens de acesso usando o SDK AWS Management Console AWS CLI, e.

Para obter informações sobre como criar um usuário do IAM, consulte Como criar um usuário do IAM em sua AWS conta. Para obter mais informações sobre como anexar uma política de permissões a um usuário, consulte Alteração de permissões para um usuário do IAM. Para obter um exemplo de uma política de permissões que você pode usar para dar permissão ao usuário para trabalhar com o AMB Access Polygon, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Instalar e configurar a AWS Command Line Interface

Se você ainda não tiver feito isso, instale o latest AWS Command Line Interface (AWS CLI) para trabalhar com AWS recursos de um terminal. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.

> **Note**
>
> Para acesso à CLI, você precisa de um ID de chave de acesso e de uma chave de acesso secreta. Use credenciais temporárias em vez de chaves de acesso de longo prazo quando possível. As credenciais temporárias incluem um ID de acesso, uma chave de acesso secreta e um token de segurança que indica quando as credenciais expiram. Para obter

mais informações, consulte Uso de credenciais temporárias com AWS recursos no Guia do usuário do IAM.

Introdução ao Amazon Managed Blockchain (AMB) Access Polygon

Comece a usar o Amazon Managed Blockchain (AMB) Access Polygon usando as informações e os procedimentos desta seção.

Tópicos

Crie uma política do IAM para acessar a rede blockchain Polygon

Para acessar o endpoint público da Polygon Mainnet para fazer chamadas JSON-RPC, você deve ter credenciais de usuário (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) que tenham as permissões apropriadas do IAM para o Amazon Managed Blockchain (AMB) Access Polygon. Em um terminal com o AWS CLI instalado, execute o comando a seguir para criar uma política do IAM para acessar os dois endpoints do 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**
>
> O exemplo anterior fornece acesso a todas as redes Polygon disponíveis. Para obter acesso a um endpoint específico, use o seguinte `Action` comando:
>
> - `"managedblockchain:InvokeRpcPolygonMainnet"`

Depois de criar a política, anexe essa política à função de usuário do IAM para que ela entre em vigor. No AWS Management Console, navegue até o serviço do IAM e anexe a política `AmazonManagedBlockchainPolygonAccess` à função atribuída ao seu usuário do IAM.

Faça solicitações de chamada de procedimento remoto (RPC) do Polygon no editor RPC do AMB Access usando o AWS Management Console

Você pode editar, configurar e enviar chamadas de procedimento remoto (RPCs) AWS Management Console usando o AMB Access Polygon. Com esses RPCs, você pode ler dados e gravar transações na rede Polygon, incluindo a recuperação de dados e o envio de transações para a rede Polygon.

Example

O exemplo a seguir mostra como obter informações sobre o bloco mais recente usando o `eth_getBlockByNumber` RPC. Altere as variáveis destacadas para suas próprias entradas ou escolha um dos métodos RPC listados e insira as entradas relevantes necessárias.

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. Escolha o editor RPC.
3. Na seção Solicitação, escolha *`POLYGON_MAINNET`* como ***`Rede Blockchain`***.
4. Escolha *`eth_getBlockByNumber`* como método RPC.
5. Insira **`latest`** como o ***`número do bloco`*** e escolha *`False`* como o indicador de transação completa.

6. Em seguida, escolha Enviar RPC.
7. Você obtém os resultados do `latest` bloqueio na seção Resposta. Em seguida, você pode copiar todas as transações brutas para análise posterior ou para usar na lógica de negócios de seus aplicativos.

Para obter mais informações, consulte os RPCs compatíveis com o AMB Access Polygon

Faça solicitações JSON-RPC do AMB Access Polygon usando o **`awscurl`**AWS CLI

Example

Assine solicitações com suas credenciais de usuário do IAM usando o Signature Version 4 (SigV4) para fazer solicitações Polygon JSON-RPC aos endpoints AMB Access Polygon. A ferramenta de linha de `awscurl`comando pode ajudá-lo a assinar solicitações para AWS serviços usando o SigV4. Para obter mais informações, consulte o awscurl README.md.

Instale `awscurl` usando o método apropriado ao seu sistema operacional. No macOS, HomeBrew é o aplicativo recomendado:

```
brew install awscurl
```

Se você já instalou e configurou o AWS CLI, suas credenciais de usuário do IAM e o padrão Região da AWS estão definidos em seu ambiente e você tem acesso a. `awscurl` Usando`awscurl`, envie uma solicitação para a Polygon Mainnet invocando a RPC. `eth_getBlockByNumber` Essa chamada aceita um parâmetro de string correspondente ao número do bloco para o qual você deseja recuperar as informações.

O comando a seguir recupera os dados do bloco da Polygon Mainnet usando o número do bloco na `params` matriz para selecionar o bloco específico para o qual recuperar os cabeçalhos.

```
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**
>
> Você também pode fazer essa mesma solicitação usando o recurso `curl` de acesso baseado em token AMB Access usando `Accessor` tokens. Para ter mais informações, consulte Criação e gerenciamento de tokens de acesso para acesso baseado em tokens para fazer solicitações do 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'
> ```

A resposta de qualquer um dos comandos retorna informações sobre o bloco mais recente. Veja o exemplo a seguir para fins ilustrativos:

