aws

Guide du développeur

Polygone d'accès AMB

Polygone d'accès AMB: Guide du développeur

Table of Contents

Amazon Managed Blockchain (AMB) Access Polygon est en version préliminaire et est susceptible d'être modifié.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.

Qu'est-ce que le polygone d'accès Amazon Managed Blockchain (AMB) ?

Amazon Managed Blockchain (AMB) Access Polygon est un service entièrement géré qui vous aide à créer des applications Web3 résilientes sur la blockchain Polygon. AMB Access Polygon fournit un accès instantané et sans serveur à la blockchain Polygon.

Polygon est une solution de mise à l'échelle qui utilise la machine virtuelle Ethereum (EVM) comme base. La blockchain Polygon est connue pour son débit de transactions élevé et ses faibles frais de transaction. La blockchain Polygon utilise un mécanisme de proof-of-stake consensus. Le polygone est couramment utilisé dans la création d'applications décentralisées (DApps) liées aux NFT, aux jeux Web3 et aux cas d'utilisation de tokenisation, entre autres.

Ce guide explique comment créer et gérer des ressources de blockchain Polygon à l'aide d'Amazon Managed Blockchain (AMB) Access Polygon.

Ressources pour les nouveaux utilisateurs d'AMB Access Polygon

Si c'est la première fois que vous utilisez AMB Access Polygon, nous vous recommandons de commencer par lire les sections suivantes :

- Concepts clés : polygone d'accès Amazon Managed Blockchain (AMB)
- Commencer à utiliser Amazon Managed Blockchain (AMB) Access Polygon
- L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon

Concepts clés : polygone d'accès Amazon Managed Blockchain (AMB)

> **Note**
>
> Ce guide part du principe que vous connaissez les concepts essentiels à Polygon. Ces concepts incluent le staking, les dApps, les transactions, les portefeuilles, les contrats intelligents, Polygon (POL, anciennement MATIC), etc. Avant d'utiliser Amazon Managed Blockchain (AMB) Access Polygon, nous vous recommandons de consulter la documentation de développement de Polygon et le wiki Polygon.

Amazon Managed Blockchain (AMB) Access Polygon vous fournit un accès sans serveur aux réseaux Polygon Mainnet et Polygon Mainnet, sans que vous ayez à provisionner et à gérer une infrastructure Polygon, y compris les nœuds. Les nœuds polygonaux d'un réseau stockent collectivement l'état d'une chaîne de blocs polygonaux, vérifient les transactions et participent à un consensus pour modifier l'état d'une chaîne de blocs. Vous pouvez utiliser ce service géré pour accéder aux réseaux Polygon rapidement et à la demande, réduisant ainsi votre coût global de propriété.

Avec AMB Access Polygon, vous avez accès aux appels JSON Remote Procedure (JSON-RPC). Vous pouvez invoquer Polygon JSON-RPC pour communiquer avec la blockchain Polygon via des nœuds gérés par Managed Blockchain. Vous pouvez utiliser le service AMB Access Polygon pour développer et utiliser des applications décentralisées (DApps) qui interagissent avec la blockchain Polygon. Les contrats intelligents font partie intégrante des DApps. Vous pouvez créer et déployer des contrats intelligents dans la blockchain Polygon à l'aide d'AMB Access Polygon. Vous pouvez également vérifier le solde de vos portefeuilles, les détails des transactions, estimer les frais, etc., en invoquant des JSON-RPC contre des points de terminaison AMB Access Polygon qui s'exécutent de manière décentralisée sur tous les nœuds homologues du réseau Polygon. Tout homologue du réseau Polygon peut développer et déployer un contrat intelligent.

> **Important**
>
> Vous êtes responsable de la création, de la maintenance, de l'utilisation et de la gestion de vos adresses Polygon. Vous êtes également responsable du contenu de vos adresses

Polygon. AWS n'est pas responsable des transactions déployées ou appelées à l'aide de nœuds Polygon sur Amazon Managed Blockchain.

Considérations et limites relatives à l'utilisation du polygone d'accès Amazon Managed Blockchain (AMB)

Lorsque vous utilisez le polygone d'accès Amazon Managed Blockchain (AMB), tenez compte des points suivants :

- Réseaux polygonaux pris en charge

  AMB Access Polygon prend en charge les réseaux publics suivants :

  - Réseau principal : chaîne de blocs Polygon publique sécurisée par proof-of-stake consensus et sur laquelle le jeton Polygon (POL) est émis et traité. Les transactions sur Mainnet ont une valeur réelle (c'est-à-dire qu'elles entraînent des coûts réels) et sont enregistrées sur la blockchain publique.

- Les réseaux ne sont plus pris en charge par Polygon

  - Comme indiqué par Polygon Labs, le réseau Mumbai Testnet cessera ses activités à la mi-avril. Conformément à cette nouvelle, AMB Access Polygon a mis fin au support du Mumbai Testnet le 15 avril 2024. Nous vous recommandons d'utiliser Amoy Testnet pour votre charge de travail de test.
  - Les réseaux privés ne sont pas pris en charge.
  - De plus, AMB Access Polygon ne prend pas en charge le réseau Polygon zKevM.

- Compatibilité avec les bibliothèques de programmation tierces les plus populaires

  AMB Access Polygon est compatible avec les bibliothèques de programmation populaires, telles que ethers.js, permettant aux développeurs d'interagir avec la blockchain Polygon à l'aide d'outils familiers pour s'intégrer facilement à leurs implémentations existantes ou développer rapidement de nouvelles applications.

- Régions prises en charge

  Ce service est pris en charge uniquement dans la région de l'est des États-Unis (Virginie du Nord).

- Points de terminaison de service

Voici les points de terminaison de service pour AMB Access Polygon. Pour vous connecter au service, vous devez utiliser un point de terminaison qui inclut l'une des régions prises en charge.

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

- Le staking n'est pas pris en charge

  AMB Access Polygon ne prend pas en charge les nœuds de validation Polygon (POL) pour. proof-of-stake

- Signature Version 4 : signature des requêtes Polygon JSON-RPC

  Lorsque vous appelez le Polygon JSON-RPC sur Amazon Managed Blockchain, vous pouvez le faire via une connexion HTTPS authentifiée à l'aide du processus de signature Signature Version 4. Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent effectuer des appels Polygon JSON-RPC. Pour ce faire, des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) doivent être fournies avec l'appel.

  > ⚠ Important
  >
  > - N'intégrez pas les informations d'identification du client dans les applications destinées aux utilisateurs.
  > - Vous ne pouvez pas utiliser les politiques IAM pour restreindre l'accès à des polygones JSON-RPC individuels.

- Support pour l'accès basé sur des jetons

  Vous pouvez également utiliser les jetons Accessor pour effectuer des appels JSON-RPC vers les points de terminaison du réseau Polygon comme alternative pratique au processus de signature de la version 4 (Sigv4). Vous devez fournir un `BILLING_TOKEN` des jetons Accessor que vous créez et ajoutez en tant que paramètre avec vos appels.

