Alibaba Cloud Elasticsearch

RAM

Document Version20200306

目次

1 許可されているリソース

リソースタイプと説明

次の表に、サポートされているリソースタイプと **Alibaba Cloud** リソース名 **(ARN)** を示します。

リソースタイプ	ARN
instances	**acs:elasticsearch:$regionId:$accountId:instances/***
instances	**acs:elasticsearch:$regionId:$accountId:instances/$instanceId**
vpc	**acs:elasticsearch:$regionId:$accountId:vpc/***
vswitch	**acs:elasticsearch:$regionId:$accountId:vswitch/***

- **$regionId**：特定のリージョンの **ID**。 アスタリスク `*` も入力できます。
- **$accountId**：**Alibaba Cloud** アカウントの **ID**。 アスタリスク `*` も入力できます。
- **$instanceId**：特定の **Elasticsearch** インスタンスの **ID**。 アスタリスク `*` も入力できます。

インスタンスの許可

 注：

次の **ARN** は短縮されています。 完全名の情報については、前述の表をご参照ください。

- インスタンスに対する共通のアクション

アクション	説明	ARN
elasticsearch:CreateInstance	インスタンスを作成します。	`instances/*`
elasticsearch:ListInstance	インスタンスを表示します。	`instances/*`
elasticsearch:DescribeInstance	インスタンスの説明を表示します。	`instances/*` または `instances/$instanceId`
elasticsearch:DeleteInstance	インスタンスを削除します。	`instances/*` または `instances/$instanceId`

アクション	説明	ARN
elasticsearch:RestartInstance	インスタンスを再起動します。	`instances/*` または `instances/$instanceId`
elasticsearch:UpdateInstance	インスタンスを更新します。	`instances/*` または `instances/$instanceId`

- プラグインに対するアクション

アクション	説明	ARN
elasticsearch:ListPlugin	プラグインのリストを取得します。	`instances/$instanceId`
elasticsearch:InstallSystemPlugin	システムプラグインをインストールします。	`instances/$instanceId`
elasticsearch:UninstallPlugin	プラグインをアンインストールします。	`instances/$instanceId`

- ネットワークに対するアクション

アクション	説明	ARN
elasticsearch:UpdatePublicNetwork	パブリックアドレスを介したアクセスが許可されているかどうかを確認します。	`instances/$instanceId`
elasticsearch:UpdatePublicIps	パブリックネットワークホワイトリストを変更します。	`instances/$instanceId`
elasticsearch:UpdateWhiteIps	**VPC** ホワイトリストを変更します。	`instances/$instanceId`
elasticsearch:UpdateKibanaIps	**Kibana** ホワイトリストを変更します。	`instances/$instanceId`

- 辞書に対するアクション

アクション	説明	ARN
elasticsearch:UpdateDict	**IK** アナライザーとシノニム辞書を変更します。	`instances/$instanceId`

許可されている CloudMonitor **アクション** (CloudMonitor **コンソール**)

注：

次の **ARN** は * ワイルドカード形式に短縮されています。

アクション	説明	ARN 形式
cms:ListProductOfActiveAlert	**CloudMonitor** を有効化しているサービスを表示します。	*
cms:ListAlarm	特定のまたはすべてのアラームルール設定を照会します。	*
cms:QueryMetricList	特定のインスタンスのモニタリングデータを照会します。	*

VPC と VSwitch の許可


注：
次の **ARN** は短縮されています。 完全名の情報については、前述の表をご参照ください。

アクション	説明	ARN
DescribeVpcs	**VPC** リストを取得します。	`vpc/*`
DescribeVswitches	**VSwitch** リストを取得します。	`vswitch/*`

Intelligent Maintenance の許可


注：
次の **ARN** は短縮されています。 完全名の情報については、前述の表をご参照ください。

アクション	説明	ARN
elasticsearch:OpenDiagnosis	ヘルス診断を有効化します。	`instances/*` または `instances/$instanceId`
elasticsearch:CloseDiagnosis	ヘルス診断を無効化します。	`instances/*` または `instances/$instanceId`
elasticsearch:UpdateDiagnosisSettings	ヘルス診断設定を更新します。	`instances/*` または `instances/$instanceId`
elasticsearch:DescribeDiagnosisSettings	ヘルス診断設定を照会します。	`instances/*` または `instances/$instanceId`
elasticsearch:ListInstanceIndices	インスタンスインデックスを照会します。	`instances/*` または `instances/$instanceId`
elasticsearch:DiagnoseInstance	ヘルス診断を開始します。	`instances/*` または `instances/$instanceId`

