图引擎服务

最佳实践

文档版本 01

发布日期 2025-09-29

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2025。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 用户授权最小化权限实践.....1

 版权所有 © 华为云计算技术有限公司

1 用户授权最小化权限实践

实践场景及目标

假设某工程师专职负责图引擎服务相关工作，且仅需要GES服务的管理员权限。则在为该用户授权时，如果项目管理员直接赋予该工程师IAM账号GES FullAccess或GES Administrator权限，则会出现非必需权限过大的风险：GES FullAccess系统策略预置了依赖服务（ECS、VPC服务）的所有权限，GES Administrator角色依赖Server Administrator权限和Tenant Guest权限，均会导致其拥有ECS和VPC服务的管理员权限。

为解决此问题，项目管理员可以按照如下解决方案进行权限最小化配置，这样既能满足实际业务使用，也避免了权限过大的风险。

1. 创建自定义策略，包含GES服务所有权限及GES服务依赖服务最小权限合集。
2. 创建用户组，将该工程师IAM账号加入到用户组中，并授予上一步中创建的自定义策略。

操作流程

1. 创建自定义策略：创建自定义策略，授予GES服务所有权限以及GES服务依赖服务的最小权限合集。
2. 创建用户组并授权：创建用户组，并授予上一步中创建的自定义策略。
3. 创建IAM用户并加入用户组：为工程师创建IAM账号，并加入到用户组中。

创建自定义策略

步骤1 使用华为账号登录“统一身份认证服务 IAM”控制台。

步骤2 在IAM服务控制台中，单击“权限管理 > 权限”，在权限页面单击右上方的“创建自定义策略”。

图 1-1 创建自定义策略

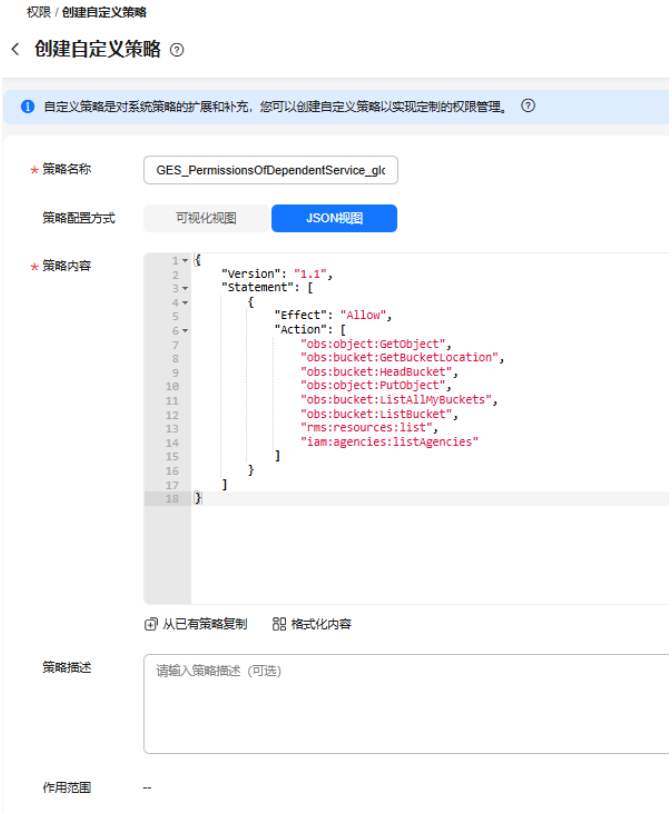
版权所有 © 华为云计算技术有限公司

步骤3 在“创建自定义策略”界面，策略配置方式切换至JSON视图，然后按照如下策略内容，分别创建GES_PermissionsOfDependentService_global和GES_PermissionsOfDependentService_region自定义策略。

说明

创建自定义策略时，暂不支持同时选全局级云服务和项目级云服务，因此需要将依赖服务自定义策略拆分为两条分别创建。

图 1-2 创建自定义策略示例



依赖的全局级（global级）云服务的自定义策略GES_PermissionsOfDependentService_global：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:GetBucketLocation",
                "obs:bucket:HeadBucket",
                "obs:object:PutObject",
                "obs:bucket:ListAllMyBuckets",
                "obs:bucket:ListBucket",
                "rms:resources:list",
                "tms:*:list",
                "eps:enterpriseProjects:list",
                "eps:enterpriseProjects:get",
                "iam:users:listUsers",
                "iam:agencies:listAgencies",
                "iam:permissions:listRolesForAgencyOnDomain",
                "iam:permissions:listRolesForAgencyOnProject",
                "iam:permissions:listRolesForAgency"
```


版权所有 © 华为云计算技术有限公司

```
        ]
      }
    ]
}
```

依赖的项目级（region级）云服务的自定义策略GES_PermissionsOfDependentService_region：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ges:*:*",
                "ecs:cloudServerNics:update",
                "ecs:flavors:get",
                "ecs:cloudServerFlavors:get",
                "ecs:availabilityZones:list",
                "evs:types:get",
                "vpc:ports:get",
                "vpc:ports:create",
                "vpc:ports:update",
                "vpc:ports:delete",
                "vpc:quotas:list",
                "vpc:securityGroups:get",
                "vpc:subnets:get",
                "vpc:vpcs:list",
                "vpc:vpcs:get",
                "ces:*:list*",
                "ces:*:get*",
                "lts:*:list",
                "lts:*:get"
            ]
        }
    ]
}
```

说明

- 当图实例需要绑定EIP时，全局级策略GES_PermissionsOfDependentService_global需要增加以下action用于创建委托：

  "iam:roles:listRoles","iam:roles:createRole","iam:permissions:grantRoleToAgencyOnDomain","iam:agencies:getAgency","iam:agencies:createAgency","iam:roles:updateRole","iam:permissions:grantRoleToAgency","iam:permissions:grantRoleToAgencyOnProject"

