Guía para desarrolladores

Polígono de acceso AMB

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Polígono de acceso AMB: Guía para desarrolladores

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

..... v
Acerca de AMB Access Polygon 1
Recursos para usuarios primerizos de AMB Access Polygon 1
Conceptos clave 2
Consideraciones y limitaciones 3
Configuración 5
Requisitos previos para usar AMB Access Polygon 5
Inscríbase en AWS 5
Cree un usuario de IAM con los permisos adecuados 6
Instalación y configuración de la AWS Command Line Interface 6
Introducción 8
Creación de una política de IAM 8
Ejemplo de RPC de consola 9
`awscurl`Ejemplo de RPC 10
Ejemplo de RPC de Node.js 12
Enviar transacción 16
Lee la transacción 18
Acceso basado en tokens 20
Crear un token de acceso para el acceso basado en un token 21
Visualización de los detalles de un token de acceso 22
Eliminar un token de acceso 23
JSON-RPC y API 24
Casos de uso de Polygon 36
Analice los datos de NFT de Polygon 36
Support NFT compras 36
Crea un monedero Polygon 37
El monedero como servicio 37
Experiencias basadas en fichas 37
Tutoriales 38
Seguridad 39
Protección de los datos 40
Cifrado de datos 41
Cifrado en tránsito 41
Identity and Access Management 41

Público 42
Autenticación con identidades 42
Administración de acceso mediante políticas 46
Cómo funciona Amazon Managed Blockchain (AMB) Access Polygon con IAM 49
Ejemplos de políticas basadas en identidades 56
Solución de problemas 61
CloudTrail registros 63
Información sobre AMB Access Polygon en CloudTrail 63
Descripción de las entradas del archivo de registro de AMB Access Polygon 64
Se usa CloudTrail para rastrear Polygon JSON- RPCs 65
Historial de documentos 67

Amazon Managed Blockchain (AMB) Access Polygon se encuentra en versión preliminar y está sujeto a cambios.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.

¿Qué es Amazon Managed Blockchain (AMB) Access Polygon?

Amazon Managed Blockchain (AMB) Access Polygon es un servicio totalmente gestionado que le ayuda a crear aplicaciones Web3 resilientes en la cadena de bloques de Polygon. AMB Access Polygon proporciona acceso instantáneo y sin servidor a la cadena de bloques de Polygon.

Polygon es una solución de escalado que utiliza la máquina virtual Ethereum (EVM) como base. La cadena de bloques Polygon es conocida por su alto rendimiento de transacciones y sus bajas tarifas de transacción. La cadena de bloques Polygon utiliza un proof-of-stake mecanismo de consenso. Polygon se usa comúnmente para crear aplicaciones descentralizadas (DApps) relacionadas con juegos Web3 y casos de uso de tokenización, entre otros. NFTs

Esta guía explica cómo crear y gestionar los recursos de la cadena de bloques de Polygon mediante Amazon Managed Blockchain (AMB) Access Polygon.

Recursos para usuarios primerizos de AMB Access Polygon

Si es la primera vez que utiliza AMB Access Polygon, le recomendamos que comience leyendo las siguientes secciones:

- Conceptos clave: polígono de acceso a Amazon Managed Blockchain (AMB)
- Introducción a Amazon Managed Blockchain (AMB) Access Polygon
- La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon

Conceptos clave: polígono de acceso a Amazon Managed Blockchain (AMB)

> **Note**
>
> En esta guía se supone que está familiarizado con los conceptos esenciales de Polygon. Estos conceptos incluyen las apuestas, las dApps, las transacciones, las carteras, los contratos inteligentes, Polygon (POL, anteriormente MATIC) y otros. Antes de usar Amazon Managed Blockchain (AMB) Access Polygon, le recomendamos que consulte la documentación de desarrollo de Polygon y la wiki de Polygon.

Amazon Managed Blockchain (AMB) Access Polygon le proporciona acceso sin servidor a las redes Polygon Mainnet y Polygon Mainnet, sin necesidad de aprovisionar ni administrar ninguna infraestructura de Polygon, incluidos los nodos. Los nodos poligonales de una red almacenan colectivamente el estado de la cadena de bloques de Polygon, verifican las transacciones y participan en el consenso para cambiar el estado de la cadena de bloques. Puede utilizar este servicio gestionado para acceder a las redes de Polygon de forma rápida y bajo demanda, lo que reduce el coste total de propiedad.

Con AMB Access Polygon, tiene acceso a las llamadas de procedimiento remoto JSON (JSON-RPC). Puede invocar Polygon JSON- RPCs para comunicarse con la cadena de bloques de Polygon a través de nodos gestionados por Managed Blockchain. Puede usar el servicio AMB Access Polygon para desarrollar y usar aplicaciones descentralizadas (DApps) que interactúan con la cadena de bloques Polygon. Una parte integral de las dApps son los contratos inteligentes. Puede crear e implementar contratos inteligentes en la cadena de bloques de Polygon utilizando AMB Access Polygon. También puedes comprobar los saldos de tus carteras, los detalles de las transacciones, las comisiones estimadas, etc., utilizando JSON y comparándolo con los puntos de conexión de RPCs AMB Access Polygon, que funcionan de forma descentralizada en todos los nodos homólogos de la red de Polygon. Cualquier usuario de la red Polygon puede desarrollar e implementar un contrato inteligente.

> **Important**
>
> Usted es responsable de crear, mantener, usar y administrar sus direcciones de Polygon. También eres responsable del contenido de tus direcciones de Polygon. AWS no se hace

responsable de ninguna transacción desplegada o llamada mediante nodos Polygon en Amazon Managed Blockchain.

Consideraciones y limitaciones para usar Amazon Managed Blockchain (AMB) Access Polygon

Cuando utilice Amazon Managed Blockchain (AMB) Access Polygon, tenga en cuenta lo siguiente:

- Redes Polygon compatibles

  AMB Access Polygon es compatible con las siguientes redes públicas:

  - Mainnet: la cadena de bloques pública de Polygon asegurada por proof-of-stake consenso y en la que se emite y se negocia el token Polygon (POL). Las transacciones en Mainnet tienen un valor real (es decir, incurren en costes reales) y se registran en la cadena de bloques pública.

- Polygon ya no admite redes

  - Según lo comunicado por Polygon Labs, la red Testnet de Mumbai dejará de funcionar a mediados de abril. En línea con esta noticia, AMB Access Polygon dejó de ofrecer soporte a la red de pruebas de Mumbai el 15 de abril de 2024. Le recomendamos que utilice Amoy Testnet para su carga de trabajo de pruebas.
  - No se admiten redes privadas.
  - Además, AMB Access Polygon no incluye soporte para la red Polygon ZKevM.

- Compatibilidad con populares bibliotecas de programación de terceros

  AMB Access Polygon es compatible con bibliotecas de programación populares, como ethers.js, lo que permite a los desarrolladores interactuar con la cadena de bloques de Polygon utilizando herramientas conocidas para integrarse fácilmente con sus implementaciones existentes o desarrollar nuevas aplicaciones rápidamente.