アクション	説明	ARN
elasticsearch:ListDiagnoseReportIds	診断レポート ID を照会します。	`instances/*` または `instances/$instanceId`
elasticsearch:DescribeDiagnoseReport	診断レポートの詳細を表示します。	`instances/*` または `instances/$instanceId`
elasticsearch:ListDiagnoseReport	診断レポートをリストします。	`instances/*` または `instances/$instanceId`

サポートされるリージョン

Elasticsearch リージョン	RegionId
中国 (杭州)	**cn-hangzhou-d**
中国 (北京)	**cn-beijing**
中国 (上海)	**cn-shanghai**
中国 (深セン)	**cn-shenzhen**
インド (ムンバイ)	**ap-south-1**
シンガポール	**ap-southeast-1**
cn-hongkong	**cn-hongkong**
米国 (シリコンバレー)	**us-west-1**
マレーシア (クアラルンプール)	**ap-southeast-3**
ドイツ (フランクフルト)	**eu-central-1**
日本 (東京)	**ap-northeast-1**
オーストラリア (シドニー)	**ap-southeast-2**
インドネシア (ジャカルタ)	**ap-southeast-5**
中国 (青島)	**cn-qingdao**
中国 (張家口)	**cn-zhangjiakou**

2 権限ポリシー

このドキュメントでは、**Elasticsearch** でサポートしている一般権限ポリシー、およびカスタム権限ポリシーについて説明します。 また、権限を付与する方法の例も紹介します。

一般権限ポリシー

Elasticsearch は、次の **2** 種類の一般権限ポリシーを提供しています。

- **AliyunElasticsearchReadOnlyAccess: Elasticsearch** にアクセスするための読み取り専用権限。 この権限は、読み取り専用ユーザーに付与できます。
- **AliyunElasticsearchFullAccess: Elasticsearch** を管理する権限。 この権限は管理者に付与できます。

> 注：
> 上記の **2** つのポリシーが要件を満たさない場合、独自のポリシーを作成できます。 カスタムポリシーの作成方法については、カスタムポリシーの作成をご参照ください。

カスタムポリシーの作成

1. **[**ポリシードキュメント**]** で、既存のシステムポリシーを選択し、スクリプトを編集します。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "",
            "Resource": ""
        }
    ],
    "Version": "1"
}
```

> 注：
> あいまい検索の検索ボックスにキーワードを入力できます。

必要に応じて権限スクリプトを入力します。

- **VPC** を照会する権限

```
[“vpc:DescribeVSwitch*”,“vpc:DescribeVpc*”]
```

> 注：

AliyunVPCReadOnlyAccess 権限を参照として使用できます。

- インスタンスを購入する権限

```
["bss:PayOrder"]
```

注：

AliyunBSSOrderAccess 権限を参照として使用できます。

- **API** 操作を実行する権限

Method	URI	Resource	Action
GET	/instances	instances/*	ListInstance
POST	/instances	instances/*	CreateInstance
GET	/instances/$instanceId	instances/$instanceId	DescribeInstance
DELETE	instances/$instanceId	instances/$instanceId	DeleteInstance
POST	/instances/$instanceId/actions/restart	instances/$instanceId	RestartInstance
PUT	instances/$instanceId	instances/$instanceId	UpdateInstance

2. **[OK]** をクリックします。

例 1

この例では、accountId が 1234 の **RAM** ユーザーアカウントに、中国 (杭州) にあるすべてのインスタンスで、**CreateInstance** 操作を除くすべての操作を実行する権限が付与されます。 指定された **IP** アドレスのみが **Elasticsearch** コンソールへのアクセスを許可されます。

次のスクリプトは、カスタムポリシーの内容を示しています。

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:ListInstance",
        "elasticsearch:DescribeInstance",
        "elasticsearch:DeleteInstance",
        "elasticsearch:RestartInstance",
        "elasticsearch:UpdateInstance"
      ],
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "xxx.xx.xxx.x/xx"
        }
```

```
      },
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:cn-hangzhou:1234:instances/*"
    }
  ],
  "Version": "1"
}
```