  > ⚠ Important
  >
  > - Si vous privilégiez la sécurité et l'auditabilité à la commodité, utilisez plutôt le processus de signature SigV4.
  > - Vous pouvez accéder aux polygones JSON-RPC à l'aide de la version de signature 4 (Sigv4) et d'un accès basé sur des jetons. Toutefois, si vous choisissez d'utiliser les deux protocoles, votre demande est rejetée.

- Vous ne devez jamais intégrer de jetons Accessor dans des applications destinées aux utilisateurs.

- Seules les soumissions de transactions brutes sont prises en charge

  Utilisez le `eth_sendrawtransaction` JSON-RPC pour soumettre des transactions qui mettent à jour l'état de la blockchain Polygon.

Configuration du polygone d'accès Amazon Managed Blockchain (AMB)

Avant d'utiliser le polygone d'accès Amazon Managed Blockchain (AMB) pour la première fois, suivez les étapes décrites dans cette section pour créer un. Compte AWS Le chapitre suivant explique comment commencer à utiliser AMB Access Polygon.

Conditions préalables à l'utilisation d'AMB Access Polygon

Avant de l'utiliser AWS pour la première fois, vous devez disposer d'un Compte AWS.

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez AWS, vous êtes automatiquement Compte AWS inscrit à tous Services AWS, y compris Amazon Managed Blockchain (AMB) Access Polygon. Seuls les services que vous utilisez vous sont facturés.

Si vous en avez Compte AWS déjà un, passez à l'étape suivante. Si vous n'avez pas de Compte AWS, utilisez la procédure suivante pour en créer un.

Pour créer un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Création d'un utilisateur IAM avec les autorisations appropriées

Pour créer et utiliser AMB Access Polygon, vous devez disposer d'un principal AWS Identity and Access Management (IAM) (utilisateur ou groupe) doté des autorisations autorisant les actions nécessaires à Managed Blockchain.

Lorsque vous appelez le Polygon JSON-RPC sur Amazon Managed Blockchain, vous pouvez le faire via une connexion HTTPS authentifiée à l'aide du processus de signature Signature Version 4. Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent effectuer des appels Polygon JSON-RPC. Pour ce faire, des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) doivent être fournies avec l'appel.

Vous pouvez également utiliser les jetons Accessor pour effectuer des appels JSON-RPC vers les points de terminaison du réseau Polygon comme alternative pratique au processus de signature de la version 4 (Sigv4). Vous devez fournir un `BILLING_TOKEN` des jetons Accessor que vous créez et ajoutez en tant que paramètre avec vos appels. Cependant, vous avez toujours besoin d'un accès IAM pour obtenir les autorisations nécessaires pour créer des jetons d'accès à l'aide du kit de développement logiciel (SDK) et du kit de AWS Management Console développement logiciel (AWS CLI SDK).

Pour plus d'informations sur la création d'un utilisateur IAM, consultez la section Création d'un utilisateur IAM dans votre AWS compte. Pour plus d'informations sur la façon d'associer une politique d'autorisations à un utilisateur, consultez la section Modification des autorisations d'un utilisateur IAM. Pour un exemple de politique d'autorisation que vous pouvez utiliser pour autoriser un utilisateur à utiliser AMB Access Polygon, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Installation et configuration de l' AWS Command Line Interface

Si ce n'est pas déjà fait, installez latest AWS Command Line Interface (AWS CLI) pour utiliser les AWS ressources d'un terminal. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.

> **Note**
>
> Pour accéder à la CLI, vous avez besoin d'un ID de clé d'accès et d'une clé d'accès secrète. Utilisation des informations d'identification temporaires au lieu des clés d'accès à long terme si possible. Les informations d'identification temporaires incluent un ID de clé d'accès, une

clé d'accès secrète et un jeton de sécurité qui indique la date d'expiration des informations d'identification. Pour plus d'informations, consultez la section Utilisation d'informations d'identification temporaires avec AWS des ressources dans le Guide de l'utilisateur IAM.

Commencer à utiliser Amazon Managed Blockchain (AMB) Access Polygon

Commencez à utiliser Amazon Managed Blockchain (AMB) Access Polygon en utilisant les informations et les procédures décrites dans cette section.

Rubriques

Créez une politique IAM pour accéder au réseau de blockchain Polygon

Pour accéder au point de terminaison public du réseau principal Polygon afin de passer des appels JSON-RPC, vous devez disposer des informations d'identification utilisateur (`AWS_ACCESS_KEY_IDetAWS_SECRET_ACCESS_KEY`) des autorisations IAM appropriées pour Amazon Managed Blockchain (AMB) Access Polygon. Dans un terminal sur lequel le est AWS CLI installé, exécutez la commande suivante pour créer une politique IAM permettant d'accéder aux deux points de terminaison Polygon :

```
cat <<EOT > ~/amb-polygon-access-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AMBPolygonAccessPolicy",
            "Effect": "Allow",
            "Action": [
                "managedblockchain:InvokeRpcPolygon*"
            ],
            "Resource": "*"
        }
```

```
    ]
}
EOT
aws iam create-policy --policy-name AmazonManagedBlockchainPolygonAccess --policy-
document file://$HOME/amb-polygon-access-policy.json
```

> **Note**
>
> L'exemple précédent vous donne accès à tous les réseaux Polygon disponibles. Pour accéder à un point de terminaison spécifique, utilisez la `Action` commande suivante :
>
> - `"managedblockchain:InvokeRpcPolygonMainnet"`

Après avoir créé la stratégie, associez-la au rôle de votre utilisateur IAM pour qu'elle prenne effet. Dans le AWS Management Console, accédez au service IAM et attachez la politique `AmazonManagedBlockchainPolygonAccess` au rôle attribué à votre utilisateur IAM.

Effectuez des demandes d'appel de procédure à distance (RPC) Polygon sur l'éditeur RPC AMB Access à l'aide du AWS Management Console

Vous pouvez modifier, configurer et soumettre des appels de procédure à distance (RPC) sur le polygone AWS Management Console d'accès AMB. Avec ces RPC, vous pouvez lire des données et écrire des transactions sur le réseau Polygon, notamment récupérer des données et soumettre des transactions au réseau Polygon.

Example

L'exemple suivant montre comment obtenir des informations sur le dernier bloc à l'aide du `eth_getBlockByNumber` RPC. Remplacez les variables surlignées par vos propres entrées ou choisissez l'une des méthodes RPC répertoriées et entrez les entrées pertinentes requises.

1. Ouvrez la console Managed Blockchain à l'adresse https://console.aws.amazon.com/managedblockchain/.
2. Choisissez l'éditeur RPC.

3. Dans la section Requête, choisissez *POLYGON_MAINNET* comme ***réseau Blockchain***.
4. Choisissez *eth_getBlockByNumber* comme méthode RPC.
5. Entrez **latest** comme ***numéro de bloc*** et choisissez *False* comme indicateur de transaction complète.
6. Choisissez ensuite Soumettre le RPC.
7. Vous pouvez obtenir les résultats du `latest` bloc dans la section Réponse. Vous pouvez ensuite copier les transactions brutes complètes pour une analyse plus approfondie ou pour les utiliser dans la logique métier de vos applications.