```
{"error":null,"id":"eth_getBlockByNumber-curltest","jsonrpc":"1.0",
      "result":{"baseFeePerGas":"0x873bf591e","difficulty":"0x18",
      "extraData":"0xd78301000683626f7288676f312e32312e32856c696e757800000000000000000009a
\
      423a58511085d90eaf15201a612af21ccbf1e9f8350455adaba0d27eff0ecc4133e8cd255888304cc
\
      67176a33b451277c2c3c1a6a6482d2ec25ee1573e8ba000",
      "gasLimit":"0x1c9c380","gasUsed":"0x14ca04d",
      "hash":"0x1ee390533a3abc3c8e1306cc1690a1d28d913d27b437c74c761e1a49********;",
      "nonce":"0x0000000000000000","number":"0x2f0ec4d",

 "parentHash":"0x27d47bc2c47a6d329eb8aa62c1353f60e138fb0c596e3e8e9425de163afd6dec",

 "receiptsRoot":"0x394da96025e51cc69bbe3644bc4e1302942c2a6ca6bf0cf241a5724c74c063fd",

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

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

Faça solicitações Polygon JSON-RPC em Node.js

Você pode invocar Polygon JSON-RPCs enviando solicitações assinadas usando HTTPS para acessar a rede Polygon Mainnet usando o módulo https nativo em Node.js, ou você pode usar uma biblioteca de terceiros, como a AXIOS. Os exemplos de Node.js a seguir mostram como fazer solicitações Polygon JSON-RPC para o endpoint AMB Access Polygon usando o Signature Version 4 (SigV4) e o acesso baseado em token. O primeiro exemplo envia uma transação de um endereço para outro e o exemplo a seguir solicita detalhes da transação e informações de saldo do blockchain.

Example

Para executar esse exemplo de script Node.js, aplique os seguintes pré-requisitos:

1. Você deve ter o node version manager (nvm) e o Node.js instalados em sua máquina. Você pode encontrar instruções de instalação para seu sistema operacional aqui.
2. Use o `node --version` comando e confirme se você está usando a versão 18 ou superior do Node. Se necessário, você pode usar o `nvm install v18.12.0` comando, seguido pelo `nvm use v18.12.0` comando, para instalar a versão 18, a versão LTS do Node.
3. As variáveis `AWS_ACCESS_KEY_ID` de ambiente `AWS_SECRET_ACCESS_KEY` devem conter as credenciais associadas à sua conta.

   Exporte essas variáveis como cadeias de caracteres em seu cliente usando os comandos a seguir. Substitua os valores em vermelho nas sequências de caracteres a seguir pelos valores apropriados da sua conta de usuário do IAM.

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

Depois de concluir todos os pré-requisitos, copie os seguintes arquivos em um diretório em seu ambiente local usando seu editor de código preferido:

pacote.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**
>
> O código a seguir usa uma chave privada codificada para gerar uma carteira que o Signatário usa apenas `Ethers.js` para fins de demonstração. Não use esse código em ambientes de produção, pois ele tem fundos reais e representa um risco de segurança.
> Se necessário, entre em contato com a equipe da sua conta para obter conselhos sobre as melhores práticas de carteira e signatários.

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

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

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

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

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

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

  console.log(tx);
};

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

readTx.js

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

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

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

  //make RPC request for transaction details
```

```
  let txDetails = await rpcRequest(url, getTransactionByHash);

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

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

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

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

Depois que esses arquivos forem salvos em seu diretório, instale as dependências necessárias para executar o código usando o seguinte comando:

```
npm install
```

Enviar uma transação em Node.js

O exemplo anterior envia o token nativo da Polygon Mainnet (POL) de um endereço para outro assinando uma transação e transmitindo-a para a Polygon Mainnet usando o AMB Access Polygon. Para fazer isso, use o `sendTx.js` script, que usa `Ethers.js` uma biblioteca popular para interagir com o Ethereum e blockchains compatíveis com o Ethereum, como o Polygon. Você precisa substituir três variáveis no código destacadas em vermelho, incluindo a do seu token de acesso *`billingToken`* para acesso baseado em token, a chave privada com a qual você assina a transação e o endereço do destinatário que recebe o POL.

> **Tip**
>
> Recomendamos que você crie uma nova chave privada (carteira) para essa finalidade, em vez de reutilizar uma carteira existente para eliminar o risco de perda de fundos. Você pode

usar o método createRandom () da classe Wallet da biblioteca Ethers para gerar uma carteira para testar. Além disso, se você precisar solicitar POL da Polygon Mainnet, poderá usar a torneira pública POL para solicitar uma pequena quantidade para usar no teste.

Depois de adicionar sua `billingToken` chave privada de uma carteira financiada e o endereço do destinatário ao código, você executa o código a seguir para assinar uma transação de 0,0001 POL a ser enviada do seu endereço para outro e transmiti-la para a Polygon Mainnet invocando o `eth_sendRawTransaction` JSON-RPC usando o AMB Access Polygon.

```
node sendTx.js
```

A resposta recebida de volta é semelhante à seguinte:

```
TransactionResponse {
provider: JsonRpcProvider {},
blockNumber: null,
blockHash: null,
index: undefined,
hash: '0x8d7538b4841261c5120c0a4dd66359e8ee189e7d1d34ac646a1d9923********',
type: 2,
to: '0xd2bb4f4f1BdC4CB54f715C249Fc5a991********',
from: '0xcf2C679AC6cb7de09Bf6BB6042ecCF05********',
nonce: 2,
gasLimit: 21000n,
gasPrice: undefined,
maxPriorityFeePerGas: 16569518669n,
maxFeePerGas: 16569518685n,
data: '0x',
value: 100000000000000n,
chainId: 80001n,
signature: Signature {
r: "0x1b90ad9e9e4e005904562d50e904f9db10430a18b45931c059960ede337238ee",
s: "0x7df3c930a964fd07fed4a59f60b4ee896ffc7df4ea41b0facfe82b470db448b7",
yParity: 0,
networkV: null
},
accessList: []
}
```

A resposta constitui o recibo da transação. Salve o valor da propriedade`hash`. Esse é o identificador da transação que você acabou de enviar para o blockchain. Você usa essa propriedade no exemplo de transação de leitura para obter detalhes adicionais sobre essa transação na Polygon Mainnet.