このポリシーで指定された権限を **RAM** ユーザーアカウントに付与します。 詳細については、「*#unique_3*」をご参照ください。

 :

Alibaba Cloud アカウントを使用して **RAM** コンソールでポリシーを作成した後、**RAM** コンソールまたは **RAM SDK** を使用して、**RAM** ユーザーアカウントに必要な権限を付与する必要があります。

例 2

この例では、accountId が 1234 の **RAM** ユーザーアカウントに、中国 (杭州) にある指定されたインスタンスで、**CreateInstance** 操作を除くすべての操作を実行する権限が付与されます。指定された **IP** アドレスのみが **Elasticsearch** コンソールへのアクセスを許可されます。

次のスクリプトは、カスタムポリシーの内容を示しています。

```
{
  "Statement": [
    {
      "Action": [
        "elasticsearch:ListInstance"
      ],
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "xxx.xx.xxx.x/xx"
        }
      },
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:cn-hangzhou:1234:instances/*"
    },
    {
      "Action": [
        "elasticsearch:DescribeInstance",
        "elasticsearch:DeleteInstance",
        "elasticsearch:RestartInstance",
        "elasticsearch:UpdateInstance"
      ],
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "xxx.xx.xxx.x/xx"
        }
      },
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:cn-hangzhou:1234:instances/$
instanceId"
    }
  ],
```

```
  "Version": "1"
}
```

このポリシーで指定された権限を RAM ユーザーアカウントに付与します。 詳細については、「#unique_3」をご参照ください。

:

Alibaba Cloud アカウントを使用して RAM コンソールでポリシーを作成した後、RAM コンソールまたは RAM SDK を使用して、RAM ユーザーアカウントに必要な権限を付与する必要があります。

例 3

この例では、accountId が 1234 の RAM ユーザーアカウントに、すべてのリージョンにある Elasticsearch インスタンスですべての操作を実行する権限が付与されます。

次のスクリプトは、カスタムポリシーの内容を示しています。

```
{
  "Statement": [
    {
      "Action": [
          "elasticsearch:*"
            ],
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:*:1234:instances/*"
    }
  ],
  "Version": "1"
}
```

このポリシーで指定された権限を RAM ユーザーアカウントに付与します。 詳細については、「#unique_3」をご参照ください。

:

Alibaba Cloud アカウントを使用して RAM コンソールでポリシーを作成した後、RAM コンソールまたは RAM SDK を使用して、RAM ユーザーアカウントに必要な権限を付与する必要があります。

例 4

この例では、accountId が 1234 の RAM ユーザーアカウントに、すべてのリージョンにある Elasticsearch インスタンスで CreateInstance および ListInstance 操作を除くすべての操作を実行する権限が付与されます。

次のスクリプトは、カスタムポリシーの内容を示しています。

```
{
```

```
  "Statement": [
    {
      "Action": [
          "elasticsearch:DescribeInstance",
          "elasticsearch:DeleteInstance",
          "elasticsearch:UpdateInstance",
          "elasticsearch:RestartInstance"
            ],
      "Effect": "Allow",
      "Resource": "acs:elasticsearch:*:1234:instances/$instanceId"
    }
  ],
  "Version": "1"
}
```

このポリシーで指定された権限を **RAM** ユーザーアカウントに付与します。 詳細については、「*#unique_3*」をご参照ください。

:

Alibaba Cloud アカウントを使用して **RAM** コンソールでポリシーを作成した後、**RAM** コンソールまたは **RAM SDK** を使用して、**RAM** ユーザーアカウントに必要な権限を付与する必要があります。

よくある質問

Q：**RAM** ユーザーアカウントを使用して **Elasticsearch** の購入ページで **VPC** を見つけることができないのはなぜですか。

A：**RAM** ユーザーアカウントを使用して **Elasticsearch** の購入ページで **VPC** を見つけることができない場合、**RAM** ユーザーアカウントに **VPC** へのアクセス権限が付与されているかどうかを確認してください。 詳細については、「*#unique_4*」をご参照ください。 **RAM** ユーザーアカウントに **VPC** へのアクセス権限が付与されていない場合は、**RAM** ユーザーアカウントに必要な権限を付与してください。 詳細については、「カスタムポリシーの作成」をご参照ください。