Pour plus d'informations, consultez les RPC pris en charge par AMB Access Polygon

Effectuez des requêtes JSON-RPC du polygone d'accès AMB à l'aide du **`awscurl`**AWS CLI

Example

Signez les demandes avec vos informations d'identification utilisateur IAM en utilisant Signature Version 4 (SigV4) afin d'envoyer des requêtes Polygon JSON-RPC aux points de terminaison AMB Access Polygon. L'outil de ligne de `awscurl`commande peut vous aider à signer des demandes adressées à des AWS services à l'aide de SigV4. Pour plus d'informations, consultez le fichier readme.md d'awscurl.

Effectuez l'installation `awscurl` en utilisant la méthode adaptée à votre système d'exploitation. Sur macOS, l'application recommandée HomeBrew est-elle la suivante :

```
brew install awscurl
```

Si vous l'avez déjà installé et configuré AWS CLI, vos informations d'identification d'utilisateur IAM et les informations par défaut Région AWS sont définies dans votre environnement et vous avez accès à`awscurl`. À l'aide de`awscurl`, soumettez une demande au réseau principal de Polygon en invoquant le RPC. `eth_getBlockByNumber` Cet appel accepte un paramètre de chaîne correspondant au numéro de bloc pour lequel vous souhaitez récupérer des informations.

La commande suivante extrait les données de bloc du réseau principal Polygon en utilisant le numéro de bloc dans le `params` tableau pour sélectionner le bloc spécifique pour lequel récupérer les en-têtes.

```
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**
>
> Vous pouvez également effectuer cette même demande en utilisant la fonctionnalité `curl` d'accès basée sur les jetons AMB Access à l'aide de `Accessor` jetons. Pour plus d'informations, consultez Création et gestion de jetons Accessor pour un accès basé sur des jetons afin de faire des demandes 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 réponse de l'une ou l'autre commande renvoie des informations sur le dernier bloc. Consultez l'exemple suivant à des fins d'illustration :

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

 "parentHash":"0x27d47bc2c47a6d329eb8aa62c1353f60e138fb0c596e3e8e9425de163afd6dec",

 "receiptsRoot":"0x394da96025e51cc69bbe3644bc4e1302942c2a6ca6bf0cf241a5724c74c063fd",

 "sha3Uncles":"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
      "size":"0xbd6b",
      "stateRoot":"0x7ca9363cfe9baf4d1c0dca3159461b2cca8604394e69b30af05d7d5c1beea6c3",
      "timestamp":"0x653ff542",
```

```
      "totalDifficulty":"0x33eb01dd","transactions":[...],

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

Effectuer des requêtes Polygon JSON-RPC dans Node.js

Vous pouvez invoquer Polygon JSON-RPC en soumettant des demandes signées via HTTPS pour accéder au réseau Polygon Mainnet à l'aide du module https natif dans Node.js, ou vous pouvez utiliser une bibliothèque tierce telle qu'AXIOS. Les exemples Node.js suivants vous montrent comment envoyer des requêtes Polygon JSON-RPC au point de terminaison AMB Access Polygon en utilisant à la fois Signature Version 4 (SigV4) et un accès basé sur des jetons. Le premier exemple envoie une transaction d'une adresse à une autre et l'exemple suivant demande les détails de la transaction et les informations de solde à la blockchain.

Example

Pour exécuter cet exemple de script Node.js, appliquez les conditions préalables suivantes :

1. Le gestionnaire de version de nœud (nvm) et Node.js doivent être installés sur votre machine. Vous trouverez les instructions d'installation pour votre système d'exploitation ici.
2. Utilisez la `node --version` commande et confirmez que vous utilisez la version 18 ou supérieure de Node. Si nécessaire, vous pouvez utiliser la `nvm install v18.12.0` commande, suivie de la `nvm use v18.12.0` commande, pour installer la version 18, la version LTS de Node.
3. Les variables `AWS_ACCESS_KEY_ID` d'environnement `AWS_SECRET_ACCESS_KEY` doivent contenir les informations d'identification associées à votre compte.

   Exportez ces variables sous forme de chaînes sur votre client à l'aide des commandes suivantes. Remplacez les valeurs en rouge dans les chaînes suivantes par les valeurs appropriées de votre compte utilisateur IAM.

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

Après avoir rempli toutes les conditions requises, copiez les fichiers suivants dans un répertoire de votre environnement local à l'aide de votre éditeur de code préféré :

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**
>
> Le code suivant utilise une clé privée codée en dur pour générer un portefeuille que Signer utilise `Ethers.js` à des fins de démonstration uniquement. N'utilisez pas ce code dans des environnements de production, car il dispose de fonds réels et présente un risque de sécurité. Si nécessaire, contactez l'équipe chargée de votre compte pour obtenir des conseils sur les meilleures pratiques en matière de portefeuille et de signature.

```
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");
```

Une fois ces fichiers enregistrés dans votre répertoire, installez les dépendances requises pour exécuter le code à l'aide de la commande suivante :

```
npm install
```

Envoyer une transaction dans Node.js

L'exemple précédent envoie le jeton Polygon Mainnet (POL) natif d'une adresse à une autre en signant une transaction et en le diffusant sur le Polygon Mainnet à l'aide d'AMB Access Polygon. Pour ce faire, utilisez le `sendTx.js` script, qui utilise `Ethers.js` une bibliothèque populaire pour interagir avec Ethereum et des blockchains compatibles avec Ethereum comme Polygon. Vous devez remplacer trois variables dans le code surlignées en rouge, notamment le `billingToken` jeton Accessor pour un accès basé sur un jeton, la clé privée avec laquelle vous signez la transaction et l'adresse du destinataire qui reçoit le POL.

> **Tip**
>
> Nous vous recommandons de créer une nouvelle clé privée (portefeuille) à cette fin plutôt que de réutiliser un portefeuille existant afin d'éliminer le risque de perte de fonds. Vous pouvez utiliser la méthode de classe Wallet createRandom () de la bibliothèque Ethers pour générer un portefeuille à tester. De plus, si vous devez demander du POL au réseau principal Polygon, vous pouvez utiliser le robinet POL public pour demander une petite quantité à utiliser pour les tests.

Une fois que votre clé privée *`billingToken`*, celle d'un portefeuille approvisionné, et l'adresse du destinataire ont été ajoutées au code, vous devez exécuter le code suivant pour signer une transaction pour un POL de .0001 à envoyer de votre adresse à une autre et le diffuser sur le réseau principal de Polygon en invoquant le `eth_sendRawTransaction` JSON-RPC à l'aide du polygone d'accès AMB.