Observe que o `blockNumber` e `blockHash` está `null` na resposta. Isso porque a transação ainda não foi registrada em um bloco na rede Polygon. Observe que esses valores são definidos posteriormente e você pode vê-los ao solicitar os detalhes da transação na seção a seguir.

Leia uma transação em Node.js

Nesta seção, você solicita os detalhes da transação enviada anteriormente e recupera o saldo POL do endereço do destinatário usando solicitações de leitura para a Polygon Mainnet usando o AMB Access Polygon. No `readTx.js` arquivo, substitua a variável *`your-transaction-id`*rotulada pela `hash` que você salvou da resposta ao executar o código na seção anterior.

Esse código usa um utilitário,`dispatch-evm-rpc.js`, que assina solicitações HTTPS para o AMB Access Polygon com os módulos Signature Version 4 (SigV4) necessários do AWS SDK e envia solicitações usando o cliente HTTP amplamente usado, o AXIOS.

A resposta recebida de volta é semelhante à seguinte:

```
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
```

A resposta representa os detalhes da transação. Observe que o `blockHash` e agora provavelmente `blockNumber` está definido. Isso indica que a transação foi registrada em um bloco. Se esses valores persistiremnull, aguarde alguns minutos e execute o código novamente para verificar se sua transação foi incluída em um bloco. Por fim, a representação hexadecimal do saldo do endereço do destinatário (0x110d9316ec000) é convertida em decimal usando o *`formatEther()`* método de Ethers, que converte o hexadecimal em decimal e desloca as casas decimais em 18 (10^18) para fornecer o verdadeiro equilíbrio em POL.

> **Tip**
>
> Embora os exemplos de código anteriores ilustrem como usar Node.js, Ethers e Axios para utilizar alguns dos JSON-RPCs compatíveis no AMB Access Polygon, você pode modificar os exemplos e escrever outro código para criar seus aplicativos no Polygon usando esse serviço. Para obter uma lista completa dos JSON-RPCs compatíveis no AMB Access Polygon, consulte. API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon

Criação e gerenciamento de tokens de acesso para acesso baseado em tokens para fazer solicitações do AMB Access Polygon

Você também pode usar tokens Accessor para fazer chamadas JSON-RPC para os endpoints da rede Polygon como uma alternativa conveniente ao processo de assinatura Signature Version 4 (SigV4). Você deve fornecer `BILLING_TOKEN` a de um dos tokens do Accessor que você cria e adiciona como parâmetro às suas chamadas.

> **Important**
>
> - Se você priorizar a segurança e a auditabilidade em vez da conveniência, use o processo de assinatura SigV4 em vez disso.
> - Você pode acessar os Polygon JSON-RPCs usando o Signature Version 4 (SigV4) e o acesso baseado em token. No entanto, se você optar por usar os dois protocolos, sua solicitação será rejeitada.
> - Você nunca deve incorporar tokens de acesso em aplicativos voltados para o usuário.

No console, a página Token Accessors exibe uma lista de todos os tokens de acesso que você pode usar para fazer chamadas JSON-RPC do AMB Access Polygon a partir do seu código de origem em um cliente. Conta da AWS

Para obter mais informações sobre solicitações AMB Access Polygon JSON-RPC, consulte. API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon

Você pode criar e gerenciar tokens de acesso usando o. AWS Management Console Você também pode criar e gerenciar tokens de acesso usando as seguintes operações de API: `CreateAccessor` `GetAccessor`,`ListAccessors`, e. `DeleteAccessor` A `BILLING_TOKEN` é uma propriedade do Acessador. Essa `BILLING_TOKEN` propriedade é usada para rastrear seu Acessador e para cobrar solicitações JSON-RPC do AMB Access Polygon feitas a partir do seu. Conta da AWS

Todas as ações de API relacionadas à criação e gerenciamento de tokens do Accessor também estão disponíveis por meio dos SDKs AWS Management Console AWS CLI,, e.

Criação de um token de acesso para acesso baseado em token

Você pode criar um token de acesso e usá-lo para fazer chamadas à API AMB Access Polygon em qualquer nó do AMB Access Polygon em seu. Conta da AWS

Crie um token de acesso para fazer solicitações JSON-RPC do AMB Access Polygon usando o AWS Management Console

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. Escolha Token Accessors.
3. Escolha Criar acessador.
4. Escolha uma rede de blockchain Polygon válida.
5. Opcionalmente, adicione tags para seu acessador.
6. Escolha Criar acessador para criar um novo token de acesso.

Crie um token de acesso para fazer solicitações JSON-RPC do AMB Access Polygon usando o AWS CLI

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

O comando anterior retorna o `AccessorId` junto com o`BillingToken`, conforme mostrado no exemplo a seguir.

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

O elemento-chave em sua resposta é `BillingToken` o. Você pode usar essa propriedade para fazer chamadas AMB Access Polygon JSON-RPC. Alguns valores no exemplo foram ofuscados por motivos de segurança, mas aparecerão totalmente nas respostas reais.