- Regiones admitidas

  Este servicio solo se admite en la región de EE. UU. Este (Virginia del Norte).

- Service endpoints

  Los siguientes son los puntos finales del servicio para AMB Access Polygon. Para conectarse al servicio, debe usar un punto final que incluya una de las regiones compatibles.

- `mainnet.polygon.managedblockchain.us-east-1.amazonaws.com`
- No se admite el replanteo

  AMB Access Polygon no admite nodos validadores Polygon (POL) para. proof-of-stake
- Firma (versión 4): firma las solicitudes JSON-RPC de Polygon

  Al realizar llamadas al polígono JSON- RPCs en Amazon Managed Blockchain, puede hacerlo a través de una conexión HTTPS autenticada mediante el proceso de firma Signature Version 4. Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden realizar llamadas JSON-RPC a Polygon. Para ello, se deben proporcionar AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.

  > **Important**
  > - No inserte las credenciales del cliente en las aplicaciones orientadas al usuario.
  > - No puede utilizar las políticas de IAM para restringir el acceso a un Polygon JSON- individual. RPCs

- Support for Token Based Access

  También puede utilizar los tokens de acceso para realizar llamadas JSON-RPC a los puntos finales de la red Polygon como una práctica alternativa al proceso de firma de la versión 4 (SiGv4) de Signature. Debe proporcionar uno `BILLING_TOKEN` de los tokens de acceso que cree y añada como parámetro a sus llamadas.

  > **Important**
  > - Si priorizas la seguridad y la auditabilidad por encima de la comodidad, utiliza el proceso de firma SigV4 en su lugar.
  > - Puede acceder al JSON de Polygon RPCs mediante la versión 4 de Signature (SiGv4) y el acceso basado en tokens. Sin embargo, si eliges usar ambos protocolos, tu solicitud será rechazada.
  > - Nunca debe incrustar los tokens de acceso en aplicaciones orientadas a los usuarios.

- Solo se admiten los envíos de transacciones sin procesar

  Usa el `eth_sendrawtransaction` JSON-RPC para enviar transacciones que actualicen el estado de la cadena de bloques de Polygon.

Configuración del polígono de acceso a Amazon Managed Blockchain (AMB)

Antes de utilizar Amazon Managed Blockchain (AMB) Access Polygon (AMB) por primera vez, siga los pasos de esta sección para crear un. Cuenta de AWS En el siguiente capítulo se explica cómo empezar a utilizar AMB Access Polygon.

Requisitos previos para usar AMB Access Polygon

Antes de usarlo AWS por primera vez, debe tener un. Cuenta de AWS

Inscríbase en AWS

Cuando te registras AWS, te Cuenta de AWS registras automáticamente para todos Servicios de AWS, incluido Amazon Managed Blockchain (AMB) Access Polygon. Solo se le cobrará por los servicios que utilice.

Si Cuenta de AWS ya tienes uno, continúa con el siguiente paso. Si no dispone de una Cuenta de AWS, utilice el siguiente procedimiento para crear una.

Para crear un Cuenta de AWS

1. Abre el https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro implica recibir una llamada telefónica o un mensaje de texto e introducir un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Cree un usuario de IAM con los permisos adecuados

Para crear y trabajar con AMB Access Polygon, debes tener un director AWS Identity and Access Management (IAM) (usuario o grupo) con permisos que permitan realizar las acciones necesarias de la cadena de bloques gestionada.

Al realizar llamadas al polígono JSON- RPCs en Amazon Managed Blockchain, puede hacerlo a través de una conexión HTTPS autenticada mediante el proceso de firma Signature Version 4. Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden realizar llamadas JSON-RPC a Polygon. Para ello, se deben proporcionar AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.

También puede utilizar los tokens de acceso para realizar llamadas JSON-RPC a los puntos finales de la red Polygon como una práctica alternativa al proceso de firma de la versión 4 (SiGv4) de Signature. Debe proporcionar uno `BILLING_TOKEN` de los tokens de acceso que cree y añada como parámetro a sus llamadas. Sin embargo, sigue necesitando acceso a IAM para obtener los permisos necesarios para crear los tokens de acceso mediante el AWS Management Console AWS CLI, y el SDK.

Para obtener información sobre cómo crear un usuario de IAM, consulte Crear un usuario de IAM en su cuenta. AWS Para obtener más información sobre cómo adjuntar una política de permisos a un usuario, consulte Cambiar los permisos de un usuario de IAM. Para ver un ejemplo de una política de permisos que puede utilizar para conceder permiso a un usuario para que trabaje con AMB Access Polygon, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

Instalación y configuración de la AWS Command Line Interface

Si aún no lo ha hecho, instale la última versión AWS Command Line Interface (AWS CLI) para trabajar con AWS los recursos de una terminal. Para obtener más información, consulte Instalación o actualización de la versión de AWS CLI más reciente.

> **Note**
>
> Para acceder a la CLI, necesita un ID de clave de acceso y una clave de acceso secreta. Cuando sea posible, utilice credenciales temporales en lugar de claves de acceso. Las credenciales temporales incluyen un ID de clave de acceso y una clave de acceso secreta, pero, además, incluyen un token de seguridad que indica cuándo caducan las credenciales.

Para obtener más información, consulte Uso de credenciales temporales con AWS recursos en la Guía del usuario de IAM.

Introducción a Amazon Managed Blockchain (AMB) Access Polygon

Comience a utilizar Amazon Managed Blockchain (AMB) Access Polygon con la información y los procedimientos de esta sección.

Temas

- Cree una política de IAM para acceder a la red de cadenas de bloques de Polygon
- Realice solicitudes de llamadas a procedimientos remotos (RPC) de Polygon en el editor RPC de AMB Access mediante el AWS Management Console
- Realice las solicitudes JSON-RPC de AMB Access Polygon mediante el awscurlAWS CLI
- Realice solicitudes JSON-RPC de Polygon en Node.js

Cree una política de IAM para acceder a la red de cadenas de bloques de Polygon

Para acceder al punto final público de la red principal de Polygon y realizar llamadas JSON-RPC, debe tener credenciales de usuario (`AWS_ACCESS_KEY_IDyAWS_SECRET_ACCESS_KEY`) los permisos de IAM adecuados para Amazon Managed Blockchain (AMB) Access Polygon. En una terminal con el terminal AWS CLI instalado, ejecute el siguiente comando para crear una política de IAM que permita acceder a los dos puntos de enlace de 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**
>
> El ejemplo anterior le da acceso a todas las redes de Polygon disponibles. Para acceder a un punto final específico, utilice el siguiente `Action` comando:
>
> - `"managedblockchain:InvokeRpcPolygonMainnet"`

Después de crear la política, asocie esa política a la función de su usuario de IAM para que surta efecto. En el AWS Management Console, navegue hasta el servicio de IAM y asocie la política `AmazonManagedBlockchainPolygonAccess` a la función asignada a su usuario de IAM.