  项目级策略GES_PermissionsOfDependentService_region需要增加以下action用于绑定eip：

  "vpc:publicIps:get","vpc:publicIps:list","vpc:publicIps:update"

- 当需要在创建图实例时自动创建eip时，项目级策略GES_PermissionsOfDependentService_region需要增加以下action用于创建eip：

  "vpc:publicIps:create"

- 当需要在删除图实例时删除绑定的eip时，项目级策略GES_PermissionsOfDependentService_region需要增加以下action用于删除eip：

  "vpc:publicIps:delete"

----结束

创建用户组并授权

步骤1 在IAM服务控制台中，左侧导航窗格中，选择“用户组”，单击右上角的“创建用户组”。

 版权所有 © 华为云计算技术有限公司

图 1-3 创建用户组

步骤2 在“创建用户组”界面，输入用户组名称“GES_Policy”。

图 1-4 用户组名称

步骤3 单击“确定”，用户组创建完成，用户组列表中显示新创建的用户组。

步骤4 在用户组列表中，单击新建用户组右侧的“授权”。

图 1-5 用户组授权

步骤5 在搜索框中输入GES_PermissionsOfDependentService_global，勾选搜索到的自定义策略，单击“下一步”。

图 1-6 授权 global 自定义策略

步骤6 授权范围方案选择“全局服务资源”，单击“确定”，完成授权。

图 1-7 设置授权范围

步骤7 重复步骤4，在搜索框中输入GES_PermissionsOfDependentService_region，勾选搜索到的自定义策略，单击“下一步”。

版权所有 © 华为云计算技术有限公司

图 1-8 授权 region 自定义策略

步骤8 授权范围方案选择“指定区域项目资源”下需要授予的区域项目，单击“确定”，完成授权。

图 1-9 设置授权范围

----结束

创建 IAM 用户并加入用户组

步骤1 在IAM服务控制台中，左侧导航窗格中，选择“用户”，单击右上方的“创建用户”。

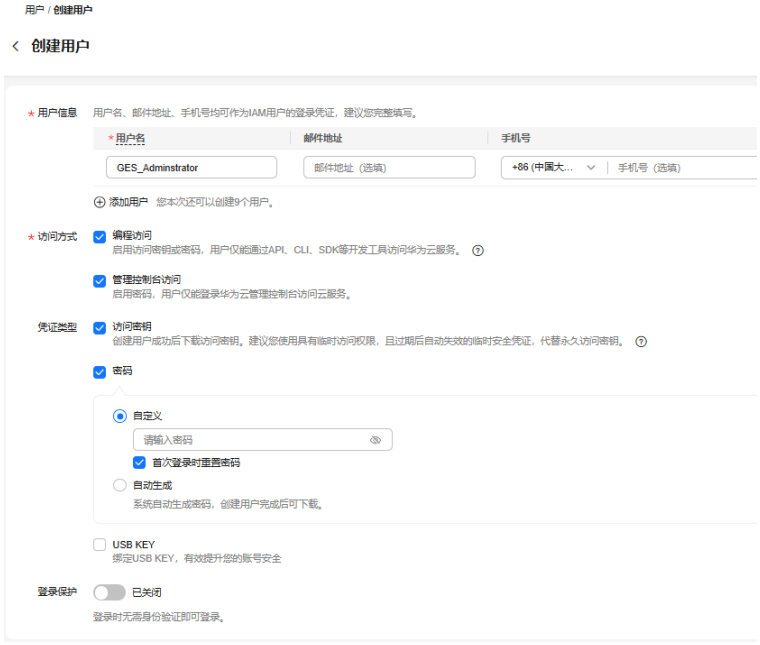
图 1-10 创建用户

步骤2 在“创建用户”页面按照下图配置“用户信息”，完成配置后单击页面右下角的“下一步”。

- 用户信息：用户名自定义填写。
- 访问方式：选择“管理控制台访问”和“编程访问”。
- 凭证类型：勾选访问密钥和密码，推荐为用户自定义初始密码。
- 登录保护：根据实际需求选择。

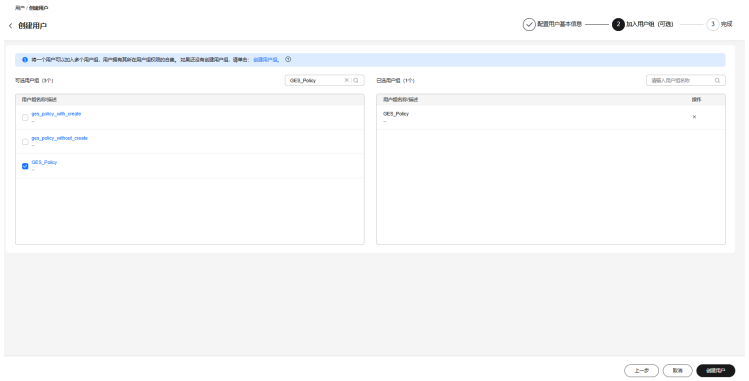
版权所有 © 华为云计算技术有限公司

图 1-11 配置用户信息



步骤3 选择将用户加入到GES_Policy用户组，单击页面右下角的“创建用户”。

图 1-12 加入用户组



----结束

用户登录并验证权限

步骤1 以**创建IAM用户并加入用户组**章节中新建的IAM账号登录华为云控制台，切换至授权区域。

步骤2 在“服务列表”中选择图引擎服务，进入图引擎服务控制台。

步骤3 进入图引擎服务控制台的各个页面，验证各项功能是否正常。

----结束

版权所有 © 华为云计算技术有限公司