> **Note**
>
> Depois que a operação é executada, o Managed Blockchain provisiona e configura o token para você. A duração desse processo depende de muitas variáveis.

Visualizando os detalhes de um token de acesso

Você pode ver as propriedades de cada token de acesso que você Conta da AWS possui. Por exemplo, você pode visualizar o ID do acessador ou o Amazon Resource Name (ARN) do acessador. Você também pode visualizar o status, o tipo, a data de criação e `BillingToken` o.

Para visualizar as informações de um token de acesso usando o AWS Management Console

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. No painel de navegação, escolha Token Accessors.
3. Escolha o ID do acessador do token na lista.

A página de detalhes do token é exibida. Nessa página, você pode ver as propriedades do token.

Para visualizar as informações de um token de acesso usando o AWS CLI

Execute o comando a seguir para ver os detalhes de um token de acesso. Substitua os valores `--accessor-id` de pelo seu ID de acesso.

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

As `BillingToken` e outras propriedades da chave são retornadas conforme mostrado no exemplo a seguir. Alguns valores no exemplo foram ofuscados por motivos de segurança, mas aparecem totalmente nas respostas reais.

```
{
  "Accessor": {
  "Id": "ac-NGQ6QNKXLNEBXD3UI6********",
  "Type": "BILLING_TOKEN",
  "BillingToken": "jZlP8OUI-PcQSKINyX9euJJDC5-IcW9e-n********",
```

```
  "Status": "AVAILABLE",
  "NetworkType": "POLYGON_MAINNET"
  "CreationDate": "2022-01-04T23:09:47.750Z",
  "Arn": "arn:aws:managedblockchain:us-east-1:666666666666:accessors/ac-
NGQ6QNKXLNEBXD3UI6********"
  }
}
```

Excluindo um token de acesso

Quando você exclui um token de acesso, o token muda do `PENDING_DELETION` status `AVAILABLE` para o. Você não pode usar um token de acesso com o `PENDING_DELETION` status.

Para excluir um token de acesso usando o AWS Management Console

1. Abra o console do Managed Blockchain em https://console.aws.amazon.com/managedblockchain/.
2. No painel de navegação, escolha Token Accessors.
3. Selecione o token de acesso que você deseja na lista.
4. Escolha Excluir.
5. Confirme sua escolha.

Você retornará à página de acessadores de Tokens com seu token de acessador excluído. A página exibe o `PENDING_DELETION` status.

Para excluir um token de acesso usando o AWS CLI

O exemplo a seguir mostra como excluir um token. Use o `delete-accessor` comando para excluir um token. Defina o valor de `--accessor-id` com sua ID de acesso.

Excluindo um token de acesso usando a CLI AWS

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

Se esse comando for executado com êxito, nenhuma mensagem será retornada.

API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon

O Amazon Managed Blockchain fornece operações de API para criar e gerenciar acessadores de token para o AMB Access Polygon. Para obter mais informações, consulte o Guia de referência da API Managed Blockchain.

O tópico a seguir fornece uma lista e uma referência dos Polygon JSON-RPCs que o AMB Access Polygon suporta. Cada JSON-RPC compatível tem uma breve descrição de seu uso. Você usa o Polygon JSON-RPCs para consultar e obter dados de contratos inteligentes, obter detalhes de transações, enviar transações e outros utilitários, como rastrear transações e estimar taxas.

O AMB Access Polygon oferece suporte aos seguintes métodos JSON-RPC. Cada JSON-RPC compatível tem uma categoria e uma breve descrição de seu utilitário e suas cotas de solicitação padrão. Considerações exclusivas para usar o método JSON-RPC com o Amazon Managed Blockchain são indicadas quando aplicável.

> **Note**
>
> - Não há suporte para nenhum método que não esteja listado.
> - Ao fazer chamadas para o Polygon JSON-RPCs no Amazon Managed Blockchain, você pode fazer isso por meio de uma conexão HTTPS autenticada usando o processo de assinatura Signature Version 4. Isso significa que somente diretores autorizados do IAM na AWS conta podem fazer chamadas Polygon JSON-RPC. Para fazer isso, AWS as credenciais (uma ID da chave de acesso e uma chave de acesso secreta) devem ser fornecidas com a chamada.
> - Você também pode usar o acesso baseado em token como uma alternativa conveniente ao processo de assinatura Signature Version 4 (SigV4). Se você priorizar a segurança e a auditabilidade em vez da conveniência, use o processo de assinatura SigV4 em vez disso. No entanto, se você usar o SigV4 e o acesso baseado em token, suas solicitações não funcionarão.
> - As solicitações em lote JSON-RPC não são suportadas no Amazon Managed Blockchain (AMB) Access Polygon para esta prévia.

- A coluna Cotas na tabela a seguir lista a cota para cada JSON-RPC. As cotas são definidas em solicitações por segundo (RPS) por região por rede poligonal (Mainnet) para cada JSON-RPC.

  Para aumentar sua cota, você deve entrar em contato AWS Support. Para entrar em contato AWS Support, faça login no AWS Support Center Console. Escolha Criar caso. Escolha Técnico. Escolha o Managed Blockchain como seu serviço. Escolha Access:Polygon como sua categoria e Orientação geral como sua severidade. Insira a Cota RPC como Assunto e, na caixa de texto Descrição, liste o JSON-RPC e os limites de cota aplicáveis às suas necessidades em RPS por rede poligonal por região. Envie seu caso.

