

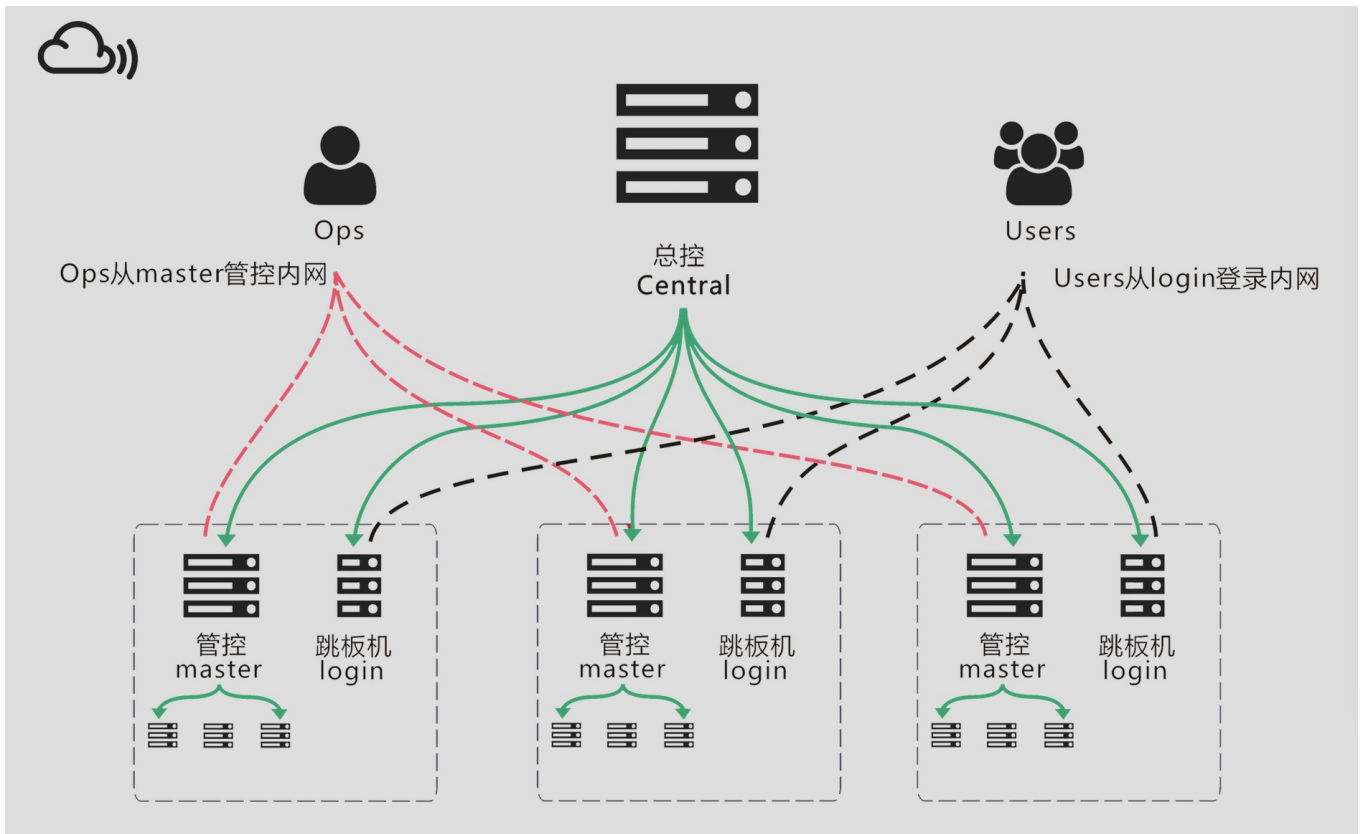
企业一体化运维管控平台

xabcloud.com

目前国内各大互联网企业面临几项基础运维问题,业界没有企业级的解决方案:

- 日益增多的主机无法统一管控
- 异地多网络节点机房,没有统一调度管理
- 企业内部技术人员众多,没有成熟的权限管理平台,大部分通过传统的一些简易的运维脚本完成内部员工账号的创建,流程混乱,权限只分配不管理,账号容易泄露,内网安全堪忧,时刻面临账号被暴力破解的风险
- 企业应用产品没有成熟易用的实时集群监控,历史监控,实时报警,大部分采用开源的一些监控产品,维护成本非常高,而且难以满足企业内部很多个性化需求,需要专业的运维工程师维护管理,成本大
- 生产内网无有效的安全审计,无法有效的完成故障追责以企业本身的内网安全审计痛点
- 无有效的批量部署平台,大部分采用一些脚本程序,人工的完成企业内部部署需求,效率低下且不可靠
- 无有效的企业内部工单系统,工作交流不方便,影响团队效率

