

Welcome

MANAGED INSTANCE

产品简介 >

快速入门

MAXGROUP

产品简介 >

基础介绍

产品优势

定价策略

快速入门 >

准备工作 >

AWS

阿里云

安装与启动 >

功能验证 >

Tag与功能

最佳实践 >

常见问题

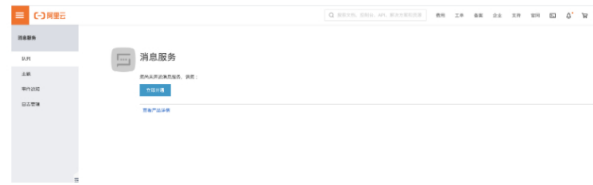
相关协议

Powered by GitBook

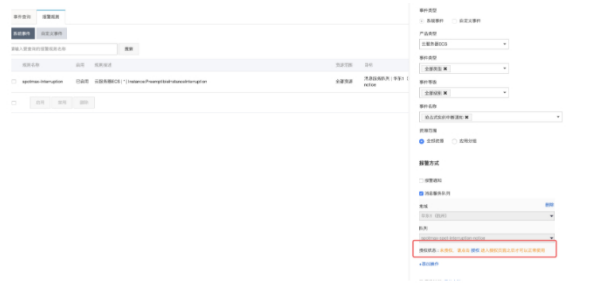
阿里云

服务开启：

1、注意检查云监控和MNS，需提前启用这两个服务，否则无法创建max_group所使用的依赖环境。（如已启用请忽略）



2、确保云监控授权给mns



授权

方法一：RAM角色授权

1、推荐使用，创建RAM角色



创建 RAM 角色

1 选择类型 — 2 配置角色 — 3 创建完成

当前可信实体类型

- 阿里云账号
受信云账号下的子用户可以通过扮演该RAM角色来访问您的云资源。受信云账号可以是当前云账号，也可以是其他云账号
- 阿里云服务
受信云服务可以通过扮演RAM角色来访问您的云资源
- 身份提供商
身份提供商功能，通过设置SSO可以实现从企业本地账号系统登录阿里云控制台，帮您解决企业的统一用户登录认证要求

创建 RAM 角色

1 选择类型 — 2 配置角色 — 3 创建完成

选择可信实体类型

阿里云服务

角色类型

 普通服务角色 服务关联角色

* 角色名称

xuanjiliang

不超过64个字符，允许英文字母、数字，或“-”

备注

* 选择受信服务

云服务器

Edit on GitHub

CONTENTS

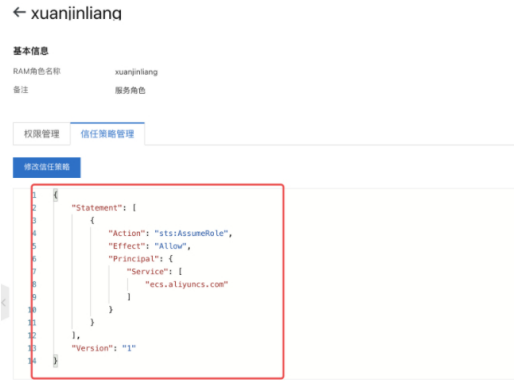
服务开启：

授权

方法一：RAM角色授权

方法二：RAM用户授权，需...

点击完成，用户创建成功，如下内容：



2、点击权限管理，授权策略如下：

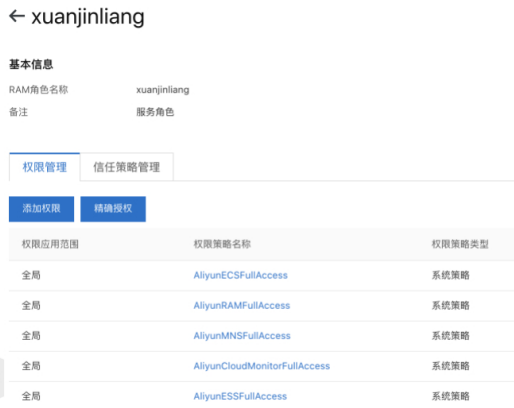
[AliyunECSFullAccess](#)

[AliyunMNSFullAccess](#)

[AliyunCloudMonitorFullAccess](#)

[AliyunESSFullAccess](#)

[AliyunRAMFullAccess](#)



创建实例时，选择创建好的RAM角色



方法二：RAM用户授权，需要AK

1、使用RAM用户对ecs进行授权，授权策略如下：

[AliyunECSFullAccess](#)

[AliyunMNSFullAccess](#)

[AliyunCloudMonitorFullAccess](#)

[AliyunESSFullAccess](#)



名称	AccessKey ID	AccessKey Secret	到期时间	操作
主账号	AKIAI44QH8DHBDF3T3466	*****	2020-01-01 00:00:00	删除
RAM用户	AKIAI44QH8DHBDF3T3466	*****	2020-01-01 00:00:00	删除
RAM用户	AKIAI44QH8DHBDF3T3466	*****	2020-01-01 00:00:00	删除
RAM用户	AKIAI44QH8DHBDF3T3466	*****	2020-01-01 00:00:00	删除

完成用户授权后，需要在系统中指定accessId和accessKeySecret。

```

1 echo 'export ALI_ACCESS_KEY_ID="accessId"' >> /etc/profile
2 echo 'export ALI_ACCESS_SECRET="accessKeySecret"' >> /etc/profile
3 source /etc/profile

```