百度
超大规模分布式安全系统实践

--欧阳君沛

Geekbang.
极客邦科技

整合全球最优质学习资源，帮助技术人和企业成长

Growing Technicians, Growing Companies

InfoQ queue

专注中高端技术人员的
技术媒体

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

高端技术人员
学习型社交网络

StuQ queue

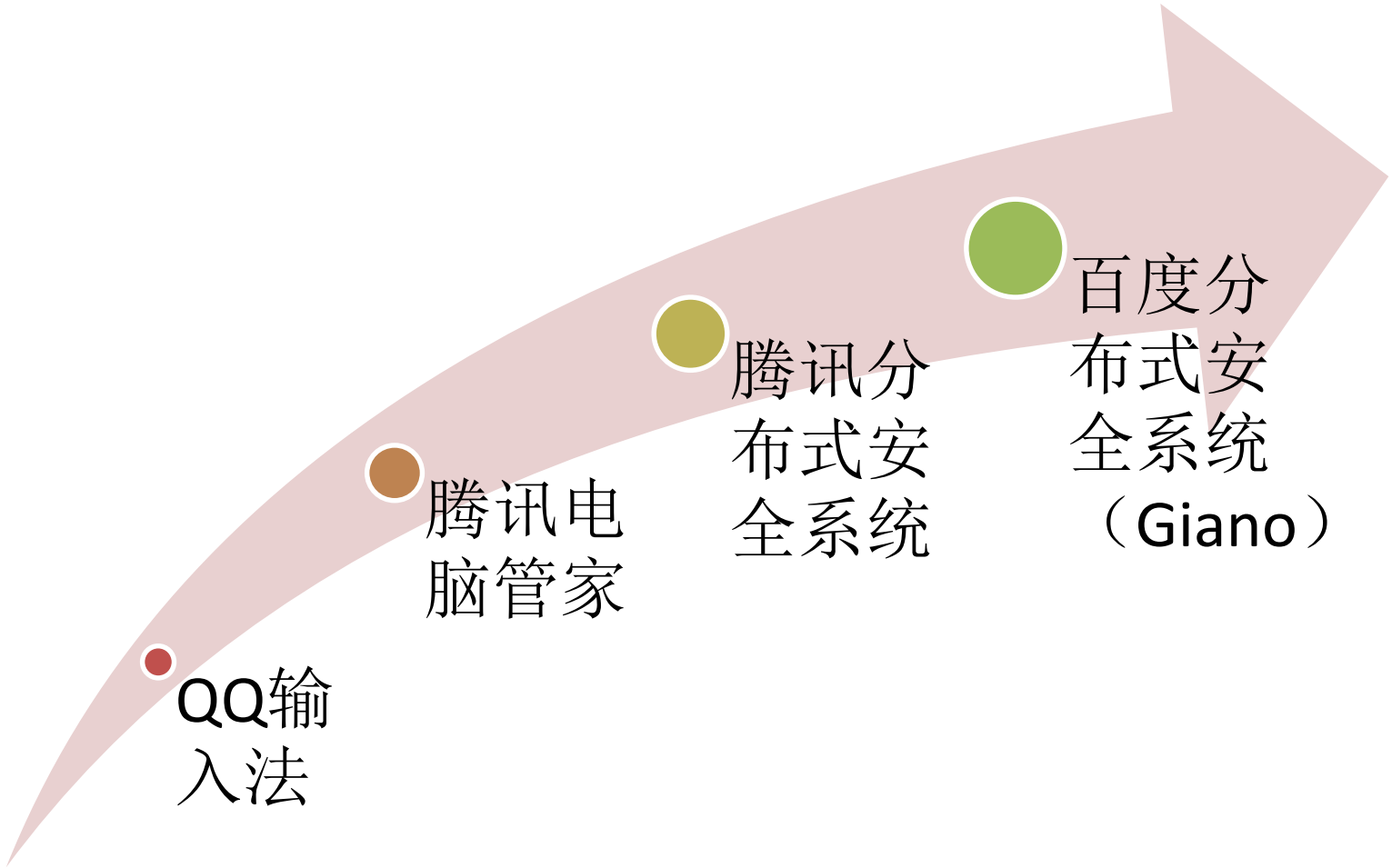
实践驱动的
IT职业学习和服务平台

GiT GEEKBANG INTERNATIONAL TRAINING 极客邦培训

一线专家驱动的
企业培训服务

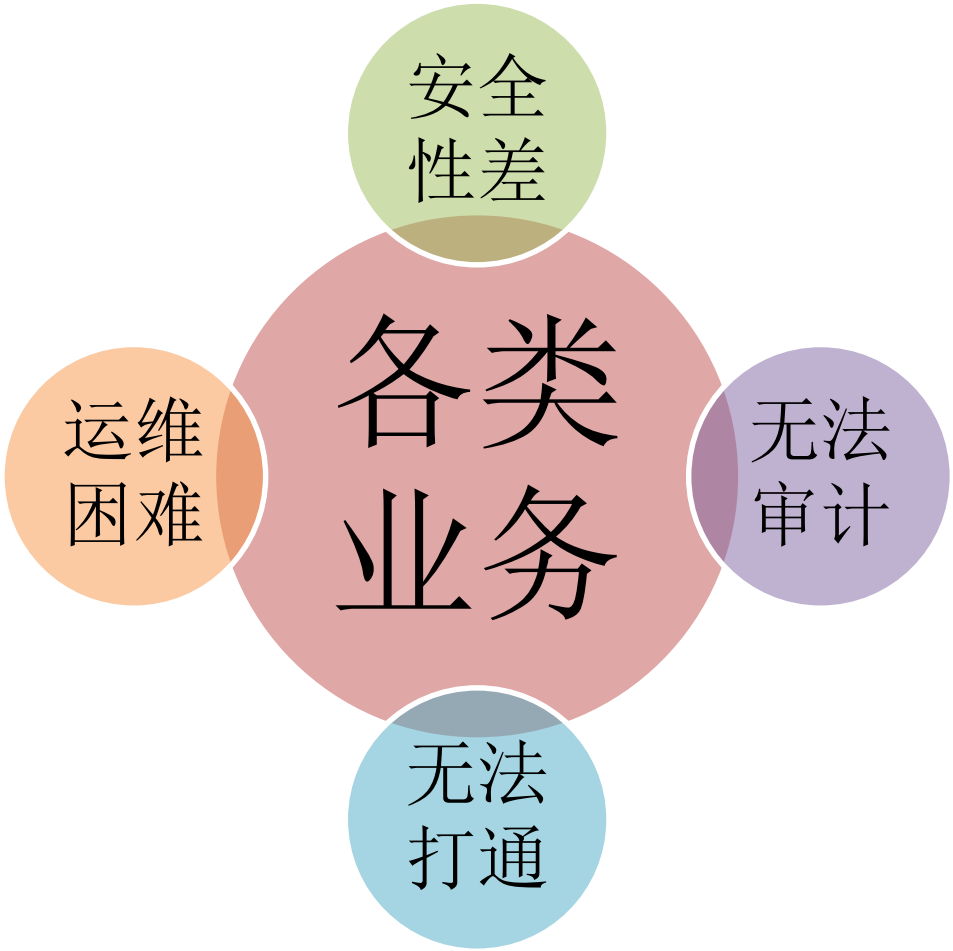
地址：北京市朝阳区洛娃大厦C座6层1607室　　网址：www.geekbang.org