悠云如何解决？



业务逻辑

三种角色:技术主管(Admin),运维工程师(Ops),开发工程师(Dev)

Admin系统初始化部署给予创建,默认注册均是Dev权限视图,Admin可以通过管理模块赋予某职员为Ops权限,从而协同处理日常权限审批,运维工单,处理日常报警等工作

一体化Ops平台(又名“小矩阵”)基本架构如上图,若某企业有三个网络环境,那么每个网络中至少需要有一台master机器接管该网络中的所有服务器,供管理人员进行管控操作;至少需要有一台login机器作为该网络区域的统一登录入口,供开发人员登录该内网。三个网络环境共三台master机器和三台login机器又由总控central机器调度管理,实现通过Web控制台对所管控的各个网络节点成千上万台机器的统一管控。

解决问题

- 非常安全,高效,易用的互联网企业跳板机系统(淘汰传统堡垒机)
- 生产机器自助式权限申请,审批,到期提醒,过期清理,解决企业客户,成百上千台机器,众多技术人员日常登录生产机器的权限管理问题痛点
- 安全审计,什么时间,什么人,在哪台机器,做过什么操作,系统都有详细记录,方便故障追踪和安全审查,同时提供操作人的全输入输出流信息,可以回放完整的操作过程

- 以企业应用组为维度,机房总览,实时监控,历史监控,以及自定义阈值报警,信息打通企业微信,让客户对自己云上业务系统的运行了如指掌
- 基础环境批量部署,比如JAVA环境,nginx,Redis等等基础环境,模版化部署,根据企业自己的规范结构,定制自己的部署模版
- 非常简洁易用的企业工单系统,促进同事之间直接发起日常工作配合,提高团队效率
- 团队协作,可以赋予Ops权限,团队协同管理更高效
- 全终端的平台系统,无论是手机还是Web端或者手持pad均可完美展现
- 支持异地多机房,无论云上有几个网络环境,无论是在阿里云,腾讯云,AWS 等或是自建机房等,均可完美轻量接入

平台特点

- 核心模块采用C语言实现,运行效率非常高
- 我们自研的全线生产RSA对无感知更替极其安全可靠,可以满足金融客户高安全需求,同时我们内置防火墙系统,可以对全线各个网络节点有效的统一管控设置
- 异地多网络环境完美支持,理论上支持无限扩展,方便企业对各个网络节点统一管控
- 分布式的设计方案,不仅可以满足中小企业成百上千台机器的管控,而且可以支持超大互联网企业上万台机器的统一管控

技术选型

数据存储: influxdb,redis,postgresql

开发语言: C,Lua,Node,Python

Agent: salt-minion

多语言融合开发,根据不同的业务逻辑选择最合适的语言开发对应的模块,从而使得系统运行效率更高,代码更加简洁,和国际一线互联网企业接轨,选择了salt作为系统agent.

图文介绍

1.这是开发人员视图,有企业跳板机入口,有权限的机器列表,历史登录login记录

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

75

报警 08-11 14:04:38 Sys
load 2.00 已恢复常态 [异常时长 1.1 分钟]
tmallbuy-10.141.41.246-bj
全部

login入口IP

Beijing: 123.206.82.57
Shanghai: 115.159.58.28

normal权限机器列表

tmallbuy-10.131.168.179-sh
tmallbuy-10.141.41.246-bj

近期登陆login概况

- 2016-08-11 01:12:47 (AM) from 115.198.130.1
- 2016-08-10 23:20:14 (PM) from 115.198.130.1
- 2016-08-10 23:18:42 (PM) from 115.198.130.182 [杭州 浙江 中国]
- 2016-08-10 23:17:45 (PM) from 115.198.130.182 [杭州 浙江 中国]
- 2016-08-10 22:55:58 (PM) from 115.198.130.182 [杭州 浙江 中国]
- 2016-08-10 21:04:25 (PM) from 125.119.121.171 [杭州 浙江 中国]
- 2016-08-10 20:52:43 (PM) from 125.119.121.171 [杭州 浙江 中国]
- 2016-08-10 17:37:32 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 17:36:41 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 17:24:22 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 16:14:06 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 15:09:59 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 14:59:15 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 14:08:00 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 13:56:59 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 13:55:05 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-10 13:54:50 (PM) from 115.196.194.76 [杭州 浙江 中国]
- 2016-08-07 10:18:21 (AM) from 10.131.173.231 [局域网 局域网]
- 2016-08-05 14:33:34 (PM) from 115.198.136.237 [杭州 浙江 中国]
- 2016-08-05 14:33:31 (PM) from 115.198.136.237 [杭州 浙江 中国]
- 2016-08-05 14:31:51 (PM) from 10.131.173.231 [局域网 局域网]