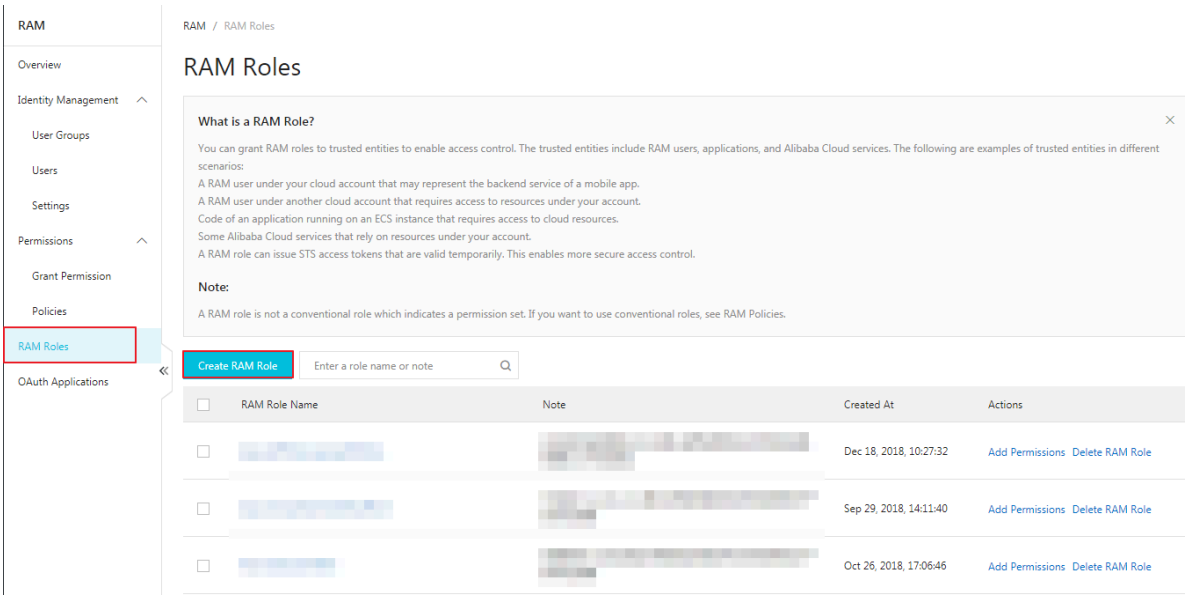
3 一時的なアクセストークン

クラウドリソースへのアクセスが稀なユーザー (人またはアプリ) を一時的なユーザーと言います。 一時的なユーザー (サブアカウント) にアクセストークンを発行するには、**Security Token Service (STS。RAM** の拡張許可サービス) を使用します。 トークンの権限と有効期限は、トークンの発行時に必要に応じて定義できます。

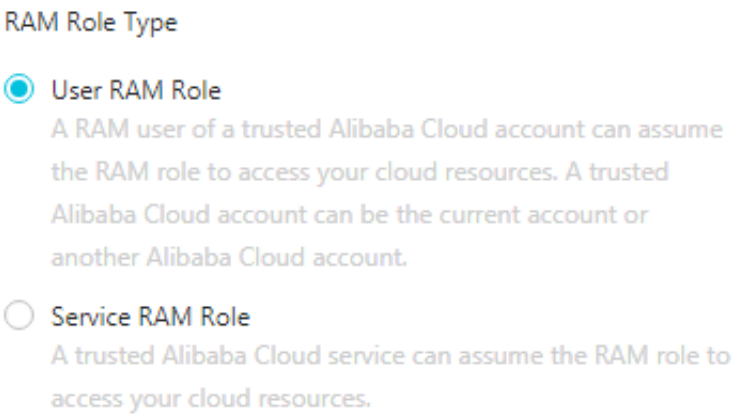
STS アクセストークンを使用して一時的なユーザーを許可する利点は、許可が管理しやすくなることです。 一時的なユーザーの場合、 **RAM** ユーザーアカウントとキーを作成する必要はありません。 **RAM** ユーザーアカウントとキーは長期間有効ですが、一時的なユーザーは長期にわたりリソースにアクセスする必要がありません。 使用例は、「*#unique_6*」と「*#unique_7*」をご参照ください。