```
node sendTx.js
```

La réponse reçue ressemble à ce qui suit :

```
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 réponse constitue le reçu de transaction. Enregistrez la valeur de la propriété`hash`. Il s'agit de l'identifiant de la transaction que vous venez de soumettre à la blockchain. Vous utilisez cette propriété dans l'exemple de transaction de lecture pour obtenir des informations supplémentaires sur cette transaction à partir du réseau principal de Polygon.

Notez que les `blockNumber` et `blockHash` se trouvent `null` dans la réponse. Cela est dû au fait que la transaction n'a pas encore été enregistrée dans un bloc sur le réseau Polygon. Notez que ces valeurs sont définies ultérieurement et que vous pouvez les voir lorsque vous demandez les détails de la transaction dans la section suivante.

Lire une transaction dans Node.js

Dans cette section, vous demandez les détails de la transaction précédemment soumise et vous récupérez le solde POL pour l'adresse du destinataire à l'aide de demandes de lecture adressées au réseau principal Polygon à l'aide d'AMB Access Polygon. Dans le `readTx.js` fichier, remplacez la variable *`your-transaction-id`*étiquetée par celle `hash` que vous avez enregistrée à partir de la réponse à l'exécution du code de la section précédente.

Ce code utilise un utilitaire qui signe les requêtes HTTPS à AMB Access Polygon avec les modules Signature Version 4 (SigV4) requis du AWS SDK et envoie les demandes à l'aide du client HTTP largement utilisé, AXIOS. `dispatch-evm-rpc.js`