Realice solicitudes de llamadas a procedimientos remotos (RPC) de Polygon en el editor RPC de AMB Access mediante el AWS Management Console

Puede editar, configurar y enviar llamadas a procedimientos remotos (RPCs) en el polígono de acceso AMB que AWS Management Console utiliza. Con ellas RPCs, puede leer datos y escribir transacciones en la red Polygon, incluida la recuperación de datos y el envío de transacciones a la red Polygon.

Example

El siguiente ejemplo muestra cómo obtener información sobre el último bloque mediante RPC. `eth_getBlockByNumber` Cambie las variables resaltadas por sus propias entradas o elija uno de los métodos de RPC de la lista e introduzca las entradas pertinentes necesarias.

1. Abre la consola de Managed Blockchain en https://console.aws.amazon.com/managedblockchain/.
2. Elija el editor RPC.
3. En la sección Solicitud, elija *`POLYGON_MAINNET`* como. ***`Blockchain Network`***
4. Elija *`eth_getBlockByNumber`* como método RPC.

5. **`latest`**Introdúzcalo como indicador de transacción completa ***`Block number`***y *`False`* selecciónelo como indicador de transacción completa.
6. A continuación, selecciona Enviar RPC.
7. Los resultados del `latest` bloqueo se muestran en la sección de respuestas. A continuación, puede copiar todas las transacciones sin procesar para analizarlas más a fondo o utilizarlas en la lógica empresarial de sus aplicaciones.

Para obtener más información, consulte la página RPCs compatible con AMB Access Polygon

Realice las solicitudes JSON-RPC de AMB Access Polygon mediante el **`awscurl`**AWS CLI

Example

Firme las solicitudes con sus credenciales de usuario de IAM mediante la versión 4 de Signature (SiGv4) para realizar solicitudes JSON-RPC de Polygon a los puntos finales de AMB Access Polygon. La herramienta de línea de `awscurl`comandos puede ayudarle a firmar las solicitudes de servicios mediante SiGv4. AWS Para obtener más información, consulta el archivo README.md de awscurl.

Realice la instalación `awscurl` mediante el método apropiado para su sistema operativo. En macOS, la aplicación recomendada HomeBrew es:

```
brew install awscurl
```

Si ya la ha instalado y configurado AWS CLI, sus credenciales de usuario de IAM y las predeterminadas Región de AWS están configuradas en su entorno y a `awscurl` las que tiene acceso. Para ello`awscurl`, envíe una solicitud a la red principal de Polygon invocando el RPC. `eth_getBlockByNumber` Esta llamada acepta un parámetro de cadena correspondiente al número de bloque del que se desea recuperar información.

El siguiente comando recupera los datos del bloque de la red principal de Polygon utilizando el número de bloque de la `params` matriz para seleccionar el bloque específico del que se van a recuperar los encabezados.

```
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**
>
> También puede realizar esta misma solicitud utilizando `curl` la función de acceso basado en el token de AMB Access mediante el uso de tokens. `Accessor` Para obtener más información, consulte Creación y administración de tokens de acceso para el acceso basado en tokens para realizar solicitudes de AMB Access Polygon.
>
> ```
> curl -X POST -d '{"jsonrpc":"2.0", "id": "eth_getBlockByNumber-curltest",
> "method":"eth_getBlockByNumber", "params":["latest", false] }'
> 'https://mainnet.polygon.managedblockchain.us-east-1.amazonaws.com?
> billingtoken=your-billing-token'
> ```

La respuesta de cualquiera de los comandos devuelve información sobre el último bloque. Consulte el siguiente ejemplo con fines ilustrativos:

```
{"error":null,"id":"eth_getBlockByNumber-curltest","jsonrpc":"1.0",
      "result":{"baseFeePerGas":"0x873bf591e","difficulty":"0x18",
      "extraData":"0xd78301000683626f7288676f312e32312e32856c696e757800000000000000009a
\
      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":[]}}
```

Realice solicitudes JSON-RPC de Polygon en Node.js

Puede invocar Polygon JSON RPCs mediante el envío de solicitudes firmadas mediante HTTPS para acceder a la red principal de Polygon mediante el módulo https nativo de Node.js, o puede utilizar una biblioteca de terceros, como AXIOS. Los siguientes ejemplos de Node.js muestran cómo realizar solicitudes JSON-RPC de Polygon al punto final de AMB Access Polygon mediante la versión 4 de Signature (SiGv4) y el acceso basado en tokens. En el primer ejemplo se envía una transacción de una dirección a otra y en el siguiente se solicitan los detalles de la transacción y la información de saldo de la cadena de bloques.

Example

Para ejecutar este script Node.js de ejemplo, aplique los siguientes requisitos previos:

1. Debe tener el administrador de versiones de nodos (nvm) y Node.js instalados en el equipo. Puede encontrar las instrucciones de instalación de su sistema operativo aquí.
2. Utilice el `node --version` comando y confirme que está utilizando la versión 18 o superior de Node. Si es necesario, puede usar el `nvm install v18.12.0` comando, seguido del `nvm use v18.12.0` comando, para instalar la versión 18, la versión LTS de Node.
3. Las variables `AWS_ACCESS_KEY_ID` de entorno `AWS_SECRET_ACCESS_KEY` deben contener las credenciales asociadas a su cuenta.

   Exporte estas variables como cadenas en su cliente mediante los siguientes comandos. Sustituya los valores en rojo de las siguientes cadenas por los valores adecuados de su cuenta de usuario de IAM.

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

Tras completar todos los requisitos previos, copie los siguientes archivos en un directorio de su entorno local mediante el editor de código que prefiera:

package.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**
>
> El siguiente código utiliza una clave privada codificada para generar una cartera que Signer utilice únicamente con `Ethers.js` fines de demostración. No utilice este código en entornos de producción, ya que tiene fondos reales y supone un riesgo para la seguridad.
> Si es necesario, ponte en contacto con tu equipo de cuentas para que te asesoren sobre las mejores prácticas de Wallet y Signer.

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

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

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

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

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

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

  console.log(tx);
};

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

readTx.js

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

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

  //set RPC request body to get transaction details
  let getTransactionByHash = {
```

```
    id: "1",
    jsonrpc: "2.0",
    method: "eth_getTransactionByHash",
    params: [txHash],
  };

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

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

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

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

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

Una vez guardados estos archivos en su directorio, instale las dependencias necesarias para ejecutar el código mediante el siguiente comando:

```
npm install
```

Envíe una transacción en Node.js

El ejemplo anterior envía el token nativo de Polygon Mainnet (POL) de una dirección a otra mediante la firma de una transacción y su transmisión a la red principal de Polygon mediante AMB Access Polygon. Para ello, utilice el `sendTx.js` script, que utiliza una biblioteca popular para interactuar con Ethereum y cadenas de bloques compatibles con Ethereum`Ethers.js`, como Polygon. Debes reemplazar las tres variables del código resaltadas en rojo: la del token de acceso `billingToken` para el acceso basado en un token, la clave privada con la que firmas la transacción y la dirección del destinatario que recibe la POL.

> **Tip**
>
> Le recomendamos que cree una clave privada (cartera) nueva para este fin, en lugar de reutilizar una cartera existente para eliminar el riesgo de perder fondos. Puedes usar el método createRandom () de la clase Wallet de la biblioteca Ethers para generar una cartera con la que realizar pruebas. Además, si necesitas solicitar POL desde la red principal de Polygon, puedes usar el recurso POL público para solicitar una pequeña cantidad para utilizarla en las pruebas.

Una vez que hayas añadido tu clave privada *`billingToken`*, la de una cartera financiada y la dirección del destinatario al código, ejecutas el siguiente código para firmar una transacción para que .0001 POL se envíe de tu dirección a otra y la transmites a Polygon Mainnet invocando el `eth_sendRawTransaction` JSON-RPC mediante el polígono de acceso AMB.

```
node sendTx.js
```

La respuesta recibida es similar a la siguiente:

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

```
},
accessList: []
}
```

La respuesta constituye el recibo de la transacción. Guarde el valor de la propiedad`hash`. Este es el identificador de la transacción que acabas de enviar a la cadena de bloques. Utiliza esta propiedad en el ejemplo de transacción de lectura para obtener detalles adicionales sobre esta transacción desde la red principal de Polygon.

Tenga en cuenta que las `blockNumber` y `blockHash` están `null` en la respuesta. Esto se debe a que la transacción aún no se ha registrado en un bloque de la red Polygon. Tenga en cuenta que estos valores se definen más adelante y es posible que los vea cuando solicite los detalles de la transacción en la siguiente sección.

Lee una transacción en Node.js

En esta sección, solicita los detalles de la transacción enviada anteriormente y recupera el saldo de POL de la dirección del destinatario mediante solicitudes de lectura a la red principal de Polygon mediante AMB Access Polygon. En el `readTx.js` archivo, sustituya la variable *`your-transaction-id`* etiquetada por la `hash` que guardó de la respuesta al ejecutar el código de la sección anterior.

Este código utiliza una utilidad que firma las solicitudes HTTPS a AMB Access Polygon con los módulos Sigv4 (SigV4) necesarios del AWS SDK y envía las solicitudes mediante el cliente HTTP AXIOS, muy utilizado. `dispatch-evm-rpc.js`

La respuesta recibida es similar a la siguiente:

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