2.这是机房总览，以应用组维度展现

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

109

机房总数: 2个
机器总数: 2台
应用分组: 1组

Beijing: 1台
应用分组: 1组

Shanghai: 1台
应用分组: 1组

tmallbuy

tmallbuy-10.131.168.179-sh
tmallbuy-10.141.41.246-bj

Beijing 应用分布

2

1

0

tmallbuy

Shanghai 应用分布

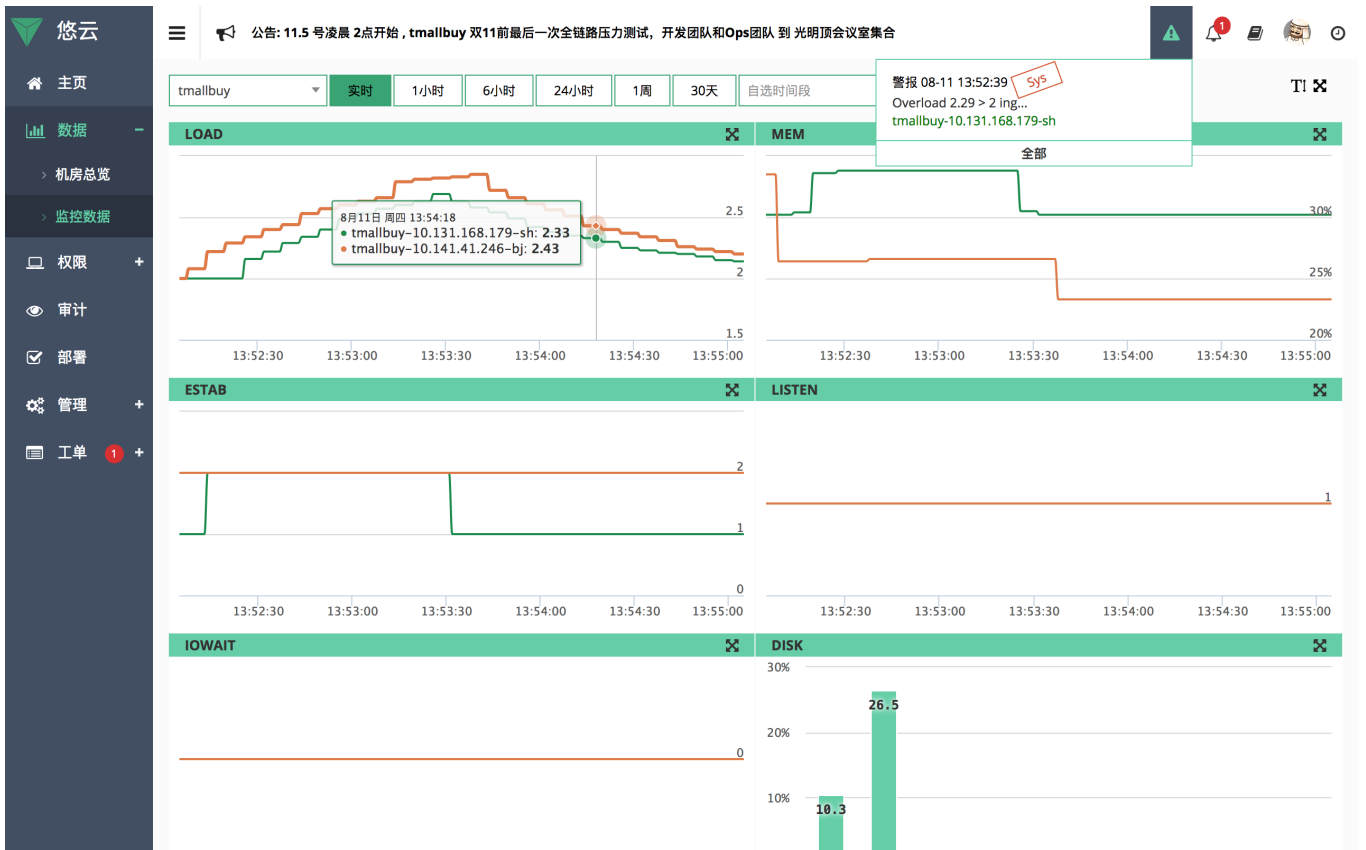
2

1

0

tmallbuy

3.这是应用集群实时监控和历史监控数据



4.开发人员申请业务机器登录权限

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

登录用户: **ywgx**

权限类型: normal sudo

权限时长: 7天 28天

应用分组: tmallbuy

机器列表: tmallbuy-10.131.168.179-sh,tmallbuy-10.141.41.246-bj

确认

5.技术主管审核审批

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

通过 拒绝

qq1040733670 [08-09 17:38:51]