La réponse reçue ressemble à ce qui suit :

```
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 réponse représente les détails de la transaction. Notez que les `blockHash` et `blockNumber` sont désormais probablement définis. Cela indique que la transaction a été enregistrée dans un bloc. Si ces valeurs sont inchangéesnull, attendez quelques minutes, puis réexécutez le code pour vérifier si votre transaction a été incluse dans un bloc. Enfin, la représentation hexadécimale du solde d'adresses du destinataire (0x110d9316ec000) est convertie en décimal à l'aide de la `formatEther()` méthode d'Ethers, qui convertit l'hexadécimal en décimal et décale les décimales de 18 (10^18) pour obtenir le véritable équilibre dans POL.

> **Tip**
>
> Bien que les exemples de code précédents illustrent comment utiliser Node.js, Ethers et Axios pour utiliser certains des JSON-RPC pris en charge sur AMB Access Polygon, vous pouvez modifier les exemples et écrire d'autres codes pour créer vos applications sur Polygon à l'aide de ce service. Pour une liste complète des JSON-RPC pris en charge sur AMB Access Polygon, voir. L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon

Création et gestion de jetons Accessor pour un accès basé sur des jetons afin de faire des demandes AMB Access Polygon

Vous pouvez également utiliser les jetons Accessor pour effectuer des appels JSON-RPC vers les points de terminaison du réseau Polygon comme alternative pratique au processus de signature de la version 4 (Sigv4). Vous devez fournir un `BILLING_TOKEN` des jetons Accessor que vous créez et ajoutez en tant que paramètre avec vos appels.

> ⚠ Important
>
> - Si vous privilégiez la sécurité et l'auditabilité à la commodité, utilisez plutôt le processus de signature SigV4.
> - Vous pouvez accéder aux polygones JSON-RPC à l'aide de la version de signature 4 (Sigv4) et d'un accès basé sur des jetons. Toutefois, si vous choisissez d'utiliser les deux protocoles, votre demande est rejetée.
> - Vous ne devez jamais intégrer de jetons Accessor dans des applications destinées aux utilisateurs.

Dans la console, la page Token Accessors affiche une liste de tous les jetons Accessor que vous pouvez utiliser pour effectuer des appels JSON-RPC AMB Access Polygon à partir de votre code from sur un client. Compte AWS

Pour plus d'informations sur les requêtes JSON-RPC AMB Access Polygon, consultez. L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon

Vous pouvez créer et gérer des jetons Accessor à l'aide du AWS Management Console. Vous pouvez également créer et gérer des jetons Accessor à l'aide des opérations d'API suivantes : `CreateAccessor` `GetAccessor`,`ListAccessors`, et `DeleteAccessor`. A `BILLING_TOKEN` est une propriété de l'Accessor. Cette `BILLING_TOKEN` propriété est utilisée pour suivre votre accesseur et pour facturer les demandes AMB Access Polygon JSON-RPC effectuées depuis votre. Compte AWS

Toutes les actions d'API liées à la création et à la gestion des jetons Accessor sont également disponibles via AWS Management Console AWS CLI les SDK et.

Création d'un jeton d'accès pour un accès basé sur un jeton

Vous pouvez créer un jeton d'accès et l'utiliser pour effectuer des appels à l'API AMB Access Polygon sur n'importe quel nœud AMB Access Polygon de votre. Compte AWS

Créez un jeton d'accès pour effectuer des requêtes JSON-RPC AMB Access Polygon à l'aide du AWS Management Console

1. Ouvrez la console Managed Blockchain à l'adresse https://console.aws.amazon.com/managedblockchain/.
2. Choisissez Token Accessors.
3. Choisissez Create Accessor.
4. Choisissez un réseau de blockchain Polygon valide.
5. Facultatif, ajoutez des tags pour votre accesseur.
6. Choisissez Create Accessor pour créer un nouveau jeton Accessor.

Créez un jeton d'accès pour effectuer des requêtes JSON-RPC AMB Access Polygon à l'aide du AWS CLI

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

La commande précédente renvoie le `AccessorId` ainsi que le`BillingToken`, comme indiqué dans l'exemple suivant.

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

L'élément clé de votre réponse est le`BillingToken`. Vous pouvez utiliser cette propriété pour effectuer des appels JSON-RPC AMB Access Polygon. Certaines valeurs de l'exemple ont été masquées pour des raisons de sécurité mais apparaîtront pleinement dans les réponses réelles.

> **Note**
>
> Une fois l'opération exécutée, Managed Blockchain approvisionne et configure le jeton pour vous. La durée de ce processus dépend de nombreuses variables.

Afficher les détails d'un jeton d'accès

Vous pouvez consulter les propriétés de chaque jeton d'accès que vous possédez Compte AWS . Par exemple, vous pouvez consulter l'identifiant ou le nom de ressource Amazon (ARN) de l'accédant. Vous pouvez également afficher le statut, le type, la date de création et le`BillingToken`.

Pour consulter les informations d'un jeton d'accès à l'aide du AWS Management Console

1. Ouvrez la console Managed Blockchain à l'adresse https://console.aws.amazon.com/managedblockchain/.
2. Dans le volet de navigation, choisissez Token Accessors.
3. Choisissez l'ID d'accès du jeton dans la liste.

La page de détails du jeton apparaît alors. Sur cette page, vous pouvez consulter les propriétés du jeton.

Pour consulter les informations d'un jeton d'accès à l'aide du AWS CLI

Exécutez la commande suivante pour afficher les détails d'un jeton d'accès. Remplacez les valeurs de `--accessor-id` par votre identifiant d'accès.

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

Les propriétés clés `BillingToken` et les autres propriétés sont renvoyées comme indiqué dans l'exemple suivant. Certaines valeurs de l'exemple ont été masquées pour des raisons de sécurité mais apparaissent pleinement dans les réponses réelles.

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

Supprimer un jeton d'accès

Lorsque vous supprimez un jeton d'accès, le jeton passe de l'`PENDING_DELETION`état `AVAILABLE` au. Vous ne pouvez pas utiliser un jeton d'accès avec le `PENDING_DELETION` statut.

Pour supprimer un jeton d'accès à l'aide du AWS Management Console

1. Ouvrez la console Managed Blockchain à l'adresse https://console.aws.amazon.com/managedblockchain/.
2. Dans le volet de navigation, choisissez Token Accessors.
3. Sélectionnez le jeton d'accès que vous souhaitez dans la liste.
4. Sélectionnez Delete (Supprimer).
5. Confirmez votre choix.

Vous êtes renvoyé à la page des accesseurs de jetons avec votre jeton d'accès supprimé. La page affiche le `PENDING_DELETION` statut.

Pour supprimer un jeton d'accès à l'aide du AWS CLI

L'exemple suivant montre comment supprimer un jeton. Utilisez la `delete-accessor` commande pour supprimer un jeton. Définissez la valeur de `--accessor-id` avec votre identifiant d'accès.

Suppression d'un jeton d'accès à l'aide de la CLI AWS

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

Si cette commande s'exécute correctement, aucun message n'est renvoyé.

L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon

Amazon Managed Blockchain fournit des opérations d'API pour créer et gérer des accesseurs de jetons pour AMB Access Polygon. Pour plus d'informations, consultez le guide de référence de l'API Managed Blockchain.

La rubrique suivante fournit une liste et une référence des polygones JSON-RPC pris en charge par AMB Access Polygon. Chaque JSON-RPC pris en charge est accompagné d'une brève description de son utilisation. Vous utilisez le Polygon JSON-RPC pour interroger et obtenir des données de contrats intelligents, obtenir les détails des transactions, soumettre des transactions et d'autres utilitaires tels que le suivi des transactions et l'estimation des frais.

AMB Access Polygon prend en charge les méthodes JSON-RPC suivantes. Chaque JSON-RPC pris en charge possède une catégorie et une brève description de son utilité et de ses quotas de requêtes par défaut. Les considérations uniques relatives à l'utilisation de la méthode JSON-RPC avec Amazon Managed Blockchain sont indiquées le cas échéant.

Note

- Les méthodes non répertoriées ne sont pas prises en charge.
- Lorsque vous appelez le Polygon JSON-RPC sur Amazon Managed Blockchain, vous pouvez le faire via une connexion HTTPS authentifiée à l'aide du processus de signature Signature Version 4. Cela signifie que seuls les principaux IAM autorisés du AWS compte peuvent effectuer des appels Polygon JSON-RPC. Pour ce faire, des AWS informations d'identification (un identifiant de clé d'accès et une clé d'accès secrète) doivent être fournies avec l'appel.
- Vous pouvez également utiliser l'accès basé sur des jetons comme alternative pratique au processus de signature Signature Version 4 (SigV4). Si vous privilégiez la sécurité et l'auditabilité à la commodité, utilisez plutôt le processus de signature SigV4. Toutefois, si vous utilisez à la fois le protocole SigV4 et l'accès basé sur des jetons, vos demandes ne fonctionneront pas.
- Les demandes par lots JSON-RPC ne sont pas prises en charge sur Amazon Managed Blockchain (AMB) Access Polygon pour cette version préliminaire.

- La colonne Quotas du tableau suivant répertorie le quota pour chaque JSON-RPC. Les quotas sont définis en demandes par seconde (RPS) par région et par réseau polygonal (réseau principal) pour chaque JSON-RPC.

  Pour augmenter votre quota, vous devez contacter AWS Support. Pour contacter AWS Support, connectez-vous au AWS Support Center Console. Choisissez Create case (Créer une demande). Choisissez Technique. Choisissez Managed Blockchain comme service. Choisissez Access:Polygon comme catégorie et Directives générales comme niveau de gravité. Entrez RPC Quota comme objet et dans la zone de texte Description, listez le JSON-RPC et les limites de quota applicables à vos besoins en RPS par réseau polygonal par région. Soumettez votre dossier.

Catégorie	JSON-RPC	Description	Considérations
Ethereum	ETH_Block Number	Renvoie le numéro du bloc le plus récent.	
	eth_call	Exécute immédiatement un nouveau message sans créer de transaction sur la blockchain.	`eth_call`consomme 0 gaz, mais possède un paramètre de gaz pour les messages qui le nécessitent.
	ETH_ChainID	Renvoie une valeur entière pour la `Chain Id` valeur actuellement configurée qui est introduite dans EIP-155. Retourne `None` si aucun n'`Chain Id`est disponible.	

Catégorie	JSON-RPC	Description	Considérations
	ETH_EstimateGas	Estime et renvoie le gaz nécessaire à une transaction sans ajouter la transaction à la blockchain.	
	Historique de ETH_FEE	Renvoie un ensemble d'informations historiques sur le gaz.	
	Prix ETH_Gas	Renvoie le prix actuel de l'essence en Wei.	
	ETH_GetBalance	Renvoie le solde d'un compte pour l'adresse de compte et l'identifiant de bloc spécifiés.	
	Hachage eth_get BlockBy	Renvoie des informations sur le bloc spécifié à l'aide du hachage du bloc.	
	Numéro eth_get BlockBy	Renvoie des informations sur le bloc spécifié à l'aide du numéro de bloc.	

Catégorie	JSON-RPC	Description	Considérations
	eth_get BlockReceipts	Renvoie les reçus relatifs au bloc spécifié à l'aide du numéro de bloc.	
	Hachage eth_get BlockTransaction CountBy	Renvoie le nombre de transactions dans le bloc spécifié à l'aide du hachage du bloc.	
	Numéro eth_get BlockTransaction CountBy	Renvoie le nombre de transactions dans le bloc spécifié à l'aide du numéro de bloc.	
	ETH_GetCode	Renvoie le code à l'adresse du compte et à l'identifiant de bloc spécifiés.	

Catégorie	JSON-RPC	Description	Considérations
	ETH_GetLogs	Renvoie un tableau de tous les journaux pour un objet de filtre spécifié.	Vous pouvez faire des `eth_getlogs` demandes sur n'importe quelle plage de blocs d'une plage de 1 000 blocs par défaut lorsqu'une adresse de contrat est fournie. Les contrats à forte activité peuvent être limités à des plages de blocs plus petites. Si aucune adresse de contrat n'est fournie, la plage de blocs sera de 8.
	eth_get RawTransaction ByHash	Renvoie la forme brute de la transaction spécifiée par le`transaction_hash` .	
	eth_get StorageAt	Renvoie la valeur de la position de stockage spécifiée pour l'adresse de compte et l'identifiant de bloc spécifiés.	

Catégorie	JSON-RPC	Description	Considérations
	eth_get TransactionBy BlockHash AndIndex	Renvoie des informations sur une transaction en utilisant le hachage de bloc et la position de l'index de transacti on spécifiés.	