```
value: '0x5af3107a4000',
type: '0x2',
accessList: [],
chainId: '0x13881',
v: '0x0',
r: '0x1b90ad9e9e4e005904562d50e904f9db10430a18b45931c059960ede337238ee',
s: '0x7df3c930a964fd07fed4a59f60b4ee896ffc7df4ea41b0facfe82b470db448b7'
} BALANCE: 0.0003
```

La respuesta representa los detalles de la transacción. Tenga en cuenta que es probable que `blockNumber` los `blockHash` y ahora estén definidos. Esto indica que la transacción se ha registrado en un bloque. Si estos valores se mantienen`null`, espere unos minutos y vuelva a ejecutar el código para comprobar si la transacción se ha incluido en un bloque. Por último, la representación hexadecimal del saldo de direcciones del destinatario (0x110d9316ec000) se convierte a decimal mediante el `formatEther()` método de Ethers, que convierte el hexadecimal en decimal y desplaza los decimales en 18 (10^18) para obtener el saldo real en POL.

> **Tip**
>
> Si bien los ejemplos de código anteriores ilustran cómo usar Node.js, Ethers y Axios para utilizar algunos de los polígonos de acceso JSON RPCs en AMB compatibles, puede modificar los ejemplos y escribir otro código para crear sus aplicaciones en Polygon mediante este servicio. Para obtener una lista completa de los polígonos de acceso JSON RPCs en AMB compatibles, consulte. La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon

Creación y administración de tokens de acceso para el acceso basado en tokens para realizar solicitudes de AMB Access Polygon

También puede utilizar los tokens de acceso para realizar llamadas JSON-RPC a los puntos finales de la red Polygon como una práctica alternativa al proceso de firma de la versión 4 (SiGv4) de Signature. Debe proporcionar uno `BILLING_TOKEN` de los tokens de acceso que cree y añada como parámetro a sus llamadas.

> **Important**
>
> - Si priorizas la seguridad y la auditabilidad por encima de la comodidad, utiliza el proceso de firma SigV4 en su lugar.
> - Puede acceder al JSON de Polygon RPCs mediante la versión 4 de Signature (SiGv4) y el acceso basado en tokens. Sin embargo, si eliges usar ambos protocolos, tu solicitud será rechazada.
> - Nunca debe incrustar los tokens de acceso en aplicaciones orientadas a los usuarios.

En la consola, la página Tokens Accessors muestra una lista de todos los tokens de acceso que puede utilizar para realizar llamadas JSON-RPC de AMB Access Polygon desde el código de un cliente. Cuenta de AWS

Para obtener más información sobre las solicitudes JSON-RPC de AMB Access Polygon, consulte. La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon

Puede crear y administrar los tokens de acceso mediante. AWS Management Console También puede crear y administrar los tokens de acceso mediante las siguientes operaciones de API:`CreateAccessor`, `GetAccessorListAccessors`, y. `DeleteAccessor` A `BILLING_TOKEN` es propiedad del descriptor de acceso. Esta `BILLING_TOKEN` propiedad se utiliza para rastrear su descriptor de acceso y para facturar las solicitudes JSON-RPC de AMB Access Polygon realizadas por usted. Cuenta de AWS

Todas las acciones de la API relacionadas con la creación y administración de los tokens de acceso también están disponibles a través de, y. AWS Management Console AWS CLI SDKs

Crear un token de acceso para el acceso basado en un token

Puede crear un token de acceso y usarlo para realizar llamadas a la API de AMB Access Polygon en cualquier nodo de AMB Access Polygon de su entorno. Cuenta de AWS

Cree un token de acceso para realizar solicitudes JSON-RPC de AMB Access Polygon mediante el AWS Management Console

1. Abra la consola de Managed Blockchain en. https://console.aws.amazon.com/managedblockchain/
2. Elija Token Accessors.
3. Elija Crear descriptor de acceso.
4. Elija una red de cadena de bloques Polygon válida.
5. Opcional, añada etiquetas para su descriptor de acceso.
6. Seleccione Crear descriptor de acceso para crear un nuevo token de acceso.

Cree un token de acceso para realizar solicitudes JSON-RPC de AMB Access Polygon mediante el AWS CLI

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

El comando anterior devuelve el valor `AccessorId` junto con el`BillingToken`, como se muestra en el siguiente ejemplo.

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

El elemento clave de su respuesta es el`BillingToken`. Puede usar esta propiedad para realizar llamadas JSON-RPC a AMB Access Polygon. Algunos valores del ejemplo se han ocultado por motivos de seguridad, pero aparecerán completamente en las respuestas reales.

> **Note**
>
> Una vez ejecutada la operación, Managed Blockchain aprovisiona y configura el token por ti. La duración de este proceso depende de muchas variables.

Visualización de los detalles de un token de acceso

Puede ver las propiedades de cada token de acceso que posea Cuenta de AWS . Por ejemplo, puede ver el ID de acceso o el nombre de recurso de Amazon (ARN) del descriptor de acceso. También puede ver el estado, el tipo, la fecha de creación y el. `BillingToken`

Para ver la información de un token de acceso mediante el AWS Management Console

1. Abra la consola de Managed Blockchain en https://console.aws.amazon.com/managedblockchain/.
2. En el panel de navegación, elija Token Accessors.
3. Elija el ID de acceso del token de la lista.

Aparece la página de detalles del token. Desde esta página, puede ver las propiedades del token.

Para ver la información de un token de acceso mediante el AWS CLI

Ejecute el siguiente comando para ver los detalles de un token de acceso. Sustituya los valores `--accessor-id` de por su ID de acceso.

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

Esta `BillingToken` y otras propiedades clave se devuelven como se muestra en el siguiente ejemplo. Algunos valores del ejemplo se han ocultado por motivos de seguridad, pero aparecen completamente en las respuestas reales.

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

Eliminar un token de acceso

Al eliminar un token de acceso, el token cambia de estado `AVAILABLE` a estado. `PENDING_DELETION` No puedes usar un token de acceso con ese estado. `PENDING_DELETION`

Para eliminar un token de acceso mediante el AWS Management Console

1. Abra la consola de Managed Blockchain en https://console.aws.amazon.com/managedblockchain/.
2. En el panel de navegación, elija Token Accessors.
3. Seleccione el token de acceso que desee de la lista.
4. Elija Eliminar.
5. Confirme su elección.

Volverás a la página de identificadores de acceso con el identificador de acceso eliminado. La página muestra el `PENDING_DELETION` estado.

Para eliminar un token de acceso mediante el AWS CLI

En el siguiente ejemplo, se muestra cómo eliminar un token. Utilice el `delete-accessor` comando para eliminar un token. Defina el valor de `--accessor-id` con su ID de acceso.

Eliminar un token de acceso mediante la CLI AWS

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

Si este comando se ejecuta correctamente, no se devuelve ningún mensaje.

La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon

Amazon Managed Blockchain proporciona operaciones de API para crear y administrar accesores de token para AMB Access Polygon. Para obtener más información, consulte la Guía de referencia de la API de cadena de bloques gestionada.

En el siguiente tema se proporciona una lista y una referencia del JSON de Polygon compatible RPCs con AMB Access Polygon. Cada JSON-RPC compatible incluye una breve descripción de su uso. El JSON- de Polygon se utiliza RPCs para consultar y obtener datos de contratos inteligentes, obtener detalles de transacciones, enviar transacciones y otras utilidades, como realizar un seguimiento de las transacciones y estimar las tarifas.

AMB Access Polygon admite los siguientes métodos JSON-RPC. Cada JSON-RPC compatible tiene una categoría y una breve descripción de su utilidad y sus cuotas de solicitud predeterminadas. Cuando proceda, se indican las consideraciones específicas sobre el uso del método JSON-RPC con Amazon Managed Blockchain.

> **Note**
>
> - No se admite ningún método que no aparezca en la lista.