Categoria	JSON-RPC	Descrição	Considerações
Ethereum	Número ETH_BLOCK	Retorna o número do bloco mais recente.	
	eth_call	Executa imediatamente uma nova chamada de mensagem sem criar uma transação no blockchain.	`eth_call`consome 0 gás, mas tem um parâmetro de gás para mensagens que precisam dele.
	ID da cadeia ETH	Retorna um valor inteiro para o `Chain Id` valor atualmente configurado que foi introduzido no EIP-155. Retorna `None` se não `Chain Id` estiver disponível.	

Categoria	JSON-RPC	Descrição	Considerações
	ETH_Estimativa de gás	Estima e retorna o gás necessário para uma transação sem adicionar a transação ao blockchain.	
	Histórico do ETH_FEE	Retorna uma coleção de informações históricas do gás.	
	Preço do ETH_GAS	Retorna o preço atual por gás em Wei.	
	ETH_GetBalance	Retorna o saldo de uma conta para o endereço da conta e o identificador de bloco especificados.	
	Hash eth_get BlockBy	Retorna informações sobre o bloco especificado usando o hash do bloco.	
	Número eth_get BlockBy	Retorna informações sobre o bloco especificado usando o número do bloco.	

Categoria	JSON-RPC	Descrição	Considerações
	eth_get BlockReceipts	Retorna recibos sobre o bloco especificado usando o número do bloco.	
	Hash eth_get BlockTransaction CountBy	Retorna o número de transações no bloco especificado usando o hash do bloco.	
	Número eth_get BlockTransaction CountBy	Retorna o número de transações no bloco especificado usando o número do bloco.	
	ETH_Obter código	Retorna o código no endereço da conta e no identific ador de bloco especificados.	

Categoria	JSON-RPC	Descrição	Considerações
	ETH_GetLogs	Retorna uma matriz de todos os registros de um objeto de filtro especificado.	Você pode fazer `eth_getloqs` solicitações em qualquer intervalo de blocos com um intervalo de blocos de 1K por padrão quando um endereço de contrato é fornecido. Contratos com alta atividade podem ser limitados a intervalos de blocos menores. Se nenhum endereço de contrato for fornecido, o intervalo de blocos será 8.
	eth_get RawTransaction ByHash	Retorna a forma bruta da transação especificada pelo`transacti on_hash` .	

Categoria	JSON-RPC	Descrição	Considerações
	eth_get StorageAt	Retorna o valor da posição de armazenamento especificada para o endereço da conta e o identificador de bloco especific ados.	
	eth_get TransactionBy BlockHash AndIndex	Retorna informaçõ es sobre uma transação usando o hash de bloco especificado e a posição do índice da transação.	
	eth_get TransactionBy BlockNumber AndIndex	Retorna informaçõ es sobre uma transação usando o número do bloco especificado e a posição do índice da transação.	
	Hash eth_get TransactionBy	Retorna informaçõ es sobre a transação com o hash de transação especificado.	

Categoria	JSON-RPC	Descrição	Considerações
	eth_get TransactionCount	Retorna o número de transaçõe s enviadas do endereço especific ado e do identific ador de bloco.	
	eth_get TransactionReceipt	Retorna o recibo da transação usando o hash de transação especific ado.	
	eth_get UncleBy BlockHash AndIndex	Retorna informaçõ es sobre o bloco tio especificado usando o hash do bloco e a posição do índice do tio.	
	eth_get UncleBy BlockNumber AndIndex	Retorna informaçõ es sobre o bloco tio especificado usando o número do bloco e a posição do índice do tio.	
	Hash eth_get UncleCount ByBlock	Retorna o número de contagens no tio especificado usando o hash do tio.	

Categoria	JSON-RPC	Descrição	Considerações
	Número eth_get UncleCount ByBlock	Retorna o número de contagens no tio especificado usando o número do tio.	
	eth_max PriorityFee PerGas	Retorna a taxa por gasolina, que é uma estimativ a de quanto você pode pagar como taxa prioritár ia, ou “gorjeta”, para incluir uma transação no bloco atual.	Geralmente, você usa o valor retornado desse método para definir o valor `maxFeePer Gas` na transação subsequente que você está enviando.
	Versão ETH_Protocol	Retorna a versão atual do protocolo Ethereum.	
	eth_send RawTransaction	Cria uma nova transação de chamada de mensagem ou uma criação de contrato para transações assinadas.	O Managed Blockchain suporta apenas transações brutas. Você deve criar e assinar transações antes de enviá-las.

Categoria	JSON-RPC	Descrição	Considerações
Depure	hash de debug_trace BlockBy	Retorna o número possível do resultado do rastreamento executando todas as transações no bloco especific ado pelo hash do bloco com um rastreador (é necessário o Modo de Rastreamento).	
	Número debug_trace BlockBy	Retorna o resultado do rastreamento executando todas as transações no bloco especificado por número com um rastreador (é necessário o Modo de Rastreamento).	

Categoria	JSON-RPC	Descrição	Considerações
	Debug_TraceCall	Retorna o número de resultados de rastreamento possíveis executando uma chamada eth dentro do contexto da execução do bloco em questão (é necessário o Modo de Rastreamento).	
	Transação DEBUG_TRACE	Retorna todos os traços de uma determinada transação (é necessário o Modo de Rastreamento).	
Net	versão_rede	Retorna o ID da rede atual.	
Rastreamento	trace_block	Retorna um rastreamento completo da pilha de todos os opcodes invocados de todas as transações que foram incluídas em um bloco.	