	eth_get TransactionBy BlockNumber AndIndex	Renvoie des informations sur une transaction en utilisant le numéro de bloc et la position de l'index de transacti on spécifiés.	
	Hachage eth_get TransactionBy	Renvoie des informations sur la transaction avec le hachage de transaction spécifié.	
	eth_get TransactionCount	Renvoie le nombre de transactions envoyées depuis l'adresse et l'identif iant de bloc spécifiés.	

Catégorie	JSON-RPC	Description	Considérations
	eth_get TransactionReceipt	Renvoie le reçu de la transaction en utilisant le hachage de transaction spécifié.	
	eth_get UncleBy BlockHash AndIndex	Renvoie des informations sur le bloc oncle spécifié à l'aide du hachage du bloc et de la position de l'index oncle.	
	eth_get UncleBy BlockNumber AndIndex	Renvoie des informations sur le bloc d'oncle spécifié à l'aide du numéro de bloc et de la position de l'index d'oncle.	
	Hachage eth_get UncleCount ByBlock	Renvoie le nombre de comptes dans l'oncle spécifié à l'aide du hachage de l'oncle.	
	Numéro eth_get UncleCount ByBlock	Renvoie le nombre de dénombrem ents dans l'oncle spécifié à l'aide du numéro d'oncle.	

Catégorie	JSON-RPC	Description	Considérations
	eth_max PriorityFee PerGas	Renvoie les frais par essence qui sont une estimation du montant que vous pouvez payer en tant que frais prioritaire, ou « pourboire », pour qu'une transaction soit incluse dans le bloc actuel.	En général, vous utilisez la valeur renvoyée par cette méthode pour définir le `maxFeePerGas` dans la transaction suivante que vous soumettez.
	ETH_Version du protocole	Renvoie la version actuelle du protocole Ethereum.	
	eth_send RawTransaction	Crée une nouvelle transaction d'appel par message ou une création de contrat pour les transactions signées.	La blockchain gérée ne prend en charge que les transactions brutes. Vous devez créer et signer des transactions avant de les envoyer.

Catégorie	JSON-RPC	Description	Considérations
Débogage	Hachage debug_trace BlockBy	Renvoie le numéro de résultat de suivi possible en exécutant toutes les transactions du bloc spécifié par le hachage du bloc avec un traceur (mode de suivi requis).	
	Numéro debug_trace BlockBy	Renvoie le résultat du suivi en exécutant toutes les transactions du bloc spécifié par un numéro avec un traceur (mode de suivi requis).	
	Debug_TraceCall	Renvoie le nombre de résultats de traçage possibles en exécutant un appel eth dans le contexte de l'exécution du bloc donné (mode Trace requis).	
	Debug_TraceTransaction	Renvoie toutes les traces d'une transaction donnée (mode de suivi requis).	

Catégorie	JSON-RPC	Description	Considérations
Filet	net_version	Renvoie l'identifiant réseau actuel.	
Tracer	trace_block	Renvoie une trace complète de tous les opcodes invoqués pour toutes les transactions incluses dans un bloc.	
	trace_call	Renvoie le nombre de résultats de traçage possibles en exécutant un appel eth dans le contexte de l'exécution du bloc donné (mode Trace requis).	
	tracer_transaction	Renvoie toutes les traces d'une transaction donnée (mode de suivi requis).	
Piscine Tx	txpool_content	Renvoie toutes les transactions en attente et en file d'attente.	

Catégorie	JSON-RPC	Description	Considérations
	txpool_status	Fournit le décompte de toutes les transactions actuellement en attente d'inclusion dans les prochains blocs, ainsi que de celles qui sont en file d'attente (prévues pour une exécution future uniquement).	
Web	Version du client Web3	Renvoie la version actuelle du client.	

Cas d'utilisation de polygones avec Amazon Managed Blockchain (AMB) Access Polygon

La blockchain Polygon est couramment utilisée dans la création d'applications décentralisées (DApps) liées aux NFT, aux jeux Web3 et aux cas d'utilisation de la tokenisation, entre autres. Cette rubrique fournit une liste de certains des cas d'utilisation que vous pouvez implémenter à l'aide d'Amazon Managed Blockchain (AMB) Access Polygon.

Rubriques

Analyser les données Polygon NFT

Vous pouvez collecter des données sur les NFT polygonaux, notamment des informations telles que les événements de transfert et les métadonnées NFT pour une période spécifiée. Vous pouvez ensuite analyser ces données pour obtenir des informations telles que les NFT sont à la mode ou les utilisateurs qui interagissent le plus fréquemment avec une collection donnée.

Pour plus d’informations, consultez L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon.

Support des achats NFT

Vous pouvez utiliser AMB Access Polygon pour soumettre des transactions pour des achats NFT à l'aide de la monnaie initiale, de listes d'autorisation ou sur le marché secondaire. En combinant d'autres AWS services, vous pouvez ensuite autoriser les achats par carte de crédit, en acceptant des Fiat ou des cryptomonnaies, avec un règlement rapide pour toutes les parties prenantes concernées.

Pour plus d’informations, consultez L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon.

Création d'un portefeuille Polygon

Vous pouvez utiliser AMB Access Polygon pour exécuter les fonctions critiques des portefeuilles d'actifs numériques, telles que la lecture des soldes de jetons des utilisateurs à partir de contrats intelligents sur la blockchain ou la diffusion de transactions signées sur la blockchain.

Pour plus d’informations, consultez L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon.

Portefeuille en tant que service

Vous pouvez utiliser AMB Access Polygon pour développer une opération wallet-as-a-service nécessaire à la prise en charge des transactions de portefeuille courantes, telles que la vérification d'un solde, le transfert d'actifs, l'envoi d'actifs et l'estimation des frais, à l'aide des RPC Polygon JSON-RPC compatibles.

Pour plus d’informations, consultez L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon.

Expériences protégées par des jetons

Vous pouvez utiliser AMB Access Polygon pour créer des expériences basées sur des jetons pour vos utilisateurs. Par exemple, vous pouvez fournir l'accès conditionnel à un contenu uniquement aux propriétaires d'un NFT spécifique. Pour ce faire, vous devez lire la blockchain afin de déterminer la propriété NFT de l'adresse d'un utilisateur.

Pour plus d'informations, voir L'API Managed Blockchain et les JSON-RPC compatibles avec AMB Access Polygon.

Tutoriels pour le polygone d'accès Amazon Managed Blockchain (AMB)

Les didacticiels suivants présentés dans cette section sont des articles de la communauté AWS re:Post qui fournissent des procédures pas à pas pour vous aider à apprendre à effectuer certaines tâches courantes sur la blockchain Polygon à l'aide d'AMB Access Polygon.

- Envoi de transactions à l'aide d'AMB Access Polygon et de web3.js
- Déployez un contrat intelligent à l'aide d'AMB Access Polygon et Hardhat Ignition
- Interaction avec un contrat intelligent
- Récupérez les données de prix actuelles hors chaîne à l'aide des flux de données AMB Access Polygon et Chainlink
- Analysez les données du jeton ERC-20 sur Polygon Mainnet avec AMB Access

Sécurité dans le polygone d'accès Amazon Managed Blockchain (AMB)

La sécurité du cloud AWS est une priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Managed Blockchain (AMB) Access Polygon, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables.

Pour assurer la protection des données, l'authentification et le contrôle d'accès, Amazon Managed Blockchain utilise les AWS fonctionnalités et les fonctionnalités du framework open source exécuté dans Managed Blockchain.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AMB Access Polygon. Les rubriques suivantes vous montrent comment configurer AMB Access Polygon pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources AMB Access Polygon.

Rubriques

Protection des données dans le polygone d'accès Amazon Managed Blockchain (AMB)

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon Managed Blockchain (AMB) Access Polygon. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels

que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AMB Access Polygon ou autre à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

Le chiffrement des données permet d'empêcher les utilisateurs non autorisés de lire les données d'un réseau blockchain et des systèmes de stockage de données associés. Cela inclut les données susceptibles d'être interceptées lorsqu'elles circulent sur le réseau, appelées données en transit.

Chiffrement en transit

Par défaut, Managed Blockchain utilise une connexion HTTPS/TLS pour chiffrer toutes les données transmises depuis un ordinateur client qui exécute les points de terminaison du AWS CLI service. AWS

Vous n'avez pas besoin de faire quoi que ce soit pour activer l'utilisation de HTTP/TLS. Il est toujours activé, sauf si vous le désactivez explicitement pour une AWS CLI commande individuelle à l'aide de la `--no-verify-ssl` commande.

Gestion des identités et des accès pour Amazon Managed Blockchain (AMB) Access Polygon

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources AMB Access Polygon. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Comment fonctionne le polygone d'accès Amazon Managed Blockchain (AMB) avec IAM
- Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)
- Résolution des problèmes liés à l'identité et à l'accès au polygone d'accès Amazon Managed Blockchain (AMB)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AMB Access Polygon.

Utilisateur du service — Si vous utilisez le service AMB Access Polygon pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'AMB Access Polygon pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AMB Access Polygon, consultez. Résolution des problèmes liés à l'identité et à l'accès au polygone d'accès Amazon Managed Blockchain (AMB)

Administrateur de service — Si vous êtes responsable des ressources AMB Access Polygon dans votre entreprise, vous avez probablement un accès complet à AMB Access Polygon. C'est à vous de déterminer à quelles fonctionnalités et ressources AMB Access Polygon doivent accéder aux utilisateurs de votre service. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AMB Access Polygon, consultez. Comment fonctionne le polygone d'accès Amazon Managed Blockchain (AMB) avec IAM

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AMB Access Polygon. Pour voir des exemples de politiques basées sur l'identité AMB Access Polygon que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas

utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d’une action, quelle que soit la méthode que vous utilisez pour exécuter l’opération. Par exemple, supposons que vous disposiez d’une politique qui autorise l’action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l’identité

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Les politiques basées sur l’identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre

une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour

une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment fonctionne le polygone d'accès Amazon Managed Blockchain (AMB) avec IAM

Avant d'utiliser IAM pour gérer l'accès à AMB Access Polygon, découvrez quelles fonctionnalités IAM peuvent être utilisées avec AMB Access Polygon.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Managed Blockchain (AMB) Access Polygon

Fonction IAM	Support du polygone d'accès AMB
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d’une politique	Non
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d’identification temporaires	Non
Autorisations de principals	Non
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AMB Access Polygon et d'autres Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AMB Access Polygon

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour AMB Access Polygon

Pour consulter des exemples de politiques basées sur l'identité d'AMB Access Polygon, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Politiques basées sur les ressources au sein d'AMB Access Polygon

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une

politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour AMB Access Polygon

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions du polygone d'accès AMB, consultez la section Actions définies par le polygone d'accès Amazon Managed Blockchain (AMB) dans le Service Authorization Reference.

Les actions politiques dans AMB Access Polygon utilisent le préfixe suivant avant l'action :

