目录

目录 1
策略文档元素解析 2
IAM授权评估逻辑 2

策略文档元素解析

1.金山云IAM的策略文档采用AWS的策略文档的语法和规范，但在支持的元素的数量上有所区别。

2.目前金山云授权策略文档支持的元素包括：

- **Version**：可选策略元素（string），形如"Version":"2015-11-01"，用于说明策略文档的版本，目前金山云的策略文档版本只有一个取值，**2015-11-01**，如果策略中没有Version元素，其默认值为2015-11-01
- **Statement**：必选策略元素（array），形如"Statement":[{...},{...},{...}]，策略的主元素，用于说明具体授权规则，每个Statement元素可以包含多条语句，每条语句用{}括起来说明。
- **Sid**：可选元素（string），形如"Sid":"1"，Statement的语句标识符，可被省略，在一个策略中需要保持唯一性。
- **Effect**：必选元素（string），形如"Effect":"Allow"，Statement的授权规则的组成元素，每条授权规则必须包括该元素，只有两种取值Allow或者Deny，分别表明“显示授权”和“显示拒绝”。
- **Action**：必选元素（String），形如"Action":"iam:CreateUser"，Statement的授权规则的组成元素，每条授权规则必须包括该元素，取值包括两个部分的内容service-name和action-name，其中service-name是服务命名空间（iam，ks3，kec等），而action-name则是各产品的操作名称，service-name和action-name的值**不区分大小写**，操作名称可以包含通配符*。
- **Resource**：必选元素（String），形如"Resource":"KRN"，Resource是授权规则的作用对象，每种service的resource各不相同，可以使用*来表示全体资源对象，也可以在KRN中使用*来匹配一类特定对象；KRN是金山云对作用对象的标准命名方法，兼容AWS的规范，但KRN域不同，具体各业务支持的KRN可以参考业务说明文档。

3.策略语法说明

- 每个策略文档可以包含多条策略语句
- 每个策略组成元素中包含的同名称元素不能重复，只能出现一次，比如不能在一个策略语句中出现两次Effect元素块
- 策略文档中各元素块的显示顺序无限制
- 策略文档中的白空格（whiteSpace）被忽略

4.策略文档的形式语法如下

```
policy = {
    <version_block?>
    <statment_block>
}
<version_block> = "Version" : "2015-11-01"
<statement_block> = "Statement" : [<statement>, <statement>, ...]
<statement> = {
    <sid_block?>,
    <effect_block>,
    <action_block>,
    <resoure_block>
}
<sid_block> = "Sid" : <sid_string>
<effect_block> = "Effect" : ("Allow" | "Deny")
<action_block> = "Action" : ( "*" | [<action_string>, <action_string>, ...])
<resoure_block> = "Resource" : ( "*" | [<resoure_string>, <resoure_string>, ...])
<action_string> = "service_name : action_name"
<resource_string> = "KRN"
```

5.策略文档示例：云主机（KEC）管理员的权限的策略文档

```
{
  "Version" : "2015-11-01",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "KEC:*",
      "Resource" : "*"
    }
  ]
}
```

IAM授权评估逻辑

IAM授权判断流程如下：

1. 如果使用**主账户**的安全信任状（即AccessKey）进行签名发起请求，且访问对象Resource的**属主**是该主账户，那么授权通过，否则授权不通过
2. 如果请求使用**IAM用户**的安全信任状进行签名发起请求，且访问对象Resource的属组是其所属主账户，那么此时调用权限评估接口，根据IAM用户身上附加的策略集合来判断是否授权通过。

3. 在评估IAM用户身上的附加策略时采用**默认/隐式拒绝（default /implicit deny）**的原则：

- 3.1 如果操作请求被“显示拒绝（explicit deny）”，则返回“授权不通过”，否则进入下一步
- 3.2 如果操作请求被“显示授权（explicit allow）”，则返回“授权通过”，否则进入下一步
- 3.3 默认/隐式拒绝（default /implicit deny）所有操作请求，返回“授权不通过”

即**显式拒绝>"显式授权">"默认/隐式拒绝"**