

# 小微金服 Login 系统服务器申请流程指南

## 一、流程描述：

Aops 主要解决用户申请测试和线上机器账号的问题，申请机器在某些条件下需要机器的 pe 责任人审核，审核通过后调用工具系统接口；机器审核的条件如下：

### 目前逻辑

\*1.\*高风险应用：如“公共服务-DB”等，可自定义配置。无论是否 sudo，均需要审批，审批人逻辑和其他相同。

\*2.\*审批人规则：用户申请-需求评估（安全）-主管审批-复审-系统处理；

## 二、帐号申请指南

### 新帐号申请步骤：

1. 申请人在服务器帐号自助平台（<http://account.taobao.org:9999/>）完成帐号注册和密码设置，统一使用个人邮箱前缀作为 IDC 服务器登录帐号，唯一标示用户身份；密码必须符合密码策略才能完成设置。

2. 申请人在 AOPS 平台（<http://aops.alibaba-inc.com/workflow/account/new/>）上提交帐号添加申请；

步骤一：小微 login 系统首先要申请 login 系统跳板机，选择应用分组 **ops\_login\_alipay** 的访问权限，且只能申请**一般用户**权限，其他申请直接拒绝（如下图）。

若账号添加失败，请用其中一台服务器直接到idcfree提单：点击[这里](#)。故障类型选择“账号问题”，并贴上AOPS申请单链接或单号。

提交人信息

暮去

查看

是否替人申请

☐ 选中表示代人申请

申请类型(\*)

帐号添加

设备OS类型(\*)

Linux

请注意：OS类型切换后，之前添加的设备列表会被清空

权限期限(\*)

1周

申请内容(\*)

IP地址

主机名

应用分组

请输入应用分组名称或任意一个IP/主机名，系统会自动关联到对应的应用分组

查询

点击查询按钮，添加设备到待申请列表（请注意：跳板机申请 应用分组 ops\_login\_prod 的访问权限，且只能申请 一般用户 权限）

	应用分组名称	应用名	应用分组PE	角色/权限
<input checked="" type="checkbox"/>	ops_login_alipay	ops_login	暮去, 兴旺, 伯越, 镇光	<input type="radio"/> 系统管理员 <input type="radio"/> 应用管理员 <input checked="" type="radio"/> 一般用户

☒ 全选 批量删除 | 批量设置 ☐ 系统管理员 ☐ 应用管理员 ☐ 一般用户

步骤二：用户申请自己所需服务器权限，角色和权限请下方账号权限分类说明。

3. 申请完成，帐号管理系统自动完成帐号添加操作（会同时在目标服务器和登录跳转服务器(login1.zue.alibaba.org、login1.ztg.alibaba.org)上添加帐号），并将操作结果邮件通知申请人；

5. 如果拒绝申请，则申请无效，流程结束。

6. 申请人可以先远程登录到跳转服务器（login1.zue.alibaba.org\

login1.ztg.alibaba.org)，然后再远程登录到目的服务器确认添加帐号是否已正常添加。

新账号权限分类说明：

系统管理员，SA，PE，现场运维，监控，技术安全等可拥有的服务器帐号，拥有大部分 sudo 权限。可查看，修改应用或系统配置。

应用管理员，核心开发可拥有的服务器帐号，拥有以 admin 身份执行命令的 sudo 权限。可查看，修改应用配置。

一般用户，只读服务器帐号，一般分配给开发人员协助排查应用故障原因使用。无 sudo 权限，只能查看应用或系统配置，无权修改配置。

当前的默认授权：

默认授权的效果：申请人提交申请后，立即添加，无审批环节

任何人都可以申请成为测试服务器的一般用户或管理员；

任何人都可以申请成为非核心服务器组的一般用户；

责任人可以申请成为其负责服务器的管理员或一般用户；

责任人可以替任何人申请其负责服务器的管理员或一般用户角色。

登录方法：

先登录相应环境的跳板机，然后从跳板机上 ssh 您要登录的目标机器。

生产机房跳板机：login1.zue.alibaba.org\login1.ztg.alibaba.org