```
managedblockchain:
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `InvokeRpcPolygon`, incluez l'action suivante :

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

Pour consulter des exemples de politiques basées sur l'identité d'AMB Access Polygon, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Ressources relatives aux politiques pour AMB Access Polygon

Prend en charge les ressources de politique	Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources AMB Access Polygon et leurs ARN, consultez la section Resources Defined by Amazon Managed Blockchain Access Polygon (AMB) dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par le polygone d'accès Amazon Managed Blockchain (AMB).

Pour consulter des exemples de politiques basées sur l'identité d'AMB Access Polygon, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Clés de conditions de politique pour AMB Access Polygon

Prend en charge les clés de condition de politique spécifiques au service	Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition du polygone d'accès AMB, consultez la section Clés de condition pour le polygone d'accès Amazon Managed Blockchain (AMB) dans le manuel Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par le polygone d'accès Amazon Managed Blockchain (AMB).

Pour consulter des exemples de politiques basées sur l'identité d'AMB Access Polygon, consultez. Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

ACL dans le polygone d'accès AMB

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec polygone d'accès AMB

Prise en charge d'ABAC (identifications dans les politiques)	Non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur l’ABAC, consultez Qu’est-ce que le contrôle d’accès basé sur les attributs (ABAC) ? dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AMB Access Polygon

Prend en charge les informations d’identification temporaires	Non

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour AMB Access Polygon

Prend en charge les sessions d'accès direct (FAS)	Non

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour AMB Access Polygon

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut perturber les fonctionnalités d'AMB Access Polygon. Modifiez les rôles de service uniquement lorsque AMB Access Polygon fournit des instructions à cet effet.

