云享家 | 没有绝对的安全，只有在阿里云的最佳实践。

原创：张小娅 BespinGlobal 1周前

数字化时代背景下，越来越多的企业选择上云。企业上云不仅可以驱动流程创新和业务创新，还会为企业带来新的利润增长点，**呈现出更为弹性化、安全化、智能化、高效化的运维特性。**

然而企业上云之后，怎么控制不同的用户访问不同的云资源将是一个头疼的事情。特别是一些大型企业客户迁移上云之后，他们的组织结构更加复杂，对云资源的安全管理需求将会非常强烈。

Bespin Global的交付工程师张小娅，将为您解析**阿里云的自定义Policy语法来实现云上指定资源访问规则！**

Policy结构

授权策略（Policy）结构包括 Policy 版本号及授权语句（Statement）列表。每个授权语句又包括以下元素：Effect（授权类型）、Action（操作名称列表）、Resource（操作对象列表）以及 Condition（条件限制），其中 Condition 是可选项。

Policy 结构简述如下：

最佳实战

场景1：对象存储OSS授权

授权子用户完全管理某个Bucket的权限。Policy语法如下：

```
{
  "Statement": [
    {
      "Action": "oss:*",
      "Effect": "Allow",
      "Resource": "acs:oss:*:*:bucket1/*"
    }
  ],
  "Version": "1"
}
```

场景2: CES 授权样例

授权子账号对某些ECS实例有访问权限 。Policy语法如下：

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
                "acs:ecs:*:*:instance/i-001",
                "acs:ecs:*:*:instance/i-002"
                ]
    },
    {
```

```
      "Action": "ecs:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

场景3：限制源 IP

授权子账号拥有所有资源操作权限，并加源IP限制。Policy语法如下：

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "121.0.27.1"
    }
  },
  "Version": "1"
}
```

授权子账号拥有所有资源只读权限，并加源IP限制。Policy语法如下:

```
{
  "Statement": [
    {
      "Action": [
          "*:Describe*",
        "*:List*",
        "*:Get*",
        "*:BatchGet*",
        "*:Query*",
        "*:BatchQuery*",
        "actiontrail:LookupEvents",
        "dm:Desc*",
        "dm:SenderStatistics*"
],
```

```
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": " 10.10.0.0/8"
    }
  },
  "Version": "1"
}
```

场景4：跨云账号访问资源

假设企业A（AccountID=11223344，别名company-a）需要授权企业B（AccountID=12345678，别名 company-b）的员工对其 RDS进行操作。

访问逻辑如下图：

授权策略如下：

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole,ecs:*",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::12345678:root"
        ]
```

```
      },
      "Resource": [
        "acs:rds:*:*:dbinstance/i-001",
        "acs:rds:*:*:dbinstance/i-002"
      ]
    }
  ],
  "Version": "1"
}
```

> 没有绝对的安全，只有最佳的实践。只有遵循最佳安全实践原则，综合利用这些保护机制，相信可以极大提高对您的账号资产的保护。话不多说，即刻动手开启云上资源访问管理之旅吧！

> 备注：
>
> Policy 语法结构参考官方文档：
> https://help.aliyun.com/document_detail/28664.html?spm=a2c4g.11186623.6.571.76ec7df6JxTsVF

相关阅读

云享家 | 医疗和金融行业在AWS平台的合规配置

云享家 | 基于AWS云平台的IDS联合监控分析

云享家 | 多面手完善AWS CloudWatch监控图表

云享家 | AWS CloudWatch如何集成微信报警

阅读原文