



云安全服务实践

爱奇艺 李晗

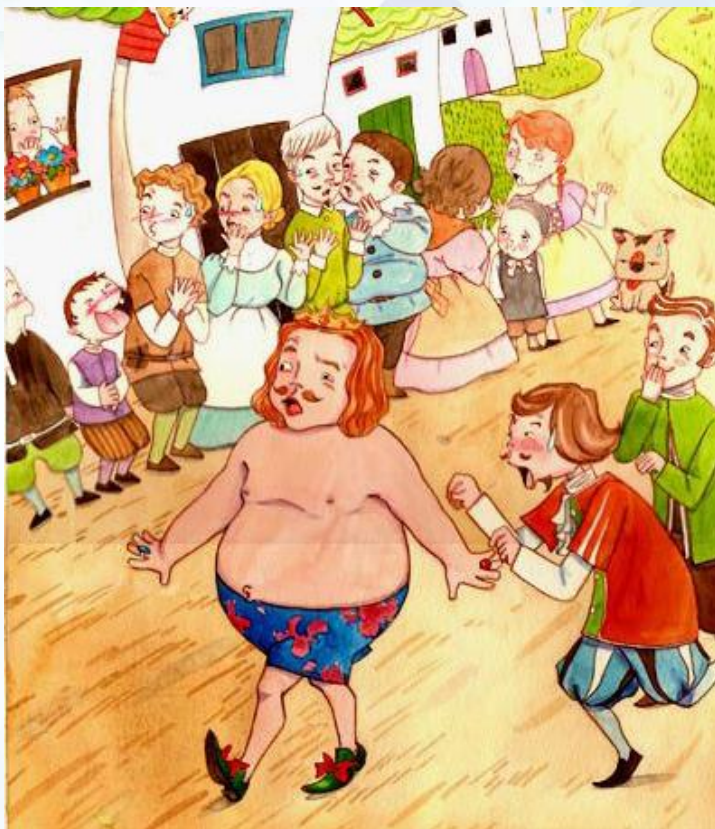
苦逼的安全工程师

- 都说“三分技术，七分管理”，互联网的安全工程师是“运维+开发+测试+QA”。
- “安全是互联网公司的生命”变成口号，普通员工感受不强烈，要做到安全也不容易。



互联网公司安全现状

- 对安全，没有出过大事就不太重视。
- 上线开发维护任务繁重，安全的事情只好先放一放。
- 普遍安全意识不好，反复强调却仍然发生各类低级错误。
- 安全好像只是安全工程师的事情。



何为云安全服务

- SecaaS，安全即服务
 - 开放服务接口，唾手可得和更加简单的安全服务
 - 按需申请和使用
 - 提供配套的监控和验证服务
- 基于云
 - 享受云平台的服务，专注安全业务，快速迭代开发
 - 弹性计算框架，自动扩展

爱奇艺网络架构简介

近十个DNS解析点

DNS解析，请求就近访问

数十个nginx反向代理点

反向代理到CDN节点

数百个CDN节点

媒资分发等

会员认证，搜索，推荐，广告等服务

云平台：云存储，云编码，会员，各类云服务和应用

爱奇艺云平台简介

应用

媒资系统

广告

推荐

账号

视频云开放
平台

...