个人介绍



大纲

初来Baidu的时候



初来Baidu的时候

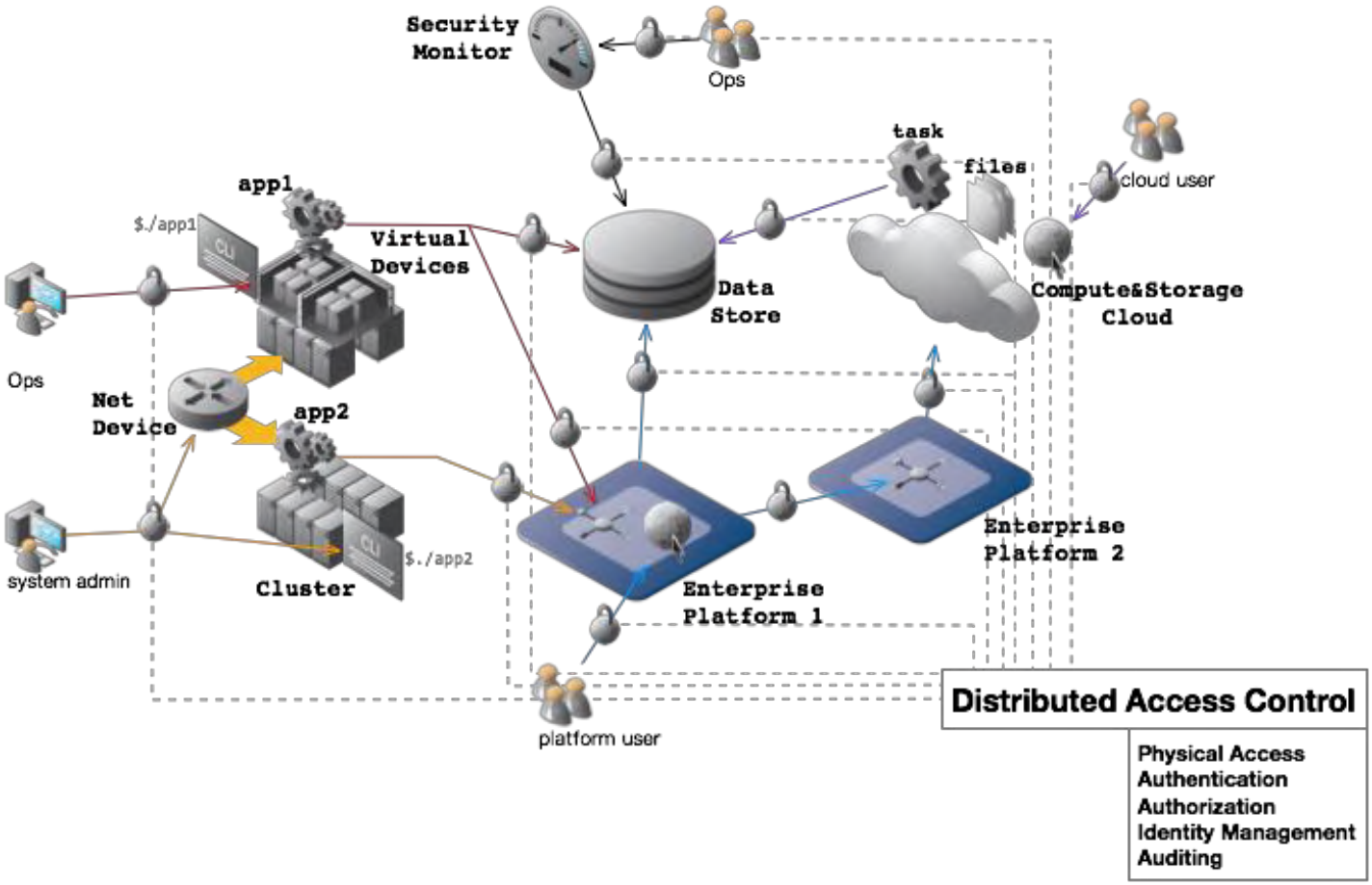
机器管理困难

- 无法追溯责任人和行为
- 信任关系、弱密码、默认密码横行

缺少系统性安全解决方案

- 经常出现线下连线上的严重事故

从访问控制系统入手，逐步拓宽

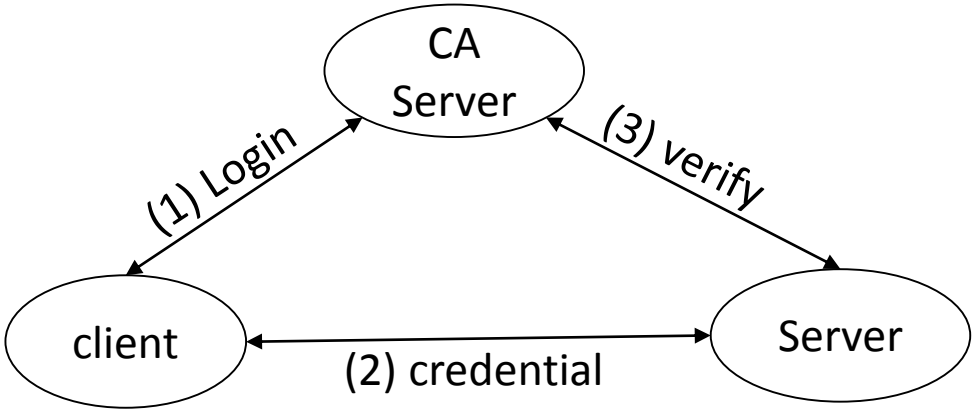