- tmallbuy-10.131.168.179-sh [7天]
- tmallbuy-10.141.41.246-bj [7天]

通过 拒绝

qq314833261 [08-09 19:15:04]

- tmallbuy-10.141.41.246-bj [sudo, 28天]
- tmallbuy-10.131.168.179-sh [sudo, 28天]

通过 拒绝

w3help [08-10 11:22:41]

- tmallbuy-10.141.41.246-bj [28天]
- tmallbuy-10.131.168.179-sh [28天]

通过 拒绝

ywgx [08-11 14:11:59]

- tmallbuy-10.131.168.179-sh [7天]
- tmallbuy-10.141.41.246-bj [7天]

通过 拒绝

6.安全审计, 什么时间? 什么人? 在哪台机器? 执行过什么操作?

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

Beijing ywgx 应用 搜索操作

时间	用户	机器	操作
08-10 23:29:01	ywgx	tmallbuy-10.141.41.246-bj	vim /etc/tmpfiles.d/python.conf
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/id -u
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/grep -qi ^COLOR.*none /etc/DIR_COLORS
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/dircolors --sh /etc/DIR_COLORS
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/tput colors
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/tty -s
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	grep -qsi ^COLOR.*none /etc/GREP_COLORS
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/libexec/grepconf.sh -c
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	ls /etc/bash_completion.d
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	id -un
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	id -gn
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/hostname
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	id -un
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	-bash
08-10 23:25:31	ywgx	tmallbuy-10.141.41.246-bj	tmux
08-10 23:24:13	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/id -u
08-10 23:24:13	ywgx	tmallbuy-10.141.41.246-bj	/usr/bin/grep -qi ^COLOR.*none /etc/DIR_COLORS