ロールの作成

1. **RAM** コンソールで、**[RAM** ロール**]** > **[RAM** ロールの作成**]** を選択します。

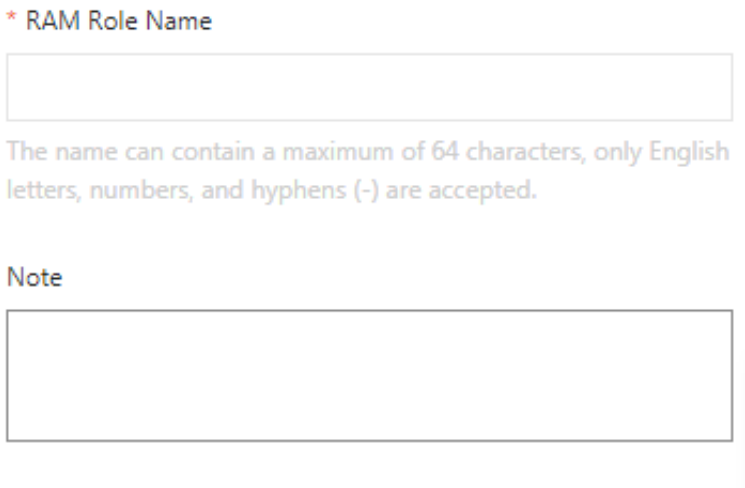


2. ロールタイプを選択します。 ここでは、ロール [ユーザー] が選択されています。



3. タイプ情報を入力します。 信頼できるアカウントのサブアカウントは、作成されたロールを使用することができます。

4. ロール名を入力します。



5. ロールが作成されたら、そのロールを許可します。 詳細は、「*#unique_8*」と「許可されているリソース」をご参照ください。

一時的なアクセス許可

STS でアクセスを許可する前に、手順 3 で作成した信頼できるクラウドアカウントのサブアカウントに引き継ぐロールを許可します。 すべてのサブアカウントにロールが引き継がれるように

すると、予期せぬリスクが生じます。 したがって、必要なロールのみが引き継がれるよう、サブアカウントは権限を明示的に設定する必要があります。

信頼できるクラウドアカウントの許可

1. ページの左側にある [権限付与ポリシー管理] をクリックして、[権限付与ポリシー管理] ページに移動します。
2. ページの右側にある [権限付与ポリシーの作成] をクリックして、[権限付与ポリシーの作成] ページに移動します。
3. [空白のテンプレート] を選択して、[カスタム権限付与ポリシーの作成] ページに移動します。
4. 権限付与ポリシー名を入力し、[ポリシーの内容] 欄に次の内容を入力します。

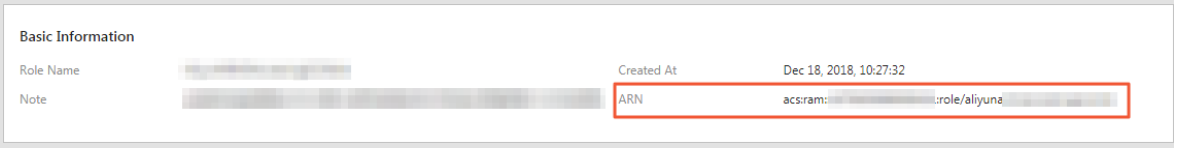
```
{
"Version": "1",
"Statement": [
{
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "acs:ram::${aliyunID}:role/${roleName}"
}
]
}
```

${aliyunID} には、ロールを作成するユーザーの **ID** を指定します。

${roleName} には、ロール名を小文字で指定します。

注：

リソースの詳細は、[ロールの詳細] の [基本情報] ページの [Arn] 欄で確認できます。



5. [ユーザー管理] ページで、サブアカウント用に作成したロールを許可します。 詳細は、「*#unique_8*」をご参照ください。

サブアカウントへのロールの引き継ぎ

許可されたロールをサブアカウントが引き継ぐには、サブアカウントでコンソールにログインし、許可されたロールに切り替えます。 手順は次のとおりです。

1. ナビゲーションバーの右上のアバターにマウスを移動し、表示されたウィンドウで [ロールの切り替え] をクリックします。

2. ロールを作成するアカウントのエンタープライズエイリアスを入力します。 エンタープライズエイリアスを変更していなければ、デフォルトでアカウント **ID** が使用されます。 ロール名を入力し、**[**切り替え**]** スイッチをクリックして、指定したロールに切り替えます。