大纲

- 背景介绍
- 分布式认证协议
- 单点登陆
- 域隔离
- 总结与展望

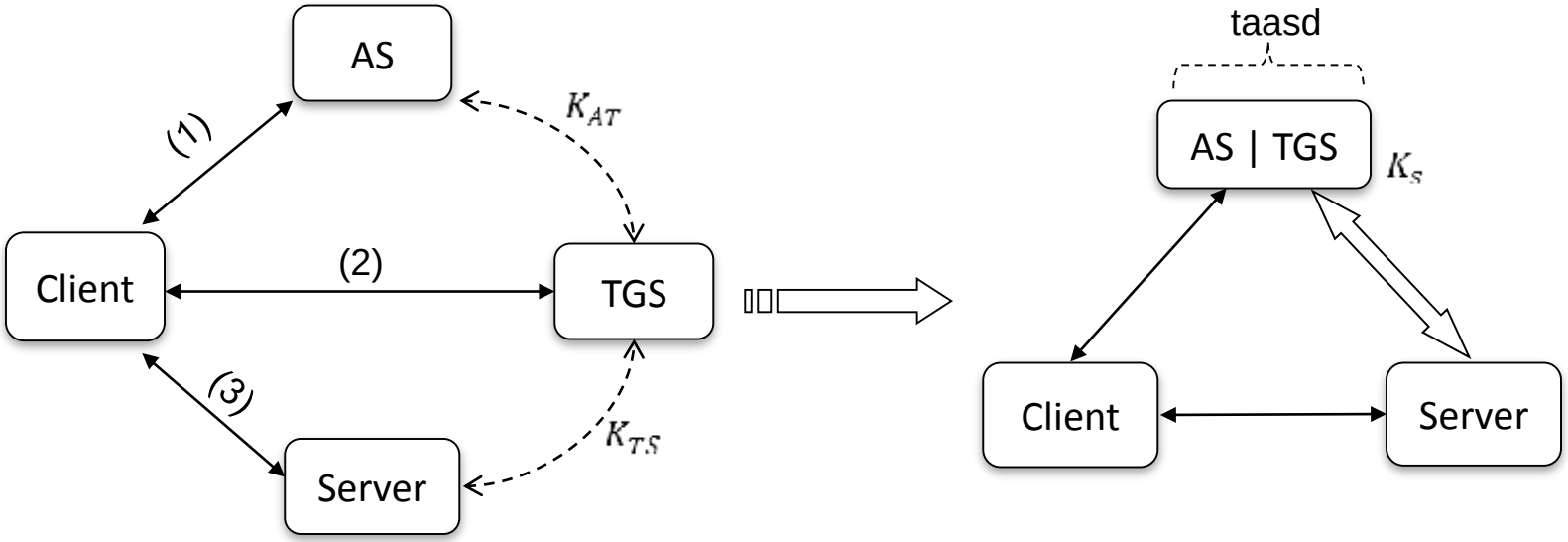
经典认证系统

- 一个经典的C-S认证过程
- 在CA端和Server端分别都有个中心式瓶颈
- Client的latency也很高

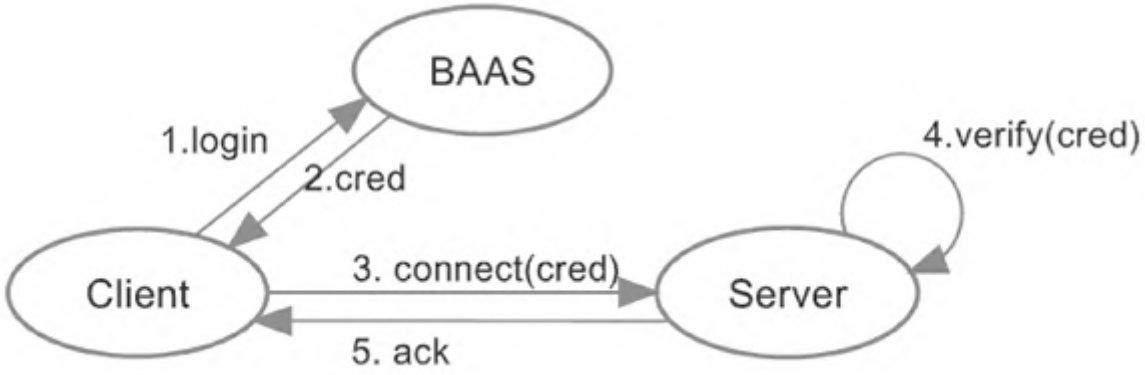