> - Al realizar llamadas al polígono JSON- RPCs en Amazon Managed Blockchain, puede hacerlo a través de una conexión HTTPS autenticada mediante el proceso de firma Signature Version 4. Esto significa que solo los directores de IAM autorizados de la AWS cuenta pueden realizar llamadas JSON-RPC a Polygon. Para ello, se deben proporcionar AWS las credenciales (un identificador de clave de acceso y una clave de acceso secreta) junto con la llamada.
> - También puede utilizar el acceso basado en un token como alternativa práctica al proceso de firma de la versión 4 (SiGv4). Si prioriza la seguridad y la auditabilidad por encima de la comodidad, utilice el proceso de firma SigV4 en su lugar. Sin embargo, si utilizas tanto el acceso SigV4 como el acceso basado en token, tus solicitudes no funcionarán.
> - Para esta versión preliminar, las solicitudes por lotes de JSON-RPC no se admiten en Amazon Managed Blockchain (AMB) Access Polygon.

- La columna Cuotas de la siguiente tabla muestra la cuota de cada JSON-RPC. Las cuotas se establecen en solicitudes por segundo (RPS) por región y red poligonal (red principal) para cada JSON-RPC.

  Para aumentar su cuota, debe ponerse en contacto con. Soporte Para ponerse en contacto Soporte, inicie sesión en AWS Support Center Console. Seleccione Crear caso. Elija Técnico. Elija Managed Blockchain como su servicio. Elija Access:Polygon como su categoría y las instrucciones generales como su gravedad. Introduzca la cuota de RPC como asunto y, en el cuadro de texto de descripción, indique el JSON-RPC y los límites de cuota aplicables a sus necesidades de RPS por red de polígonos y región. Envíe su caso.

Categoría	JSON-RPC	Descripción	Consideraciones
Ethereum	Número ETH_BLOCK	Devuelve el número del bloque más reciente.	
	eth_call	Ejecuta inmediatamente una nueva llamada de mensaje sin crear una transacción en la cadena de bloques.	`eth_call`no consume gas, pero tiene un parámetro de gas para los mensajes que lo requieren.
	ETH_Chainid	Devuelve un valor entero para el valor actualmente configurado que se introdujo en el `Chain Id` EIP-155. Retorna `None` si no hay ninguno disponible`Chain Id`.	

Categoría	JSON-RPC	Descripción	Consideraciones
	ETH_EstimateGas	Calcula y devuelve el gas necesario para una transacción sin añadir la transacción a la cadena de bloques.	
	Historial de ETH_FEE	Devuelve una colección de información histórica sobre los gases.	
	Precio de ETH_GasPrice	Devuelve el precio actual del gas en Wei.	
	ETH_GetBalance	Devuelve el saldo de una cuenta para la dirección de la cuenta y el identificador de bloque especificados.	
	eth_ Hash getBlockBy	Devuelve información sobre el bloque especificado mediante el hash del bloque.	
	eth_ Número getBlockBy	Devuelve información sobre el bloque especificado mediante el número de bloque.	

Categoría	JSON-RPC	Descripción	Consideraciones
	eth_ getBlockReceipts	Devuelve los recibos del bloque especificado utilizando el número de bloque.	
	eth_ getBlockTransaction CountByHash	Devuelve el número de transacciones del bloque especific ado mediante el hash del bloque.	
	eth_ getBlockTransaction CountByNu mber	Devuelve el número de transacciones del bloque especific ado mediante el número de bloque.	
	ETH_GetCode	Devuelve el código en la dirección de la cuenta y el identificador de bloque especific ados.	

Categoría	JSON-RPC	Descripción	Consideraciones
	ETH_GetLogs	Devuelve una matriz de todos los registros de un objeto de filtro especificado.	Puede realizar `eth_getloqs` solicitudes en cualquier rango de bloques con un rango de bloques de 1 000 por defecto si se proporcio na una dirección de contrato. Los contratos con alta actividad pueden estar limitados a rangos de bloques más pequeños. Si no se proporcio na la dirección del contrato, el rango de bloques será 8.
	eth_ getRawTransaction ByHash	Devuelve la forma bruta de la transacción especificada por. `transacti on_hash`	

Categoría	JSON-RPC	Descripción	Consideraciones
	eth_ getStorageAt	Devuelve el valor de la posición de almacenamiento especificada para la dirección de la cuenta y el identificador de bloque especificados.	
	eth_ getTransactionBy BlockHash AndIndex	Devuelve información sobre una transacción utilizando el hash de bloque especificado y la posición del índice de transacciones.	
	eth_ getTransactionBy BlockNumberAndIndex	Devuelve información sobre una transacción utilizando el número de bloque y la posición del índice de transacciones especificados.	
	eth_ Hash getTransactionBy	Devuelve información sobre la transacción con el hash de transacción especificado.	

Categoría	JSON-RPC	Descripción	Consideraciones
	eth_ getTransactionCount	Devuelve el número de transacciones enviadas desde la dirección y el identificador de bloque especific ados.	
	eth_ getTransactionReceipt	Devuelve el recibo de la transacción utilizando el hash de transacción especificado.	
	eth_ getUncleBy BlockHashAndIndex	Devuelve informaci ón sobre el bloque tío especificado mediante el hash del bloque y la posición del índice tío.	
	eth_ getUncleBy BlockNumberAndIndex	Devuelve informaci ón sobre el bloque tío especific ado mediante el número de bloque y la posición del tío en el índice.	

Categoría	JSON-RPC	Descripción	Consideraciones
	eth_ getUncleCount ByBlockHash	Devuelve el número de recuentos del tío especificado mediante el hash del tío.	
	eth_ getUncleCount ByBlockNumber	Devuelve el número de recuentos del tío especific ado mediante el número del tío.	
	eth_ maxPriorityFee PerGas	Devuelve la tarifa por gas, que es una estimación de cuánto puedes pagar como tarifa prioritaria, o «propina», para que una transacci ón se incluya en el bloque actual.	Por lo general, se utiliza el valor que se devuelve con este método para fijar el `maxFeePer Gas` importe de la siguiente transacci ón que se va a enviar.
	Versión de ETH_Protocol	Devuelve la versión actual del protocolo Ethereum.	

Categoría	JSON-RPC	Descripción	Consideraciones
	eth_ sendRawTransaction	Crea una nueva transacción de llamada de mensaje o una creación de contrato para las transacciones firmadas.	La cadena de bloques gestionada solo admite transacciones sin procesar. Debe crear y firmar las transacciones antes de enviarlas.
Debug	debug_ Hash traceBlockBy	Devuelve el posible número del resultado del rastreo ejecutando todas las transacciones del bloque especificado por el hash del bloque con un rastreador (se requiere el modo de rastreo).	
	debug_ Número traceBlockBy	Devuelve el resultado del rastreo ejecutando todas las transacciones del bloque especificado por número con un rastreador (se requiere el modo de rastreo).	

Categoría	JSON-RPC	Descripción	Consideraciones
	Debug_traceCall	Devuelve el número de posibles resultados de rastreo al ejecutar una llamada eth en el contexto de la ejecución del bloque dado (se requiere el modo de rastreo).	
	Debug_traceTransaction	Devuelve todos los rastros de una transacción determinada (se requiere el modo de rastreo).	
Net	net_version	Devuelve el identificador de red actual.	
Rastreo	trace_block	Devuelve un seguimiento completo de todos los códigos de operación invocados de todas las transacciones que se incluyeron en un bloque.	

Categoría	JSON-RPC	Descripción	Consideraciones
	trace_call	Devuelve el número de posibles resultados de rastreo al ejecutar una llamada eth en el contexto de la ejecución del bloque en cuestión (se requiere el modo de rastreo).	
	trace_transaction	Devuelve todos los rastros de una transacción determinada (se requiere el modo de rastreo).	
Tx Pool	txpool_content	Devuelve todas las transacciones pendientes y en cola.	

Categoría	JSON-RPC	Descripción	Consideraciones
	txpool_status	Proporciona un recuento de todas las transacci ones actualmen te pendientes de inclusión en los siguientes bloques y de las que están en cola (solo están programadas para su ejecución futura).	
Web	Web3_ClientVersion	Devuelve la versión actual del cliente.	

Casos de uso de Polygon con Amazon Managed Blockchain (AMB) Access Polygon

La cadena de bloques Polygon se usa comúnmente para crear aplicaciones descentralizadas (DApps) relacionadas con juegos Web3 y casos de uso de tokenización, entre otros. NFTs En este tema se proporciona una lista de algunos de los casos de uso que puede implementar con Amazon Managed Blockchain (AMB) Access Polygon.

Temas