Categoria	JSON-RPC	Descrição	Considerações
	trace_call	Retorna o número de resultados de rastreamento possíveis executando uma chamada eth dentro do contexto da execução do bloco em questão (é necessário o Modo de Rastreamento).	
	trace_transaction	Retorna todos os traços de uma determinada transação (é necessário o Modo de Rastreamento).	
Piscina Tx	txpool_content	Retorna todas as transações pendentes e em fila.	

Categoria	JSON-RPC	Descrição	Considerações
	txpool_status	Fornece uma contagem de todas as transaçõe s atualmente pendentes de inclusão nos próximos blocos e daquelas que estão na fila (sendo programad as somente para execução futura).	
Web	Versão Web3_Client	Retorna a versão atual do cliente.	

Casos de uso do Polygon com o Amazon Managed Blockchain (AMB) Access Polygon

O blockchain Polygon é comumente usado na criação de aplicativos descentralizados (DApps) relacionados a NFTs, jogos Web3 e casos de uso de tokenização, entre outros. Este tópico fornece uma lista de alguns dos casos de uso que você pode implementar usando o Amazon Managed Blockchain (AMB) Access Polygon.

Tópicos

Analise dados Polygon NFT

Você pode coletar dados sobre Polygon NFTs, incluindo informações como eventos de transferência e metadados NFT por um período especificado. Em seguida, você pode analisar esses dados para obter informações como quais NFTs estão em alta ou quais usuários estão interagindo com mais frequência com uma determinada coleção.

Para ter mais informações, consulte API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon.

Support compras de NFT

Você pode usar o AMB Access Polygon para enviar transações para compras de NFT usando o Initial Mint, as listas de permissões ou no mercado secundário. Usando uma combinação de outros AWS serviços, você pode então permitir compras usando cartões de crédito, aceitando Fiat ou criptomoedas, com um acordo rápido para todas as partes interessadas envolvidas.

Para ter mais informações, consulte API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon.

Crie uma carteira Polygon

Você pode usar o AMB Access Polygon para atender a funções críticas de carteiras de ativos digitais, como ler saldos de tokens de usuários de contratos inteligentes no blockchain ou transmitir transações assinadas para o blockchain.

Para ter mais informações, consulte API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon.

Carteira como serviço

Você pode usar o AMB Access Polygon para desenvolver uma operação wallet-as-a-service necessária para suportar transações comuns de carteira, como verificação de saldo, transferência de ativos, envio de ativos e estimativas de taxas, usando os Polygon JSON-RPCs compatíveis.

Para ter mais informações, consulte API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon.

Experiências bloqueadas por tokens

Você pode usar o AMB Access Polygon para criar experiências controladas por tokens para seus usuários. Por exemplo, você pode fornecer acesso condicional a um conteúdo somente para os proprietários de um NFT específico. Para conseguir isso, você deve ler o blockchain para determinar a propriedade NFT do endereço de um usuário.

Para ter mais informações, consulte API de blockchain gerenciada e JSON-RPCs compatíveis com o AMB Access Polygon.

Tutoriais para o Amazon Managed Blockchain (AMB) Access Polygon

Os tutoriais a seguir destacados nesta seção são artigos da comunidade AWS re:Post que fornecem orientações para ajudá-lo a aprender como realizar algumas tarefas comuns no blockchain Polygon usando o AMB Access Polygon.

- Envio de transações usando AMB Access Polygon e web3.js
- Implemente um contrato inteligente usando o AMB Access Polygon e o Hardhat Ignition
- Interagindo com um contrato inteligente
- Recupere dados de preços atuais fora da cadeia usando os feeds de dados AMB Access Polygon e Chainlink
- Analise os dados do token ERC-20 na Polygon Mainnet com o AMB Access

Segurança no polígono de acesso do Amazon Managed Blockchain (AMB)

A segurança na nuvem AWS é da mais alta prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança na nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Managed Blockchain (AMB) Access Polygon, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Para fornecer proteção de dados, autenticação e controle de acesso, o Amazon Managed Blockchain usa AWS recursos e os recursos da estrutura de código aberto executada no Managed Blockchain.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AMB Access Polygon. Os tópicos a seguir mostram como configurar o AMB Access Polygon para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do AMB Access Polygon.

Tópicos

Proteção de dados no Amazon Managed Blockchain (AMB) Access Polygon

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no Amazon Managed Blockchain (AMB) Access Polygon. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AMB Access Polygon ou outro Serviços da

AWS usando o console, a API ou os AWS CLI SDKs. AWS Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados

A criptografia de dados ajuda a impedir que usuários não autorizados leiam dados de uma rede blockchain e dos sistemas de armazenamento de dados associados. Isso inclui dados que podem ser interceptados enquanto viajam pela rede, conhecidos como dados em trânsito.

Criptografia em trânsito

Por padrão, o Managed Blockchain usa uma conexão HTTPS/TLS para criptografar todos os dados transmitidos de um computador cliente que executa os AWS CLI dois endpoints de serviço. AWS

Você não precisa fazer nada para ativar o uso do HTTPS/TLS. Ele está sempre ativado, a menos que você o desative explicitamente para um AWS CLI comando individual usando o `--no-verify-ssl` comando.

Gerenciamento de identidade e acesso para o Amazon Managed Blockchain (AMB) Access Polygon

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AMB Access Polygon. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Solução de problemas de identidade e acesso ao Amazon Managed Blockchain (AMB) Access Polygon

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AMB Access Polygon.