解决Server瓶颈 – 共享密钥

- 引入新的问题，共享密钥给非信任第三方



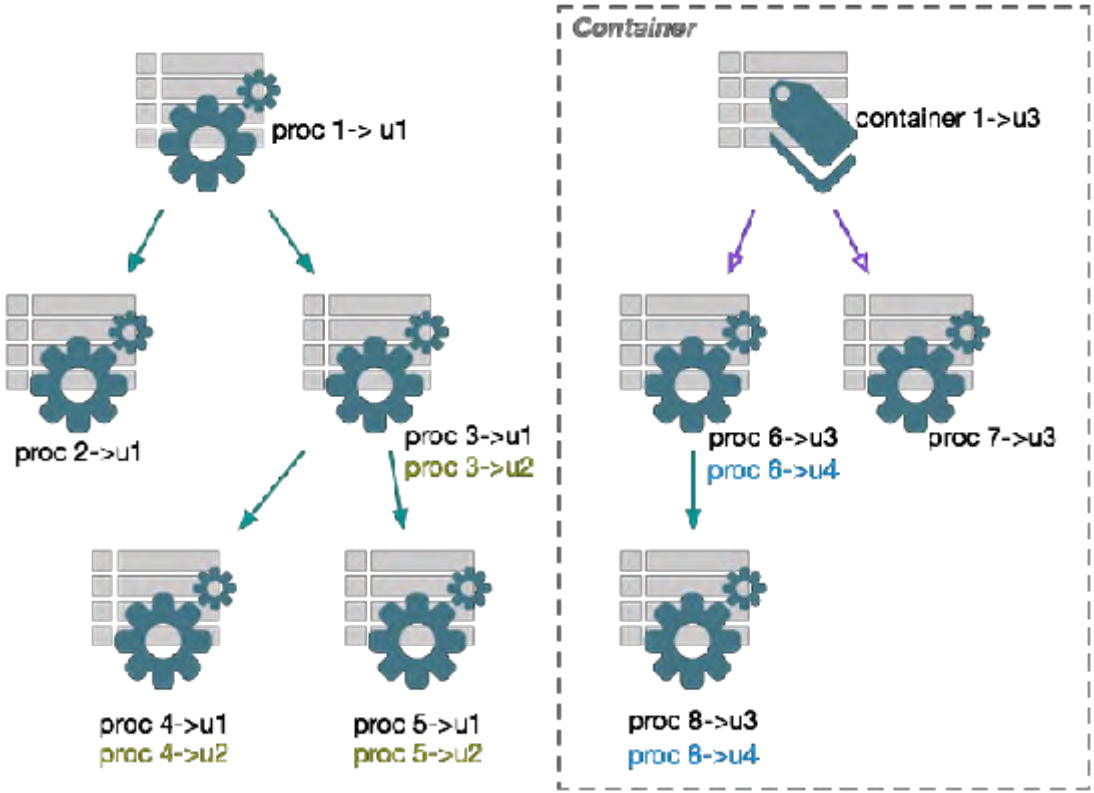
解决Server瓶颈 – PKI



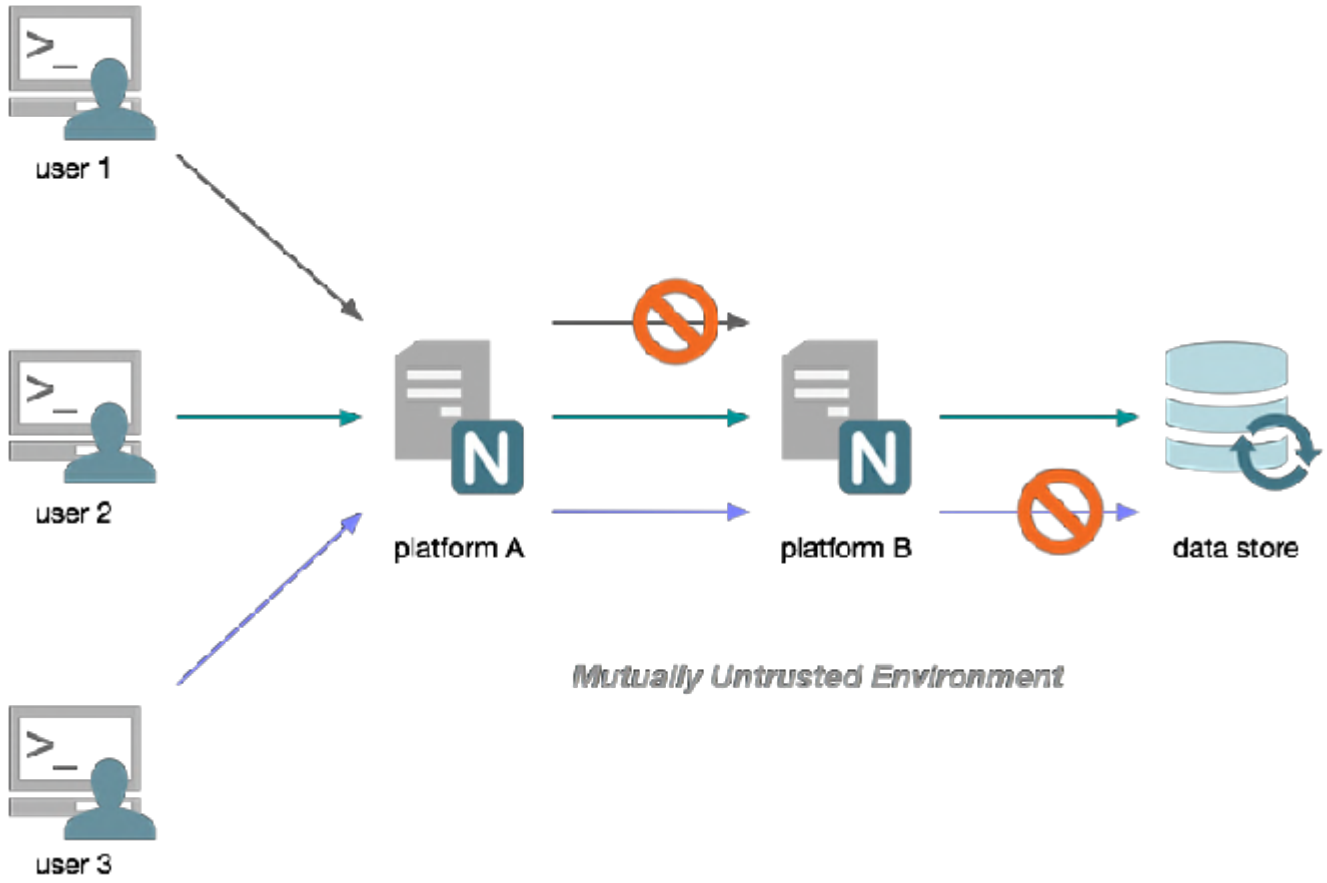
CA瓶颈的解决方案 – agent+client_cache

进程级认证

