目录

对云上应用进行动态身份管理与授权

当企业购买了金山云的产品后，应用程序可以通过访问控制（IAM）可以获取到IAM角色的临时安全令牌，从而访问金山云服务。

背景介绍

企业A购买了KEC实例，并计划在KEC实例中部署企业的应用程序。这些应用程序需要使用访问密钥（AccessKey）访问其它云服务API。

有两种做法：

- 将访问密钥直接嵌入在代码里。
- 将访问密钥保存在应用程序的配置文件中。

这样会带来两个问题：

- 保密性问题：如果访问密钥以明文形式存在于KEC实例中，可能会随着快照、镜像及镜像创建出来的实例泄露。
- 难运维问题：由于访问密钥存在于实例中，如果要更换访问密钥（例如：周期性轮转或切换用户身份），那么需要对每个实例和镜像进行更新并重新部署，这会增加对实例和镜像管理的复杂性。

解决方案

KEC结合访问控制提供的访问控制能力，允许给每一个KEC实例配置一个拥有合适权限的IAM角色身份。应用程序通过获取该IAM角色的临时安全令牌来访问云API。

操作流程

步骤一：创建IAM角色并为角色授权

1. 使用金山云账号创建一个IAM角色。

   创建IAM角色时受信实体选择金山云服务，受信服务选择云服务器，即允许KEC扮演该IAM角色来访问金山云资源。

2. 为IAM角色授权。参考IAM角色授权。

   如果临时安全令牌权限不足时，您可以根据需要为IAM角色添加相应的权限。权限更新后立即生效，无需重新启动KEC实例。

步骤二：为KEC实例绑定IAM角色

1. 登录云服务器控制台。

   被授权的IAM用户才能为KEC实例配置IAM角色，参考系统策略KECAdminFullAccess （提供云主机全部操作管理的权限）。

2. 在左侧导航菜单，单击**实例**列表。

3. 在实例列表中，根据实际需求选择如下操作：

   - 单个实例绑定/解绑IAM角色：在实例列表找到目标实例，选择**更多**> **绑定/解绑IAM角色**。
   - 批量实例绑定/解绑IAM角色：批量选中目标实例，选择**更多**> **绑定/解绑IAM角色**。（注：仅支持为同批实例绑定同一个IAM角色，不支持批量多角色绑定）

4. 在绑定/解绑IAM角色弹窗中选择操作类型为**绑定**，并为实例选择IAM角色。（若无角色请先前往IAM角色列表创建授信实体为金山云服务的IAM角色。）

5. 单击确定，完成绑定。

   您也可以在创建KEC实例时，并在系统配置页面高级选项的实例IAM角色属性中为实例选择已创建好的实例IAM角色或者新建实例IAM角色

步骤三：在实例内部访问实例元数据URL获取STS临时凭证

1.启动KEC，KEC调用STS API AssumeRole去获取该IAM角色的临时安全令牌。 2.STS将临时安全令牌返回给KEC。 3.KEC将通过实例元数据将临时安全令牌传递给KEC实例中的应用程序。 **（1）Linux系统** 通过实例元数据可以获取临时安全令牌及过期时间等信息。

请求示例
```
curl http://global.cloudinit.sdns.ksyun.com:8775/latest/iam
```

返回示例
```
{
<SecretAccessKey>wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY</SecretAccessKey>
<Expiration>2017-07-15T23:28:33.359Z</Expiration>
<AccessKeyId>AKIAIOSFODNN7EXAMPLE</AccessKeyId>
<SecurityToken>V1xxxxxxxxxxxx</SecurityToken>
<IamRoleName>XXXXX</IamRoleName>
}
```

（2）Windows系统

- 若安装的windows系统支持powershell和curl命令，则获取临时安全令牌及过期时间等信息的方法同Linux系统。
- 若安装的windows系统不支持，则可使用其他http请求调试工具，如postman、Chrome插件等（需要自行安装）访问http://global.cloudinit.sdns.ksyun.com:8775/latest/iam获取临时安全令牌及过期时间等信息。