7.新机器基础环境 批量部署

悠云

公告: 11.5 号凌晨 2点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

flume
tmallbuy-10.131.168.179-sh
tmallbuy-10.141.41.246-bj

部署

8.运维公告

悠云

公告: 11.5 号凌晨 2点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

公告: 11.5 号凌晨 2点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

发布 清空

9.日常工单需求

悠云

- 主页
- 数据 +
- 权限 +
- 审计
- 部署
- 管理 +
- 工单 1 -
 - 创建
 - 已收到 1
 - 已发送
 - 草稿
 - 全部 4

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

× ywgx

双11就要来了, 我们 商城 store 扩容 20台机器 什么时候到位? |

发送 附件

10.日常警报和日常信息

悠云

- 主页
- 数据 -
 - 机房总览
 - 监控数据
- 权限 +
- 审计
- 部署
- 管理 +
- 工单 2 +

公告: 11.5 号凌晨 2 点开始, tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合

tmallbuy

实时 1小时 6小时 24小时 1周 30天 自选时间段

警报 08-11 14:14:44 Sys
load 2.00 已恢复正常 [异常时长 0.6 分钟]
tmallbuy-10.141.41.246-bj

警报 08-11 14:12:08 Sys
Overload 2.06 > 2 ing...
tmallbuy-10.141.41.246-bj

警报 08-11 14:11:50 Sys
Overload 2.08 > 2
tmallbuy-10.141.41.246-bj

警报 08-11 14:10:38 Sys
load 2.00 已恢复正常 [异常时长 2.7 分钟]
tmallbuy-10.141.41.246-bj

警报 08-11 14:08:57 Sys
load 2.00 已恢复正常 [异常时长 1.5 分钟]
tmallbuy-10.131.168.179-sh

警报 08-11 14:05:09 Sys
Overload 2.22 > 2 ing...
tmallbuy-10.131.168.179-sh

全部

TI

LOAD

MEM

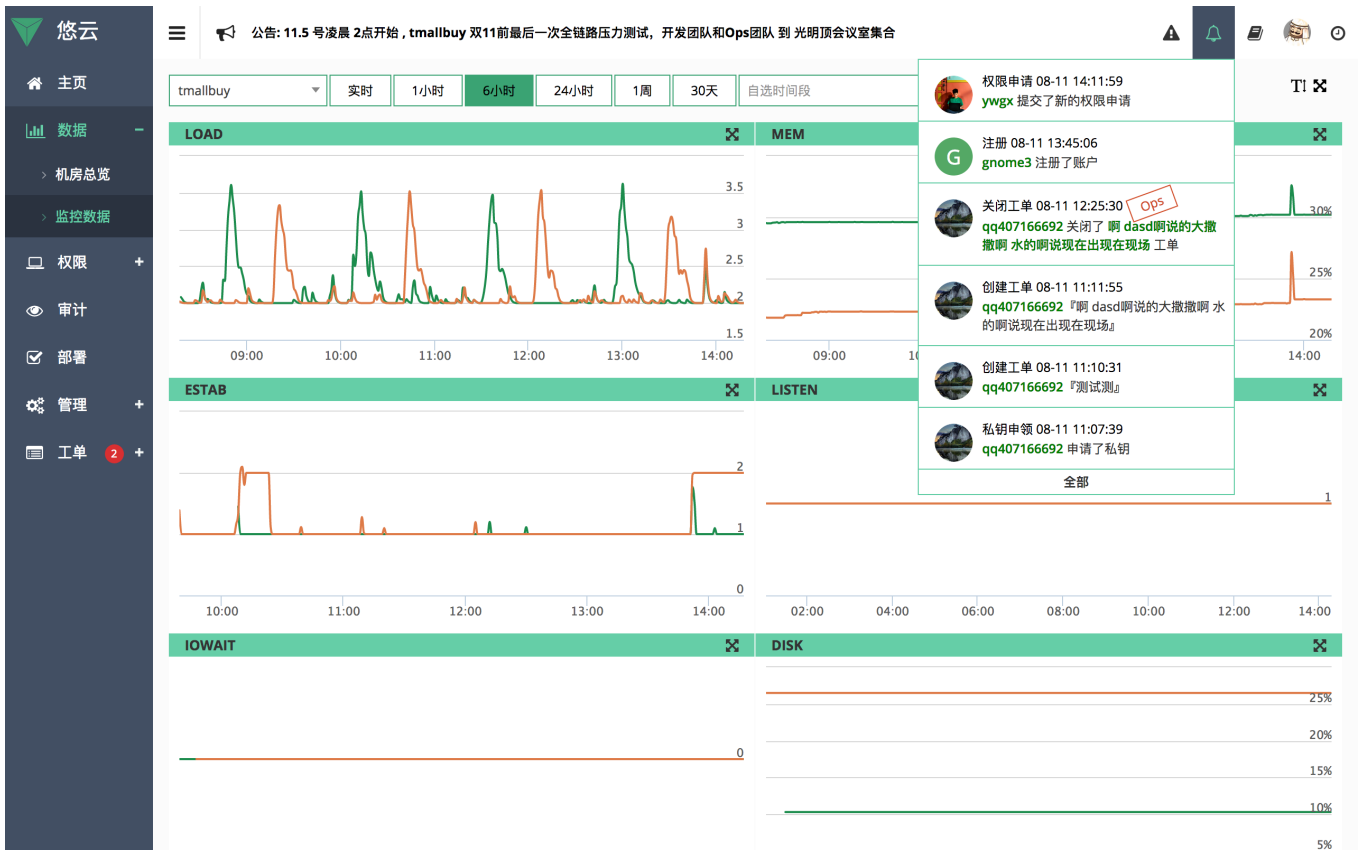
ESTAB

LISTEN

IOWAIT

DISK

全部



11.开发人员登录生产机器

```

=====
w3help:44 ywgx:33 qq407166692:9 qq1040733670:7 xufengtian14:5 admin:4
ywgx: 1
2016-08-13) $ssh 01 -----> tmallbuy-10.141.41.246-bj
=====

谁要是没有强烈的感情, 它就不会具有强烈的志向, 也就不能够热烈地把这个志向体现于事业之上。
=====

[ywgx@login-123.206.82.57-bj 14:19 ~]
$ ssh 01
Last login: Thu Aug 11 01:12:51 2016 from 10.141.60.94
公告: 11.5 号凌晨 2点开始 , tmallbuy 双11前最后一次全链路压力测试, 开发团队和Ops团队 到 光明顶会议室集合
ywgx@tmallbuy-10.141.41.246-bj ~$

```