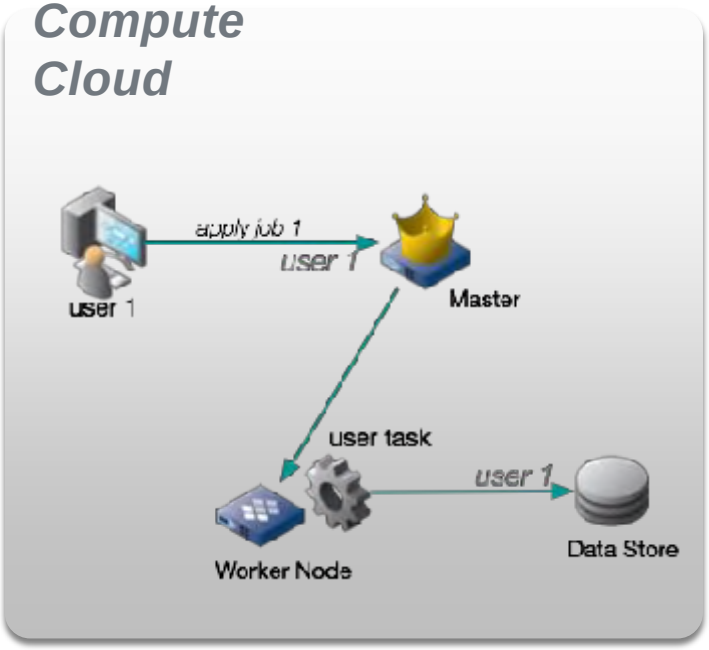
- 安全性强于linux账号级认证

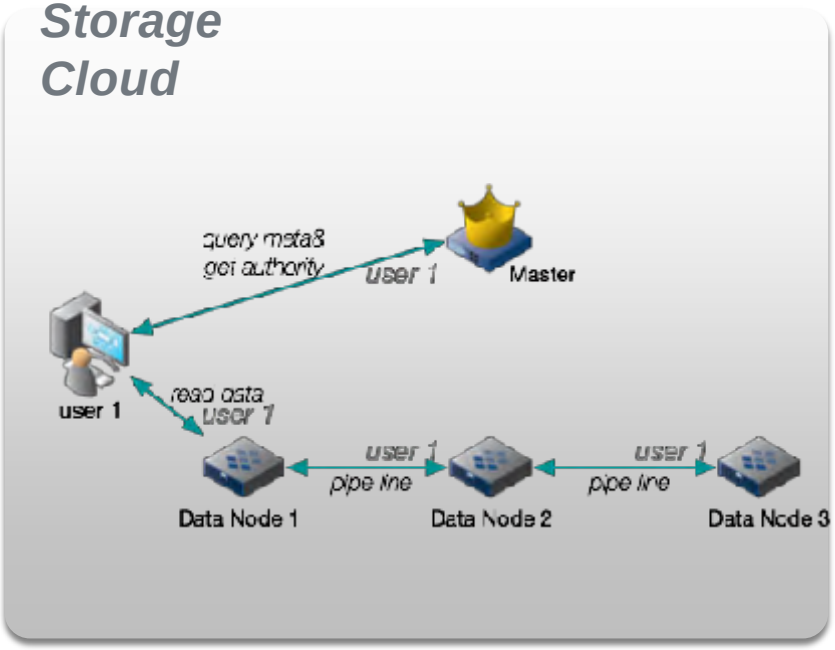


多层次依赖-代理协议


user 1
user 2
user 3
platform A
platform B
data store
Mutually Untrusted Environment