服务

计算服务

数据服务

开发者服务

转码服务

内存数据库

公共组件库框架

MapReduce

备份、容灾

Client SDKs

弹性计算

数据平台

开发者和运维手册

平台

计算云

存储云

网络云

建立私有云的平台和服务架构，将资源服务化，全面为业务系统提供计算、存储、网络平台以及建立在平台之上的各类服务

PS

我们的云安全服务

- 跳板机服务
- 在线站点和主机扫描测试服务
- 主机入侵检测服务
- WEB防火墙服务

跳板机服务

- 业务部门按需申请，并指定一名管理员
- 支持操作记录监控，统计和报警

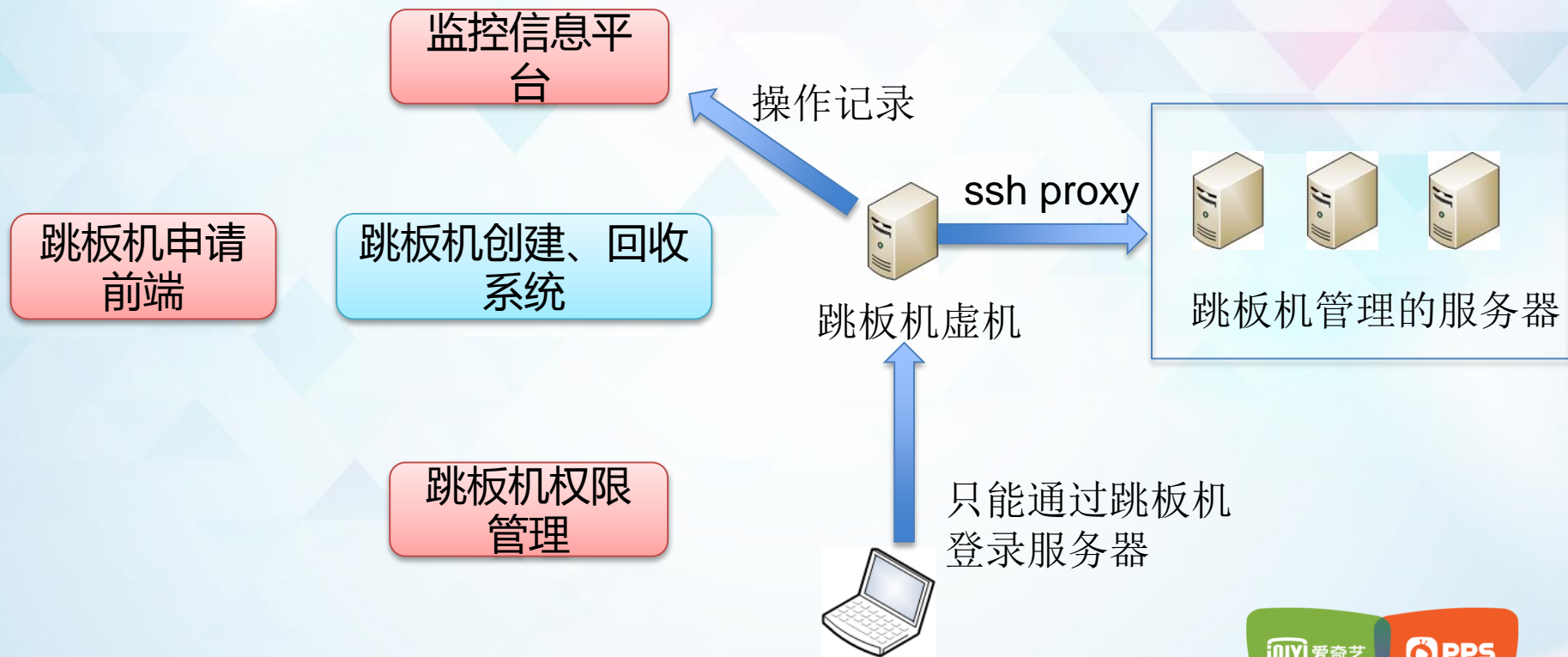
跳板机Session

首页 > 运维审计 > 跳板机Session 结果

来源IP: 目的IP: 用户名:
Session开始时间: Session结束时间: [查询](#)

ID	用户名	跳板机IP	来源IP	开始时间	结束时间
30086	li	10.10.10.10	10.10.10.10	2013-12-11 16:40:29	2013-12-11 17:13:00
30085	li	10.10.10.10	10.10.10.10	2013-12-11 15:38:33	2013-12-11 17:12:18
30084	li	10.10.10.10	10.10.10.10	2013-12-11 15:34:34	2013-12-11 15:34:36
30083	li	10.10.10.10	10.10.10.10	2013-12-11 15:02:14	2013-12-11 15:35:01
30082	li	10.10.10.10	10.10.10.10	2013-12-11 14:28:47	2013-12-11 18:15:22