- Analice los datos de NFT de Polygon
- Support NFT compras
- Crea un monedero Polygon
- El monedero como servicio
- Experiencias basadas en fichas

Analice los datos de NFT de Polygon

Puede recopilar datos sobre Polygon NFTs, incluida información como los eventos de transferencia y los metadatos de NFT durante un período específico. A continuación, puedes analizar estos datos para obtener información sobre cuáles NFTs son las tendencias o qué usuarios interactúan con más frecuencia con una colección determinada.

Para obtener más información, consulte La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon.

Support NFT compras

Puedes usar AMB Access Polygon para enviar transacciones de compras de NFT mediante acuñación inicial, listas de permitidos o en el mercado secundario. Al utilizar una combinación de otros AWS servicios, puedes permitir las compras con tarjetas de crédito, aceptando monedas fiduciarias o criptomonedas, con un rápido pago para todas las partes implicadas.

Para obtener más información, consulte La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon.

Crea un monedero Polygon

Puede utilizar AMB Access Polygon para realizar funciones esenciales de las carteras de activos digitales, como leer los saldos simbólicos de los usuarios a partir de contratos inteligentes en la cadena de bloques o transmitir transacciones firmadas a la cadena de bloques.

Para obtener más información, consulte La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon.

El monedero como servicio

Puede usar AMB Access Polygon para desarrollar una operación wallet-as-a-service necesaria para respaldar las transacciones de monedero más comunes, como la consulta de un saldo, la transferencia de activos, el envío de activos y las estimaciones de comisiones, utilizando el Polygon JSON- compatible. RPCs

Para obtener más información, consulte La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon.

Experiencias basadas en fichas

Puede usar AMB Access Polygon para crear experiencias protegidas por tokens para sus usuarios. Por ejemplo, puedes proporcionar acceso condicional a un contenido solo a los propietarios de un NFT específico. Para lograrlo, debes leer la cadena de bloques para determinar si el NFT es el propietario de la dirección de un usuario.

Para obtener más información, consulte La API de cadena de bloques gestionada y el JSON son RPCs compatibles con AMB Access Polygon.

Tutoriales sobre Amazon Managed Blockchain (AMB) Access Polygon

Los siguientes tutoriales destacados en esta sección son artículos de la comunidad AWS re:Post que proporcionan tutoriales que le ayudarán a aprender cómo realizar algunas tareas comunes en la cadena de bloques de Polygon utilizando AMB Access Polygon.

- Envío de transacciones mediante AMB Access Polygon y web3.js
- Implemente un contrato inteligente con AMB Access Polygon y Hardhat Ignition
- Interactuar con un contrato inteligente
- Recupere los datos de precios actuales fuera de la cadena utilizando las fuentes de datos AMB Access Polygon y Chainlink
- Analice los datos del token ERC-20 en la red principal de Polygon con AMB Access

Seguridad en el polígono de acceso a Amazon Managed Blockchain (AMB)

La seguridad en la nube AWS es de máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon Managed Blockchain (AMB) Access Polygon, consulte AWS Services in Scope by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Para proporcionar protección de datos, autenticación y control de acceso, Amazon Managed Blockchain utiliza AWS características y características del marco de código abierto que se ejecuta en Managed Blockchain.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar AMB Access Polygon. Los siguientes temas muestran cómo configurar AMB Access Polygon para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de AMB Access Polygon.

Temas

- Protección de datos en Amazon Managed Blockchain (AMB) Access Polygon
- Gestión de identidades y accesos para Amazon Managed Blockchain (AMB) Access Polygon

Protección de datos en Amazon Managed Blockchain (AMB) Access Polygon

El modelo de se aplica a protección de datos en Amazon Managed Blockchain (AMB) Access Polygon. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los. Nube de AWS Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AMB Access Polygon u otro Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

El cifrado de datos ayuda a evitar que usuarios no autorizados lean datos de una red blockchain y de los sistemas de almacenamiento de datos asociados. Esto incluye los datos que podrían interceptarse a medida que viajan por la red, lo que se conoce como datos en tránsito.

Cifrado en tránsito

De forma predeterminada, Managed Blockchain utiliza una conexión HTTPS/TLS para cifrar todos los datos que se transmiten desde un ordenador cliente que ejecuta los puntos finales del servicio. AWS CLI AWS

No es necesario hacer nada para habilitar el uso de HTTPS/TLS. Siempre está habilitada, a menos que la inhabilites explícitamente para un AWS CLI comando individual mediante el comando. `--no-verify-ssl`

Gestión de identidades y accesos para Amazon Managed Blockchain (AMB) Access Polygon

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de AMB Access Polygon. Puede utilizar IAM Servicio de AWS sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas

- Cómo funciona Amazon Managed Blockchain (AMB) Access Polygon con IAM
- Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)
- Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access Polygon

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AMB Access Polygon.

Usuario del servicio: si utiliza el servicio AMB Access Polygon para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AMB Access Polygon para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función de AMB Access Polygon, consulte. Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access Polygon

Administrador de servicios: si está a cargo de los recursos de AMB Access Polygon en su empresa, probablemente tenga acceso completo a AMB Access Polygon. Es su trabajo determinar a qué funciones y recursos de AMB Access Polygon deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AMB Access Polygon, consulte. Cómo funciona Amazon Managed Blockchain (AMB) Access Polygon con IAM

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a AMB Access Polygon. Para ver ejemplos de políticas basadas en la identidad de AMB Access Polygon que puede usar en IAM, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

Autenticación con identidades

La autenticación es la forma de iniciar sesión con sus credenciales de identidad AWS . Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario

a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon Managed Blockchain (AMB) Access Polygon con IAM

Antes de usar IAM para administrar el acceso a AMB Access Polygon, conozca qué funciones de IAM están disponibles para su uso con AMB Access Polygon.

Funciones de IAM que puede utilizar con Amazon Managed Blockchain (AMB) Access Polygon

Característica de IAM	Compatibilidad con AMB Access Polygon
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	No
Permisos de entidades principales	No

Característica de IAM	Compatibilidad con AMB Access Polygon
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo AMB Access Polygon y otros Servicios de AWS funcionan con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AMB Access Polygon

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para el polígono de acceso a AMB

Para ver ejemplos de políticas basadas en la identidad de AMB Access Polygon, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

Políticas basadas en recursos dentro de AMB Access Polygon

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las

políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para AMB Access Polygon

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones del polígono de acceso a AMB, consulte Acciones definidas por el polígono de acceso de Amazon Managed Blockchain (AMB) en la Referencia de autorización de servicios.

Las acciones políticas en AMB Access Polygon utilizan el siguiente prefijo antes de la acción:

```
managedblockchain:
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `InvokeRpcPolygon`, incluya la siguiente acción:

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

Para ver ejemplos de políticas basadas en la identidad de AMB Access Polygon, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

Recursos de políticas para AMB Access Polygon

Compatibilidad con recursos de políticas: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de AMB Access Polygon y sus correspondientes ARNs, consulte Resources Defined by Amazon Managed Blockchain (AMB) Access Polygon (AMB) en la

Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por el polígono de acceso a Amazon Managed Blockchain (AMB).

Para ver ejemplos de políticas basadas en la identidad de AMB Access Polygon, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

Claves de condición de la política para AMB Access Polygon

Compatibilidad con claves de condición de políticas específicas del servicio: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición del polígono de acceso a AMB, consulte Claves de condición del polígono de acceso a Amazon Managed Blockchain (AMB) en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Actions Defined by Amazon Managed Blockchain (AMB) Access Polygon.

Para ver ejemplos de políticas basadas en la identidad de AMB Access Polygon, consulte. Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

ACLs en AMB Access Polygon

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AMB Access Polygon

Compatibilidad con ABAC (etiquetas en las políticas): no

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AMB Access Polygon

Compatible con el uso de credenciales temporales: no

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para AMB Access Polygon

Compatibilidad con sesiones de acceso directo (FAS): no

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Funciones de servicio para AMB Access Polygon

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad del polígono de acceso de AMB. Edite las funciones de servicio solo cuando AMB Access Polygon le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para AMB Access Polygon

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para el polígono de acceso a Amazon Managed Blockchain (AMB)

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AMB Access Polygon. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AMB Access Polygon, incluido el formato de cada uno de los ARNs tipos de recursos, consulte Actions, Resources and Condition Keys for Amazon Managed Blockchain (AMB) Access Polygon (AMB) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola AMB Access Polygon
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceso a las redes de Polygon

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear los recursos de AMB Access Polygon de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola AMB Access Polygon

Para acceder a la consola de Access Polygon de Amazon Managed Blockchain (AMB), debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AMB Access Polygon que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola del polígono de acceso a la AMB, adjunte también el polígono de acceso a la AMB `ConsoleAccess` o la política `ReadOnly` AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
```

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

Acceso a las redes de Polygon

> **Note**
>
> Para acceder a los puntos finales públicos del polígono `mainnet` y realizar llamadas JSON-RPC, necesitará credenciales de usuario (`AWS_ACCESS_KEY_IDyAWS_SECRET_ACCESS_KEY`) disponer de los permisos de IAM adecuados `mainnet` para el polígono de acceso a AMB.

Example Política de IAM para acceder a todas las redes poligonales

En este ejemplo, se concede a un usuario de IAM el Cuenta de AWS acceso a todas las redes de Polygon.

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

Example Política de IAM para acceder a la red principal de Polygon

En este ejemplo, se concede a un usuario de IAM el Cuenta de AWS acceso a la red principal de Polygon.

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

Solución de problemas de identidad y acceso a Amazon Managed Blockchain (AMB) Access Polygon

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AMB Access Polygon e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AMB Access Polygon
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AMB Access Polygon

No estoy autorizado a realizar ninguna acción en AMB Access Polygon

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `managedblockchain::`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `managedblockchain::`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a AMB Access Polygon.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AMB Access Polygon. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AMB Access Polygon

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AMB Access Polygon admite estas funciones, consulte. Cómo funciona Amazon Managed Blockchain (AMB) Access Polygon con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro de eventos de Amazon Managed Blockchain (AMB) Access Polygon mediante AWS CloudTrail

> **Note**
> Amazon Managed Blockchain (AMB) Access Polygon no admite eventos de administración.

Se ejecuta Amazon Managed Blockchain AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Managed Blockchain. CloudTrail captura quién invocó los puntos finales del polígono de acceso AMB para Managed Blockchain como eventos del plano de datos.

Si crea un registro correctamente configurado que esté suscrito para recibir los eventos del plano de datos que desee, podrá recibir el envío continuo de los eventos relacionados con CloudTrail AMB Access Polygon a un bucket de S3. Con la información recopilada por ellos CloudTrail, puede determinar si se ha realizado una solicitud a uno de los puntos finales de AMB Access Polygon, la dirección IP de la que procede la solicitud, quién la ha realizado, cuándo se ha realizado y otros detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Información sobre AMB Access Polygon en CloudTrail

CloudTrail está activado en su dispositivo Cuenta de AWS cuando lo crea. Sin embargo, debe configurar los eventos del plano de datos para ver quién invocó los puntos finales de AMB Access Polygon.

Para obtener un registro continuo de los eventos de su entorno Cuenta de AWS, incluidos los eventos del AMB Access Polygon, cree un recorrido. Un rastro permite CloudTrail enviar archivos de registro a un depósito de S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro registra los eventos de todas las regiones compatibles en la AWS partición y envía los archivos de registro al depósito de S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para más información, consulte los siguientes temas:

- Se usa CloudTrail para rastrear Polygon JSON- RPCs
- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Al analizar los eventos de CloudTrail datos, puede controlar quién invocó los puntos finales de AMB Access Polygon.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM)
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o un usuario federado
- Si la solicitud la realizó otra persona Servicio de AWS

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas del archivo de registro de AMB Access Polygon

En el caso de los eventos del plano de datos, un registro es una configuración que permite la entrega de eventos como archivos de registro a un depósito de S3 específico. Cada archivo de CloudTrail registro contiene una o más entradas de registro que representan una única solicitud de cualquier fuente. Estas entradas proporcionan detalles sobre la acción solicitada, incluidas la fecha y la hora de la acción, y cualquier parámetro de solicitud asociado.

> **Note**
>
> CloudTrail Los eventos de datos de los archivos de registro no son un seguimiento de pila ordenado de las llamadas a la API de AMB Access Polygon, por lo que no aparecen en ningún orden específico.

Se usa CloudTrail para rastrear Polygon JSON- RPCs

Puede usarlo CloudTrail para rastrear quién en su cuenta invocó los puntos finales de AMB Access Polygon y qué JSON-RPC se invocó como eventos de datos. De forma predeterminada, al crear una ruta, los eventos de datos no se registran. Para registrar quién invocó los puntos finales del polígono de acceso de AMB como eventos de CloudTrail datos, debe añadir de forma explícita los recursos o tipos de recursos compatibles para los que desea recopilar la actividad en un sendero. AMB Access Polygon permite añadir eventos de datos mediante el uso de, y el AWS Management Console SDK. AWS CLIPara obtener más información, consulte Registrar eventos mediante selectores avanzados en la Guía del AWS CloudTrail usuario.

Para registrar los eventos de datos en una ruta, utilice la put-event-selectorsoperación después de crear la ruta. Utilice la `--advanced-event-selectors` opción para especificar los tipos de `AWS::ManagedBlockchain::Network` recursos para empezar a registrar los eventos de datos y determinar quién invocó los puntos finales del AMB Access Polygon.

Example Entrada en el registro de eventos de datos de todas las solicitudes de puntos finales de AMB Access Polygon de su cuenta

En el siguiente ejemplo, se muestra cómo utilizar la `put-event-selectors` operación para registrar todas las solicitudes de puntos finales de AMB Access Polygon de su cuenta para el sendero de la región. `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"] } ]}]'
```

Después de suscribirse, puede realizar un seguimiento del uso en el depósito de S3 que está conectado al sendero especificado en el ejemplo anterior.

El siguiente resultado muestra una entrada en el registro de eventos de CloudTrail datos con la información recopilada por CloudTrail. Puede determinar si se ha realizado una solicitud JSON-RPC de Polygon a uno de los puntos finales de AMB Access Polygon, la dirección IP de la que procede la solicitud, quién la ha realizado, cuándo se ha realizado y otros detalles adicionales. Algunos valores

del siguiente ejemplo se han ocultado por motivos de seguridad, pero aparecen completamente en las entradas de registro reales.


```
{
        "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"
}
```

Historial de documentos de la Guía del usuario de AMB Access Polygon

En la siguiente tabla se describen las versiones de documentación de AMB Access Polygon.

Cambio	Descripción	Fecha
Cuotas actualizadas para JSON-RPC	Se actualizan las cuotas que AMB Access Polygon admite para cada JSON-RPC compatible.	12 de abril de 2024
Fin del soporte para la red de redes de prueba de Mumbai	AMB Access Polygon dejó de ofrecer soporte a la red de pruebas de Bombay el 15 de abril de 2024.	10 de abril de 2024
Adición del tema Tutoriales	Tutoriales de AMB Access Polygon de la sección de artículos de la comunidad de AWS Re:post.	9 de abril de 2024
Vista previa pública	Versión preliminar pública del servicio Amazon Managed Blockchain (AMB) Access Polygon.	24 de noviembre de 2023