Prof-carrying authorization





系统的安全性

- PKI
- 防止replay-attack（time & address）
- 私钥分发机制+分片机制
- 单机被攻破root，威胁低

系统的高可用性

- 无状态协议、平行扩展
- 中心服务的异地容灾和就近接入
- 客户端和中心服务分别的负载均衡
- 服务端和中心服务分别的服务降级能力

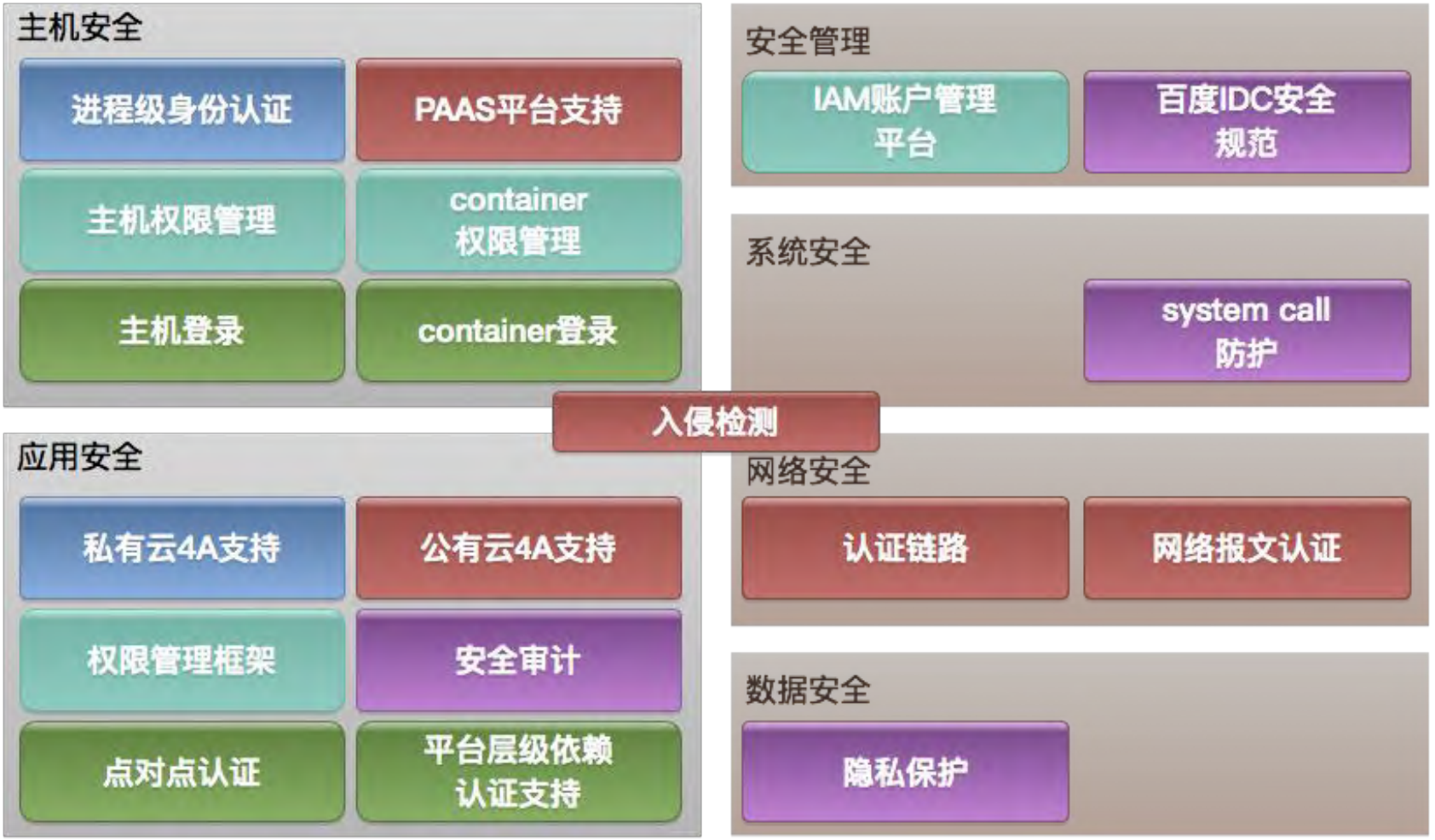
强大的运营能力

- 客户端热升级
- 命令下发
- 数据上报（心跳数据和流水数据）
- 实时和离线数据分析

易用性

- 适配公司container
- 嵌入各类通讯协议中，使接入成本异常容易
- 通过swig转成各类语言，满足多语言需求
- 二进制工具/API皆可完成接入

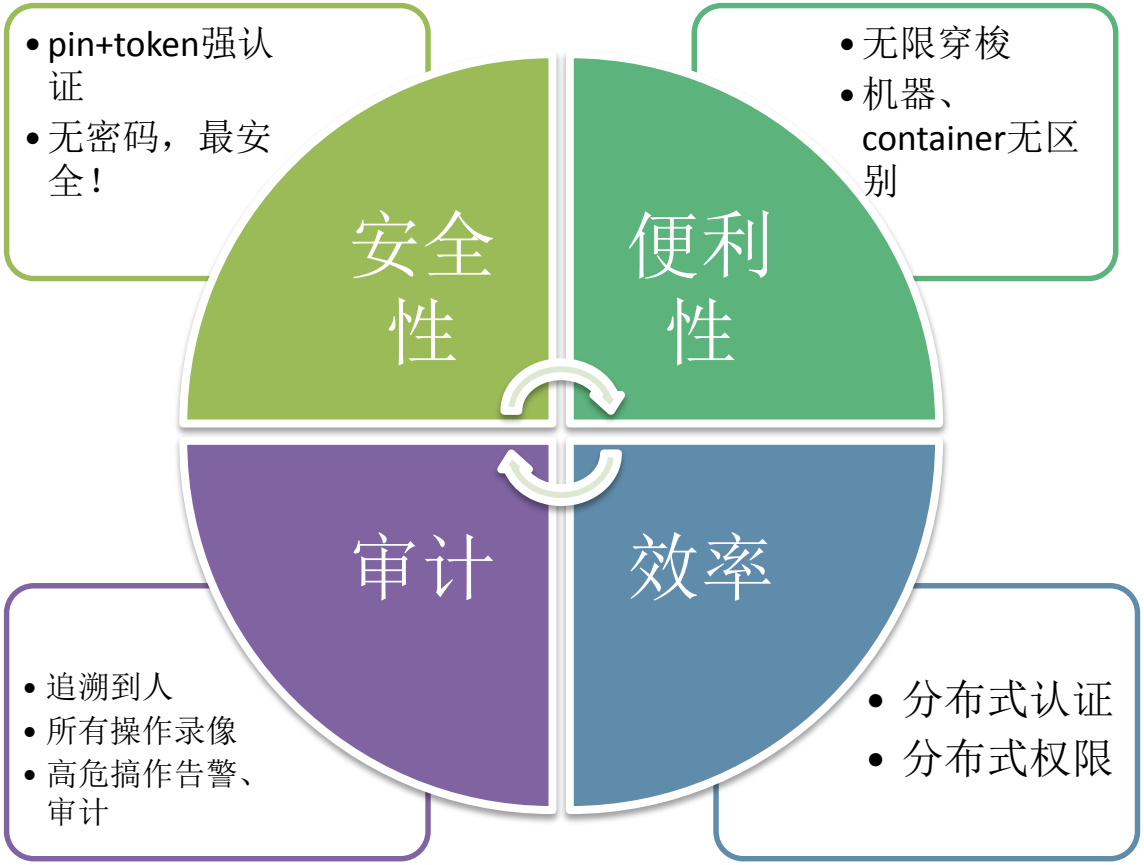
扩展


主机安全
进程级身份认证
PAAS平台支持
主机权限管理
container
权限管理
主机登录
container登录
安全管理
IAM账户管理
平台
百度IDC安全
规范
系统安全
system call
防护
入侵检测
应用安全
私有云4A支持
公有云4A支持
权限管理框架
安全审计
点对点认证
平台层级依赖
认证支持
网络安全
认证链路
网络报文认证
数据安全
隐私保护