Rôles liés à un service pour AMB Access Polygon

Prend en charge les rôles liés à un service	Non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la

colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour le polygone d'accès Amazon Managed Blockchain (AMB)

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources AMB Access Polygon. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AMB Access Polygon, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour le polygone d'accès Amazon Managed Blockchain (AMB) dans le Service Authorization Reference.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AMB Access Polygon dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez

les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AMB Access Polygon

Pour accéder à la console Amazon Managed Blockchain (AMB) Access Polygon, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources AMB Access Polygon de votre. Compte AWS Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console AMB Access Polygon, attachez également le polygone d'accès AMB *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
        }
    ]
}
```

Accès aux réseaux Polygon

> **Note**
>
> Pour accéder aux points de terminaison publics du polygone `mainnet` et `mainnet` pour effectuer des appels JSON-RPC, vous aurez besoin d'informations d'identification utilisateur (`AWS_ACCESS_KEY_IDetAWS_SECRET_ACCESS_KEY`) disposant des autorisations IAM appropriées pour AMB Access Polygon.

Example Politique IAM pour accéder à tous les réseaux polygonaux

Cet exemple permet à un utilisateur IAM d' Compte AWS accéder à tous les réseaux Polygon.

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

```
    ]
}
```

Example Politique IAM pour accéder au réseau principal Polygon

Cet exemple accorde à un utilisateur IAM l' Compte AWS accès au réseau principal Polygon.

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

Résolution des problèmes liés à l'identité et à l'accès au polygone d'accès Amazon Managed Blockchain (AMB)

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AMB Access Polygon et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AMB Access Polygon
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources AMB Access Polygon

Je ne suis pas autorisé à effectuer une action dans AMB Access Polygon

Si vous recevez une erreur qui indique que vous n’êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d’effectuer l’action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `managedblockchain::`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `managedblockchain::`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AMB Access Polygon.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AMB Access Polygon. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources AMB Access Polygon

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si AMB Access Polygon prend en charge ces fonctionnalités, consultez. Comment fonctionne le polygone d'accès Amazon Managed Blockchain (AMB) avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Journalisation des événements du polygone d'accès Amazon Managed Blockchain (AMB) en utilisant AWS CloudTrail

> **Note**
>
> Amazon Managed Blockchain (AMB) Access Polygon ne prend pas en charge les événements de gestion.

Amazon Managed Blockchain fonctionne sur AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Managed Blockchain. CloudTrail capture qui a invoqué les points de terminaison du polygone d'accès AMB pour Managed Blockchain en tant qu'événements du plan de données.

Si vous créez un journal correctement configuré auquel vous êtes abonné pour recevoir les événements du plan de données souhaités, vous pouvez recevoir une livraison continue des CloudTrail événements liés à AMB Access Polygon vers un compartiment S3. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer si une demande a été envoyée à l'un des points de terminaison AMB Access Polygon, l'adresse IP d'origine de la demande, l'auteur de la demande, la date à laquelle elle a été faite et d'autres informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le polygone d'accès AMB dans CloudTrail

CloudTrail est activé sur votre ordinateur Compte AWS lorsque vous le créez. Cependant, vous devez configurer les événements du plan de données pour savoir qui a invoqué les points de terminaison du polygone d'accès AMB.

Pour un enregistrement continu des événements de votre site Compte AWS, y compris des événements pour AMB Access Polygon, créez un parcours. Un journal permet CloudTrail de fournir des fichiers journaux à un compartiment S3. Par défaut, lorsque vous créez un journal d’activité dans la console, il s’applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions prises en charge dans la AWS partition et transmet les fichiers journaux au

compartiment S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour effectuer une analyse plus approfondie et agir sur les données d'événements collectées dans CloudTrail les journaux. Pour plus d’informations, consultez les ressources suivantes :

- Utilisation CloudTrail pour suivre les polygones JSON-RPC
- Présentation de la création d’un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

En analysant les événements de CloudTrail données, vous pouvez contrôler qui a invoqué les points de terminaison AMB Access Polygon.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l’identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM)
- Si la requête a été effectuée avec des informations d’identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre Service AWS

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal AMB Access Polygon

Pour les événements du plan de données, un suivi est une configuration qui permet de transmettre les événements sous forme de fichiers journaux à un compartiment S3 spécifié. Chaque fichier CloudTrail journal contient une ou plusieurs entrées de journal qui représentent une seule demande provenant de n'importe quelle source. Ces entrées fournissent des détails sur l'action demandée, y compris la date et l'heure de l'action, ainsi que les éventuels paramètres de demande associés.

> **Note**
>
> CloudTrail les événements de données dans les fichiers journaux ne constituent pas une trace ordonnée des appels d'API AMB Access Polygon. Ils n'apparaissent donc pas dans un ordre spécifique.

Utilisation CloudTrail pour suivre les polygones JSON-RPC

Vous pouvez l'utiliser CloudTrail pour savoir qui, dans votre compte, a invoqué les points de terminaison AMB Access Polygon et quel JSON-RPC a été invoqué en tant qu'événements de données. Par défaut, lorsque vous créez un suivi, les événements liés aux données ne sont pas enregistrés. Pour enregistrer les personnes qui ont invoqué les points de terminaison du polygone d'accès AMB en tant qu'événements de CloudTrail données, vous devez ajouter explicitement les ressources prises en charge ou les types de ressources pour lesquels vous souhaitez collecter des activités à un suivi. AMB Access Polygon prend en charge l'ajout d'événements de données à l'aide du AWS Management Console AWS CLI, et du SDK. Pour plus d'informations, voir Enregistrer les événements à l'aide de sélecteurs avancés dans le Guide de l'AWS CloudTrail utilisateur.

Pour enregistrer les événements liés aux données dans un suivi, utilisez l'opération put-event-selectors après avoir créé le suivi. Utilisez l'`--advanced-event-selectors`option pour spécifier les types de `AWS::ManagedBlockchain::Network` ressources afin de commencer à enregistrer les événements de données afin de déterminer qui a invoqué les points de terminaison du polygone d'accès AMB.

Example Entrée dans le journal des événements de données de toutes les demandes de points de terminaison AMB Access Polygon de votre compte

L'exemple suivant montre comment utiliser l'`put-event-selectors`opération pour enregistrer toutes les demandes de point de terminaison AMB Access Polygon de votre compte pour le sentier `my-polygon-trail` dans la `us-east-1` région.

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

Une fois inscrit, vous pouvez suivre l'utilisation dans le compartiment S3 connecté à la piste spécifiée dans l'exemple précédent.

Le résultat suivant montre une entrée dans le journal des événements de CloudTrail données contenant les informations collectées par CloudTrail. Vous pouvez déterminer qu'une demande Polygon JSON-RPC a été envoyée à l'un des points de terminaison AMB Access Polygon, l'adresse IP d'origine de la demande, l'auteur de la demande, la date à laquelle elle a été faite et d'autres informations supplémentaires. Certaines valeurs de l'exemple suivant ont été masquées pour des raisons de sécurité mais apparaissent intégralement dans les entrées du journal.


```
{
        "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"
}
```

Historique du document pour le guide de l'utilisateur d'AMB Access Polygon

Le tableau suivant décrit les versions de documentation pour AMB Access Polygon.

Modification	Description	Date
Quotas mis à jour pour JSON-RPC	Les quotas pris en charge par AMB Access Polygon pour chaque JSON-RPC pris en charge sont mis à jour.	12 avril 2024
Fin du support pour le réseau testnet de Mumbai	AMB Access Polygon a mis fin au support du réseau de test de Mumbai le 15 avril 2024.	10 avril 2024
Ajout de la rubrique Tutoriels	Tutoriels AMB Access Polygon disponibles dans la section Articles communautaires d'AWS Re:POST.	9 avril 2024
Avant-première publique	Version préliminaire publique du service Amazon Managed Blockchain (AMB) Access Polygon.	24 novembre 2023