跳板机服务



在线站点和主机扫描测试服务

- 提供包括xss，sql注入，弱密码，信息泄露等扫描服务
- 按需申请，即时发现问题即时处理

 云安全服务平台 [首页](#) [扫描队列](#) [帮助中心](#) [关于我们](#)

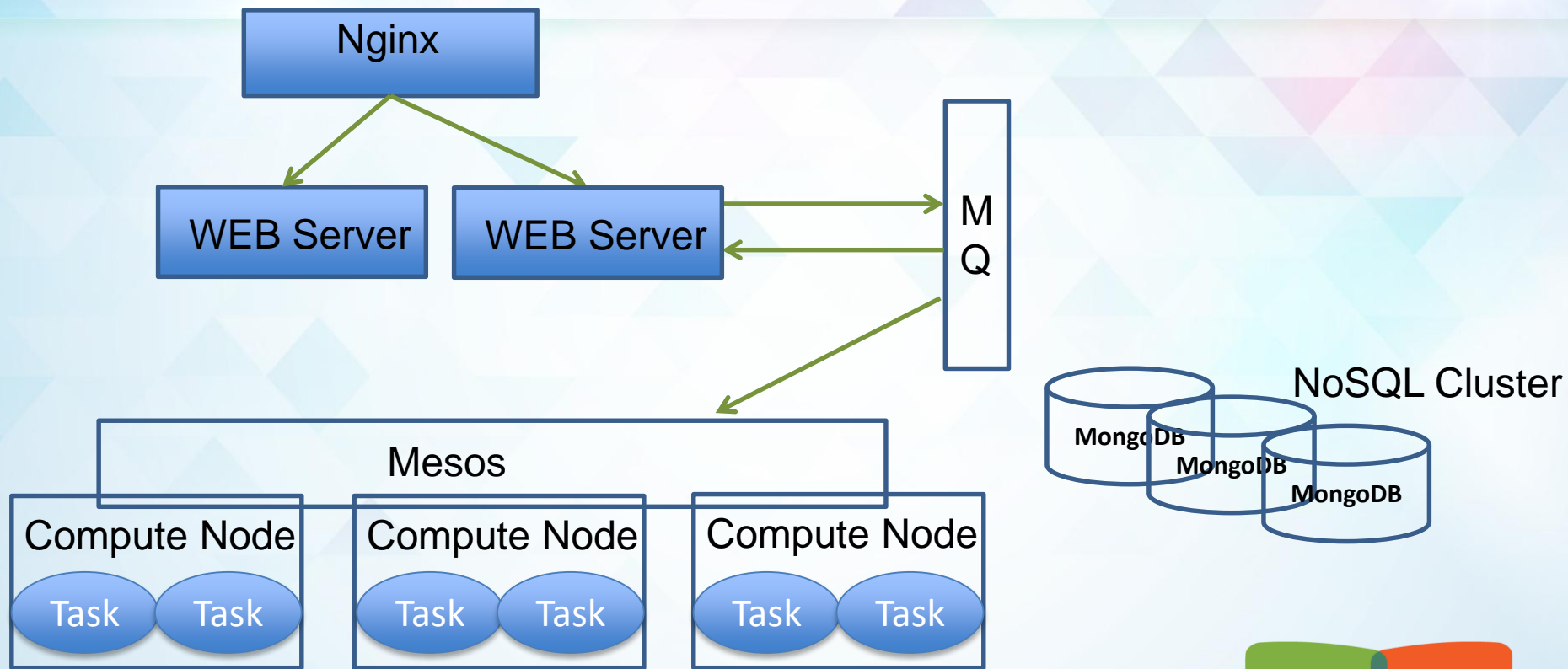
* * [AD认证登录](#)

Cloud Scanner 

提示：请先用AD账号登录，再执行扫描和查询操作

开始扫描


在线站点和主机扫描服务



主机入侵检测服务

- 为在线主机提供HIDS服务
- 支持监控、统计和报警

主机地址:




-

Qiyi

▼

公司邮箱:



@qiyi.com

申请

查看

主机入侵检测服务

在线主机入侵
检测注册

一键部署agent

入侵检测监控
平台

```
# wget http://[redacted]/dl/ossec/install/install-qiyi.sh&&sh install-qiyi.sh
```

agent



agent



agent



采集数据

策略更新

入侵检测云服
务

WEB防火墙服务

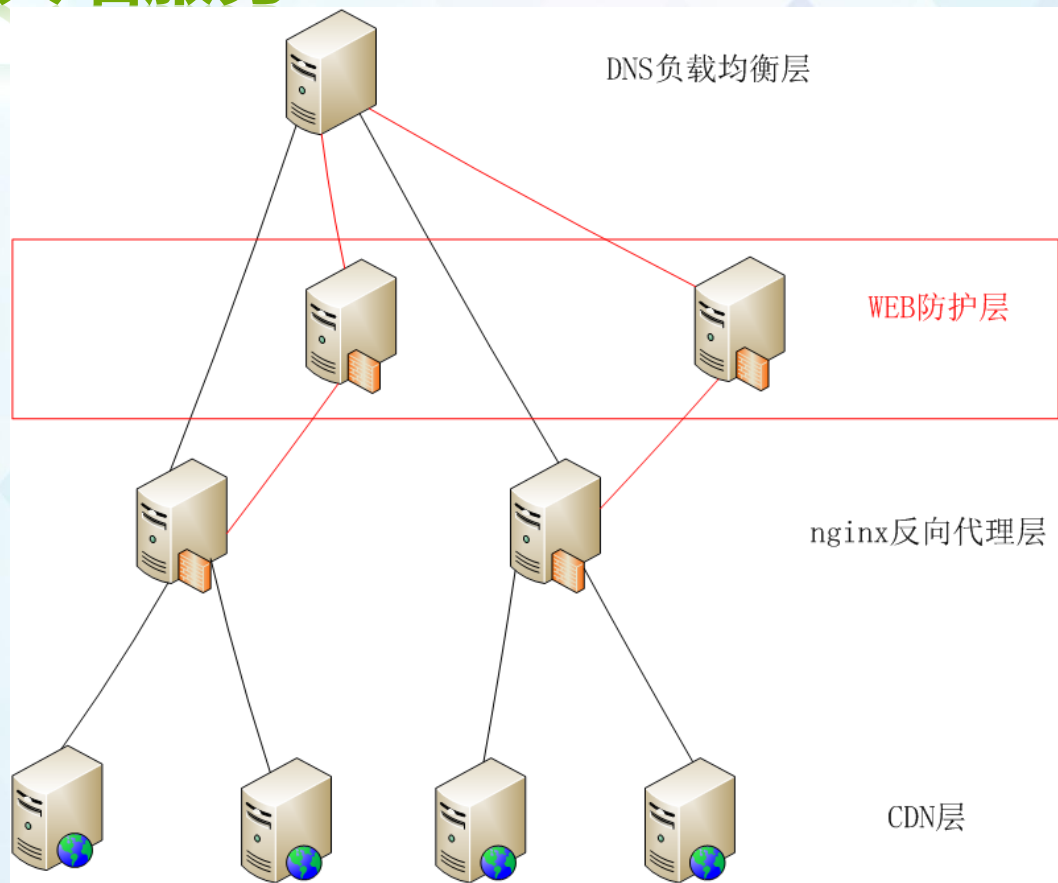
- 按需申请，提交申请只需要一条URL
- 不影响未申请防火墙服务的网站

Cloud WAF



要保护的URL

WEB防火墙服务



后续计划提供的云安全服务

- 在线代码检查服务
- 密码管理和分享服务
- DDOS防御服务

◦ ◦ ◦ ◦ ◦ ◦



iQIYI 爱奇艺



PPS

开启全新视界