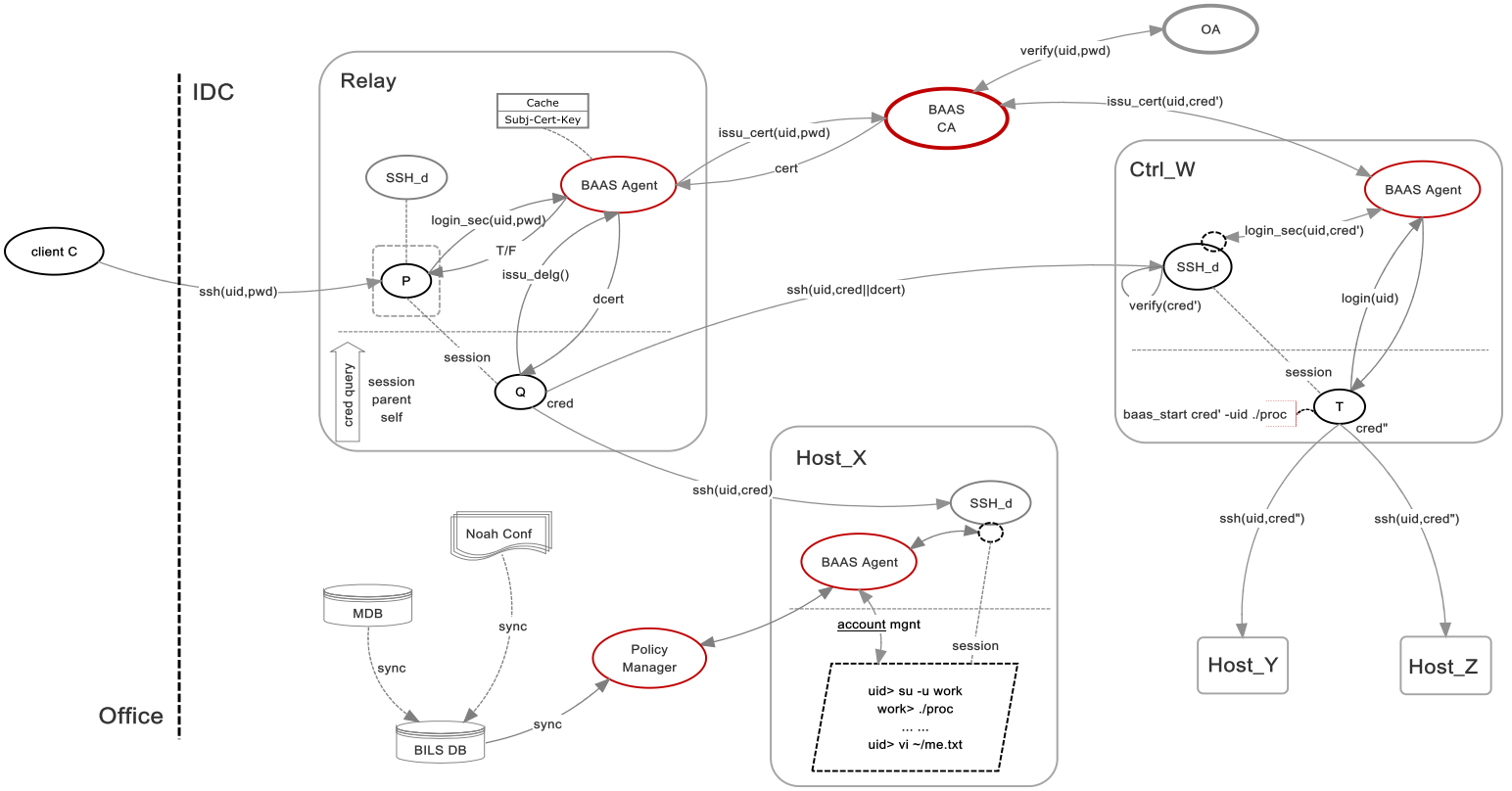
大纲

- 背景介绍
- 分布式认证协议
- 单点登陆
- 域隔离
- 总结与展望

BILS（百度IDC机器登陆系统）



BILS Protocol



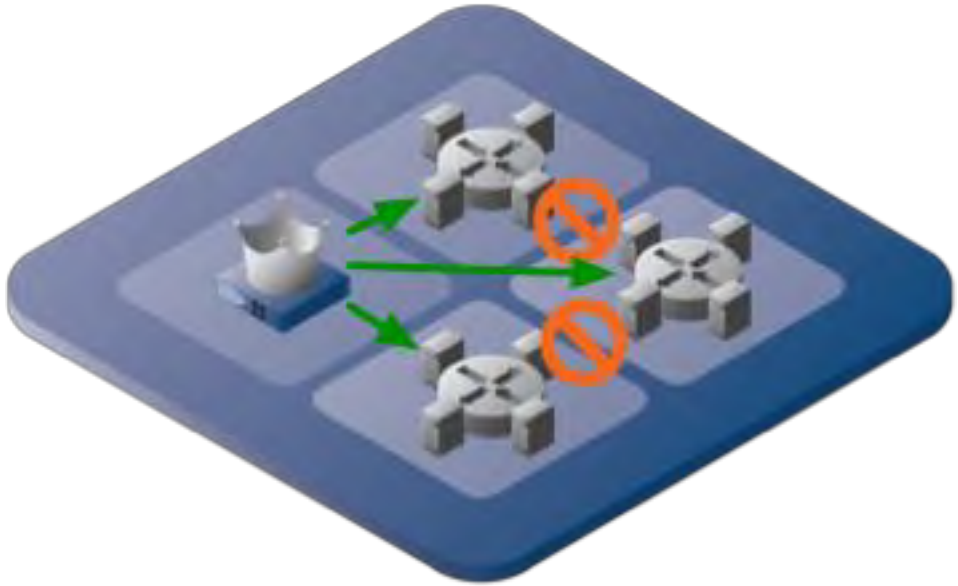
BILS Core Modules

大纲

- 背景介绍
- 分布式认证协议
- 单点登陆
- 域隔离
- 总结与展望

域隔离

- 线上线下环境隔离
- 不同区域、功能的环境隔离