Usuário do serviço — Se você usar o serviço AMB Access Polygon para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do AMB Access Polygon para fazer seu trabalho, talvez você precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no AMB Access Polygon, consulte. Solução de problemas de identidade e acesso ao Amazon Managed Blockchain (AMB) Access Polygon

Administrador de serviços — Se você é responsável pelos recursos do AMB Access Polygon em sua empresa, provavelmente tem acesso total ao AMB Access Polygon. É seu trabalho determinar quais recursos e recursos do AMB Access Polygon seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o AMB Access Polygon, consulte. Como o Amazon Managed Blockchain (AMB) Access Polygon funciona com o IAM

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AMB Access Polygon. Para ver exemplos de políticas baseadas em identidade do AMB Access Polygon que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos

de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "O que é o Centro de Identidade do IAM?" no Guia do usuário AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de

serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon Managed Blockchain (AMB) Access Polygon funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AMB Access Polygon, saiba quais recursos do IAM estão disponíveis para uso com o AMB Access Polygon.

Recursos do IAM que você pode usar com o Amazon Managed Blockchain (AMB) Access Polygon

Atributo do IAM	Suporte para AMB Access Polygon
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Não
Chaves de condição de políticas	Não
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Não
Permissões de entidade principal	Não
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para ter uma visão de alto nível de como o AMB Access Polygon e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte os AWS serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AMB Access Polygon

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o AMB Access Polygon

Para ver exemplos de políticas baseadas em identidade do AMB Access Polygon, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Políticas baseadas em recursos no AMB Access Polygon

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para

o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para o AMB Access Polygon

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AMB Access Polygon, consulte Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon na Referência de Autorização de Serviço.

As ações de política no AMB Access Polygon usam o seguinte prefixo antes da ação:

```
managedblockchain:
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `InvokeRpcPolygon`, inclua a seguinte ação:

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

Para ver exemplos de políticas baseadas em identidade do AMB Access Polygon, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Recursos de política para o AMB Access Polygon

Oferece compatibilidade com recursos de políticas	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do AMB Access Polygon e seus ARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Access Polygon na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon.

Para ver exemplos de políticas baseadas em identidade do AMB Access Polygon, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Chaves de condição de política para o AMB Access Polygon

Suporta chaves de condição de política específicas de serviço	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AMB Access Polygon, consulte Chaves de condição para o Amazon Managed Blockchain (AMB) Access Polygon na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon.

Para ver exemplos de políticas baseadas em identidade do AMB Access Polygon, consulte. Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

ACLs no AMB Access Polygon

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com polígono de acesso AMB

Oferece compatibilidade com ABAC (tags em políticas)	Não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com o AMB Access Polygon

Oferece compatibilidade com credenciais temporárias	Não

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para o AMB Access Polygon

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Não

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um

serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções de serviço para AMB Access Polygon

Oferece suporte a perfis de serviço	Não

Um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AMB Access Polygon. Edite as funções de serviço somente quando o AMB Access Polygon fornecer orientação para fazer isso.

Funções vinculadas a serviços para AMB Access Polygon

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna

Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o Amazon Managed Blockchain (AMB) Access Polygon

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AMB Access Polygon. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AMB Access Polygon, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o polígono de acesso do Amazon Managed Blockchain (AMB) na Referência de autorização de serviço.

Tópicos

- Melhores práticas de política
- Usando o console AMB Access Polygon
- Permitir que usuários visualizem suas próprias permissões
- Acessando redes Polygon

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do AMB Access Polygon em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões

definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.

- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usando o console AMB Access Polygon

Para acessar o console Access Polygon do Amazon Managed Blockchain (AMB), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AMB Access Polygon em seu. Conta da AWS Se você criar uma

política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console AMB Access Polygon, anexe também o AMB Access Polygon *ConsoleAccess* ou *ReadOnly* AWS a política gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

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

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acessando redes Polygon

> **Note**
>
> Para acessar os endpoints públicos do Polygon `mainnet` e fazer chamadas JSON-RPC, você precisará de credenciais de usuário (`AWS_ACCESS_KEY_IDeAWS_SECRET_ACCESS_KEY`) que tenham as permissões apropriadas do IAM `mainnet` para o AMB Access Polygon.

Example Política do IAM para acessar todas as redes poligonais

Este exemplo concede a um usuário do IAM em seu Conta da AWS acesso a todas as redes Polygon.

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

Example Política do IAM para acessar a rede Polygon Mainnet

Este exemplo concede a um usuário do IAM seu Conta da AWS acesso à rede Polygon Mainnet.

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

Solução de problemas de identidade e acesso ao Amazon Managed Blockchain (AMB) Access Polygon

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AMB Access Polygon e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no AMB Access Polygon
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus recursos Conta da AWS do AMB Access Polygon

Não estou autorizado a realizar uma ação no AMB Access Polygon

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `managedblockchain::`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `managedblockchain::`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AMB Access Polygon.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AMB Access Polygon. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus recursos Conta da AWS do AMB Access Polygon

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de

controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AMB Access Polygon oferece suporte a esses recursos, consulte. Como o Amazon Managed Blockchain (AMB) Access Polygon funciona com o IAM
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Registrando eventos do Amazon Managed Blockchain (AMB) Access Polygon usando AWS CloudTrail

> **Note**
>
> O Amazon Managed Blockchain (AMB) Access Polygon não oferece suporte a eventos de gerenciamento.

O Amazon Managed Blockchain é executado em AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Managed Blockchain. CloudTrail captura quem invocou os endpoints AMB Access Polygon para o Managed Blockchain como eventos do plano de dados.

Se você criar uma trilha configurada corretamente que esteja inscrita para receber os eventos do plano de dados desejados, poderá receber a entrega contínua de CloudTrail eventos relacionados ao AMB Access Polygon em um bucket do S3. Usando as informações coletadas por CloudTrail, você pode determinar se uma solicitação foi feita para um dos endpoints do AMB Access Polygon, o endereço IP de onde a solicitação veio, quem fez a solicitação, quando ela foi feita e outros detalhes adicionais.

Para saber mais CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações do AMB Access Polygon em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você o cria. No entanto, você deve configurar os eventos do plano de dados para ver quem invocou os endpoints AMB Access Polygon.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do AMB Access Polygon, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões suportadas na AWS partição e entrega os arquivos de log ao bucket do S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar mais detalhadamente e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Usando CloudTrail para rastrear Polygon JSON-RPCs

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Ao analisar os eventos de CloudTrail dados, você pode monitorar quem invocou os endpoints AMB Access Polygon.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM)
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro AWS service (Serviço da AWS)

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

Compreendendo as entradas do arquivo de log do AMB Access Polygon

Para eventos do plano de dados, uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket S3 especificado. Cada arquivo de CloudTrail log contém uma ou mais entradas de log que representam uma única solicitação de qualquer fonte. Essas entradas fornecem detalhes sobre a ação solicitada, incluindo a data e a hora da ação e quaisquer parâmetros de solicitação associados.

> **Note**
>
> CloudTrail os eventos de dados nos arquivos de log não são um rastreamento de pilha ordenado das chamadas da API AMB Access Polygon, portanto, eles não aparecem em nenhuma ordem específica.

Usando CloudTrail para rastrear Polygon JSON-RPCs

Você pode usar CloudTrail para rastrear quem em sua conta invocou os endpoints AMB Access Polygon e qual JSON-RPC foi invocado como eventos de dados. Por padrão, quando você cria uma trilha, os eventos de dados não são registrados. Para registrar quem invocou os endpoints do AMB Access Polygon como eventos de CloudTrail dados, você deve adicionar explicitamente os recursos suportados ou os tipos de recursos para os quais deseja coletar atividades em uma trilha. O AMB Access Polygon suporta a adição de eventos de dados usando o AWS Management Console SDK AWS CLI, e. Para obter mais informações, consulte Registrar eventos usando seletores avançados no Guia do AWS CloudTrail usuário.

Para registrar eventos de dados em uma trilha, use a operação put-event-selectors depois de criar a trilha. Use a `--advanced-event-selectors` opção para especificar os tipos de `AWS::ManagedBlockchain::Network` recursos para começar a registrar eventos de dados para determinar quem invocou os endpoints AMB Access Polygon.

Example Entrada do registro de eventos de dados de todas as solicitações de endpoints AMB Access Polygon da sua conta

O exemplo a seguir demonstra como usar a `put-event-selectors` operação para registrar todas as solicitações de endpoint AMB Access Polygon da sua conta para a trilha na região. `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"] } ]}]'
```