4.应用程序使用临时安全令牌访问金山云API。

限制子用户的访问IP地址

访问控制可以限制用户只能通过指定的IP地址访问企业的云资源，从而增强访问安全性。

背景介绍

企业A买了很多金山云资源开展业务，为了确保其业务和数据安全，企业希望用户只能通过企业专用网络的IP地址访问金山云，而不是在任意地点都可以访问金山云。

方案介绍

您可以根据需要创建自定义策略，然后创建IAM子用户并为子用户授予对应权限，确保IAM子用户只能通过指定的IP地址访问金山云。

步骤一：创建自定义策略

1. 登录访问控制控制台。
2. 选择**权限管理** > **策略**，进入到权限策略管理页面。
3. 单击**自定义策略**页签，进入**自定义策略**列表页面。
4. 单击**新建策略**，进入新建自定义策略页面，输入策略名称和备注。
5. 在设置策略类型区域选择**策略语法**，然后编辑策略内容。

策略内容实例：
```
{
    "Version": "2015-11-01",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kec:*",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "ksc:SourceIp": [
                        "192.168.0.0/16"
                    ]
                }
            }
        }
    ]
}
```

6. 单击**确定**，完成自定义策略创建。

步骤二：创建IAM子用户

1. 登录访问控制控制台。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 单击**新建用户**按钮，进入新建用户页面。
4. 在新建用户页面用户登录信息区域按提示填写信息。

> **登录账号**：必填，为子用户的用户名，一旦创建无法修改。 **显示名称**：必填，方便按照自身业务定义使用者对应名称。 **邮箱**：选填，用于接收消息。 **手机号**：选填，用于接收消息。 **是否开启接收消息**：开启后，邮箱与手机号为必填内容。

5. 在**访问方式**区域，选择访问方式。为了保障账号安全，建议只选择一种登录方式。

   控制台访问：设置控制台登录密码、重置密码策略、多因素认证策略、操作保护策略，是否允许查看所有项目。 **编程访问**：自动为子用户用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问金山云。

6. 单击**确定**，完成子用户创建。

步骤三：为IAM用户授权

1. 登录访问控制控制台。
2. 选择**权限管理** > **授策略**。
3. 在**策略列表**页面，找到要授权的目标策略，单击**操作**列的**关联对象**按钮。
4. 在**关联对象**面板，选择要授权的IAM子用户。
5. 单击**确定**，完成权限添加。

只允许操作特定VPC下的路由数据

本文介绍如何通过IAM的权限管理功能，创建相应策略，从而对虚拟私有网络（VPC）进行VPC级别的权限管控需求。

背景

客户账号下有多个VPC，希望仅对子账号授予特定的VPC的权限，就可以实现子账号拥有操作该VPC下相应的资源数据。无需对VPC下的资源一一授权。

注意事项

当前仅支持通过授权到特定的VPC管理VPC下的路由数据。

操作步骤

1.创建IAM子用户。 具体操作见创建IAM子用户。

2.创建自定义策略。 更多信息，请参见创建自定义策略和下文的权限策略示例。 3.为IAM子用户授权。 具体操作，请参见为为IAM子用户授权。

权限策略示例

示例：授权子用户具有VPID：43d6c641-3d08-4415-***-f49341d75d0b下所有路由的删除权限，其他VPC下路由无删除权限。

```
{
    "Version": "2015-11-01",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:deleteroute"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "ksc:ResourceAttribute": [
                        "krn:ksc:vpc:cn-shanghai-3:200010***6:vpc/43d6c641-3d08-4415-***-f49341d75d0b"
                    ]
                }
            }
        }
    ]
}
```

说明： （1）策略语言需要将指定的VPC资源的信息用“Condition”条件来描述。条件关键词为ksc:ResourceAttribute。 （2）VPC的资源需要使用VPC资源对应的KRN格式，当前仅支持完全匹配，不支持使用通配符。