- 登陆隔离
- 进程级别隔离



Domain as an attribute

大纲

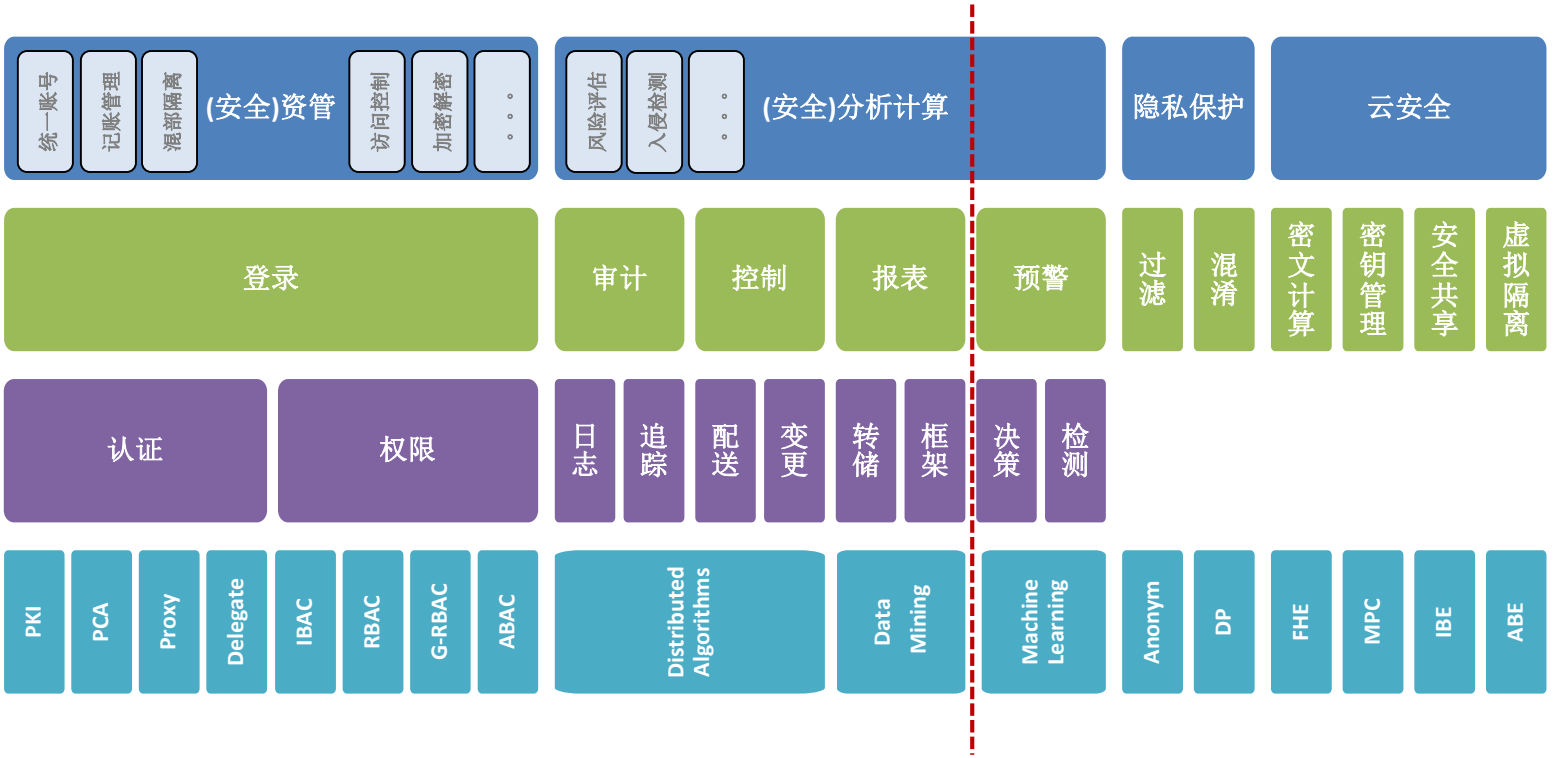
- 背景介绍
- 分布式认证协议
- 单点登陆
- 域隔离
- 总结与展望

使用数据

- Giano是百度强制接入标准，覆盖？万物理服务器

大量审计成果，形成闭环

Technology - Products - Services



Thanks!

Group-Role based Access Control Model