Depois de se inscrever, você pode monitorar o uso no bucket do S3 que está conectado à trilha especificada no exemplo anterior.

O resultado a seguir mostra uma entrada no registro de eventos de CloudTrail dados das informações coletadas pelo CloudTrail. Você pode determinar se uma solicitação Polygon JSON-RPC foi feita para um dos endpoints do AMB Access Polygon, o endereço IP de onde a solicitação veio, quem fez a solicitação, quando ela foi feita e outros detalhes adicionais. Alguns valores no

exemplo a seguir foram ofuscados por motivos de segurança, mas aparecem totalmente nas entradas de registro reais.


```
{
        "eventVersion": "1.09",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA554UO62RJ7KSB7FAX:777777777777",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/777777777777",
            "accountId": "111122223333"
        },
        "eventTime": "2023-04-12T19:00:22Z",
        "eventSource": "managedblockchain.amazonaws.com",
        "eventName": "gettxout",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "111.222.333.444",
        "userAgent": "python-requests/2.28.1",
        "errorCode": "-",
        "errorMessage": "-",
        "requestParameters": {
            "jsonrpc": "2.0",
            "method": "gettxout",
            "params": [],
            "id": 1
        },
        "responseElements": null,
        "requestID": "DRznHHEj********",
        "eventID": "baeb232d-2c6b-46cd-992c-0e40********",
        "readOnly": true,
        "resources": [{
            "type": "AWS::ManagedBlockchain::Network",
            "ARN": "arn:aws:managedblockchain:::networks/n-polygon-mainnet"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data"
}
```

Histórico de documentos do Guia do usuário do AMB Access Polygon

A tabela a seguir descreve as versões da documentação do AMB Access Polygon.

Alteração	Descrição	Data
Cotas atualizadas para JSON-RPC	As cotas suportadas pelo AMB Access Polygon para cada JSON-RPC compatível são atualizadas.	12 de abril de 2024
Fim do suporte para a rede testnet de Mumbai	O AMB Access Polygon encerrou o suporte da testnet de Mumbai em 15 de abril de 2024.	10 de abril de 2024
Adição do tópico Tutoriais	Tutoriais do AMB Access Polygon da seção Artigos da comunidade do AWS re:POST.	9 de abril de 2024
Pré-visualização pública	Versão prévia pública do serviço Amazon Managed Blockchain (AMB) Access Polygon.	24 de novembro de 2023