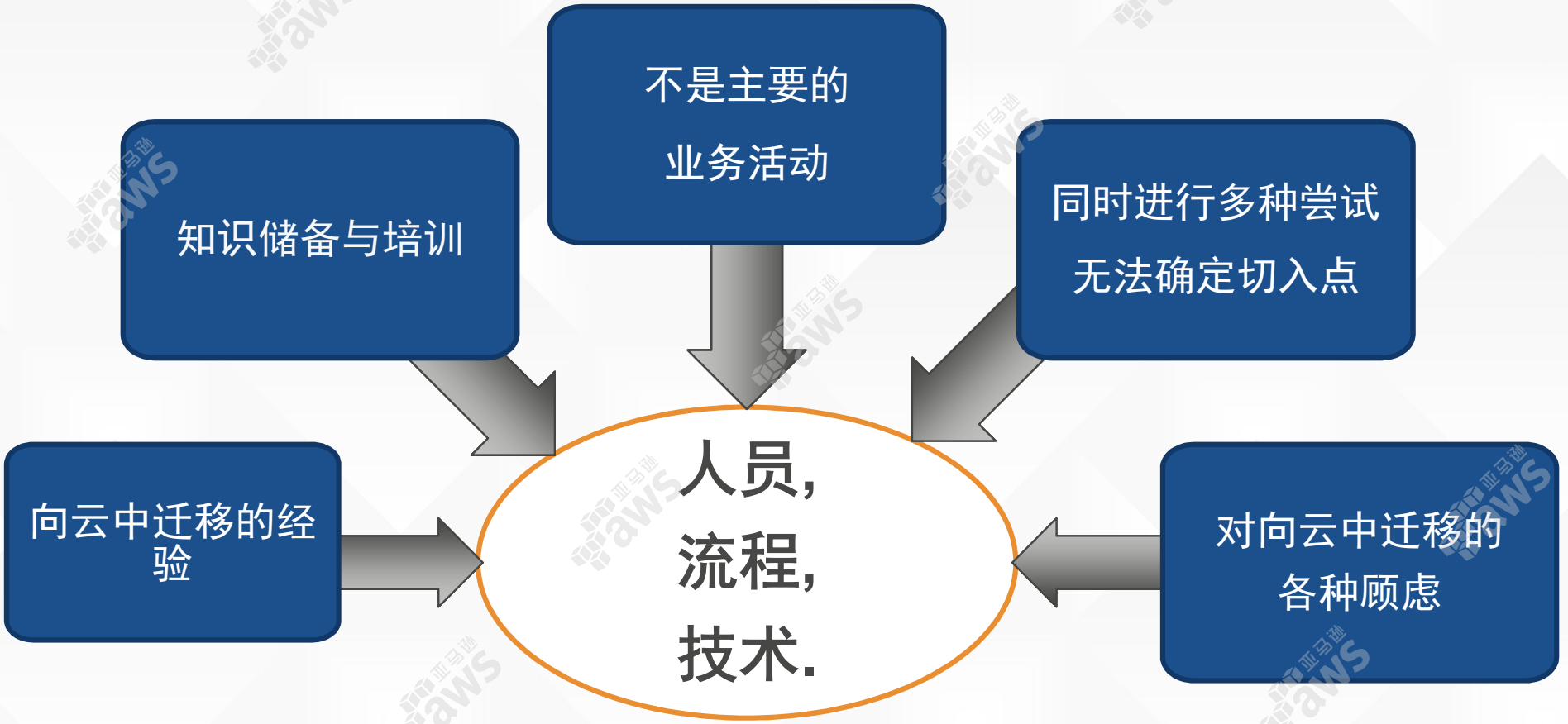

AWS Summit
AWS技术峰会2015 · 上海
亚马逊
aws

企业现代化应用向云中迁移

陈亮, 解决方案架构师

向AWS云中迁移的方法

向云中迁移的挑战


不是主要的
业务活动
知识储备与培训
同时进行多种尝试
无法确定切入点
向云中迁移的经验
人员,
流程,
技术.
对向云中迁移的
各种顾虑

向云中迁移的方法

应用程序迁移评估

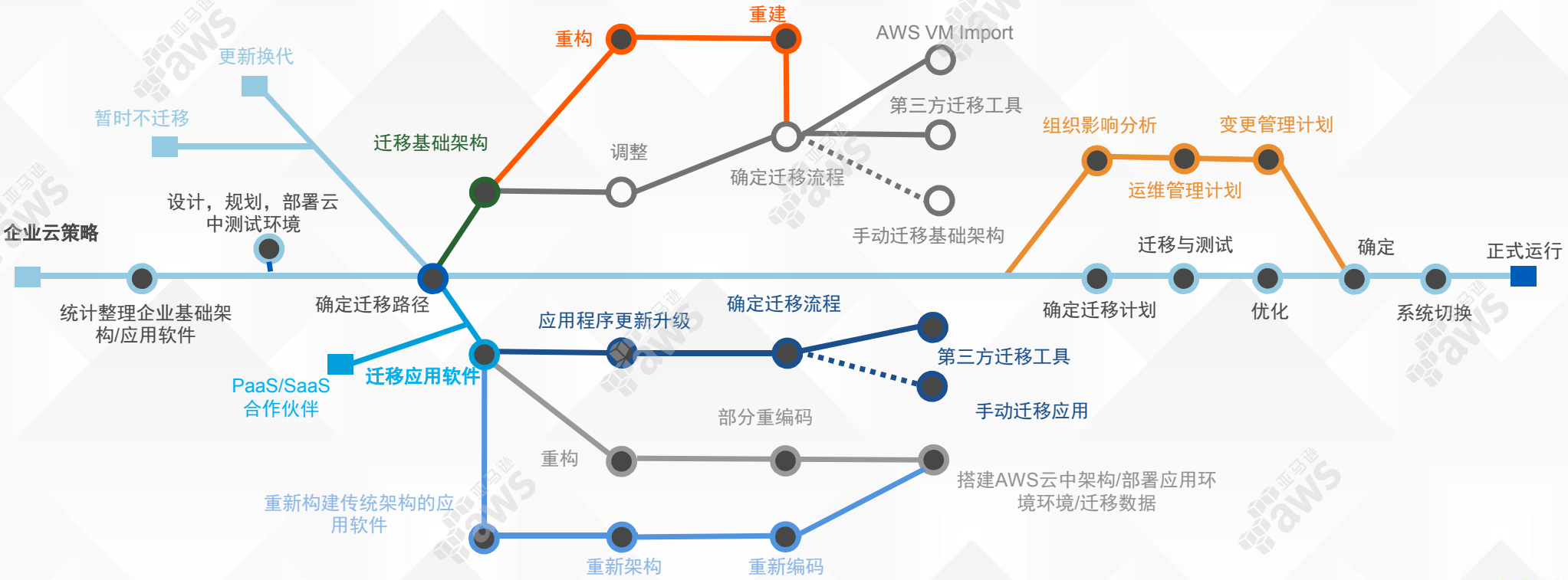
重新托管
（升力和位移）

重新构建平台
（提升和重塑）

应用组合优化

规划迁移

迁移到云中可以使用许多路径之一



AWS云中服务体系架构

亚马逊 aws

规划您在AWS中的系统架构

设计云计算环境和体系结构是非常重要的，实现云计算的好处，如敏捷性和成本节约

网络	安全	合规	数据管理	监控
融合了本地和云	SSO	计费和成本管理	RPO/ RTO	通知及提醒
面向云的协议	访问策略	服务目录	保持政策	应用层意识
IP方案和解决	最小特权	配置管理	复制	阈值
VPC和帐户配置	审计	建筑标准	存储优化	服务台集成
	合规	SLA/ SLO	ILM	
	入侵检测与防御	采购	数据质量	
	记录			

您的数据中心基础架构 - AWS云服务

技术	数据中心	AWS
Network	VPN, MPLS	Amazon VPC, AWS Direct Connect
Storage	DAS, SAN, NAS, SSD	Amazon Elastic Block Store, Amazon S3, Amazon EC2 instance storage, distributed & clustered FS on Amazon EC2
Compute	Hardware, virtualization	Amazon EC2, Amazon ECS, AWS Lambda
Content delivery	Third-party CDN	Amazon CloudFront
Databases	MS SQL Server, MySQL, Oracle, DB2, PostgreSQL, MongoDB,. …	Amazon RDS, Amazon DynamoDB, Amazon Amazon ElastiCache, DB software on Amazon EC2
Load balancing	Hardware and software load balancers	Elastic Load Balancing, software load balancers
Scaling & cluster management	Hardware and software clustering tools	Auto Scaling, software clustering solutions
DNS	BIND, Windows Server, third party	Amazon Route 53, third-party DNS software on EC2

您的数据中心基础架构 - AWS云服务

技术	数据中心	AWS
Analytics & data warehouse	Hadoop, Vertica, Cassandra, specialized hardware and software	Amazon EMR, Amazon Redshift, software on Amazon EC2
Messaging and workflow	RabbitMQ, ActiveMQ, Kafka, …	Amazon SQS, Amazon SNS, Amazon SWF, software on EC2
Caching	Redis, Memcached, …	Amazon ElastiCache, Memcached, SAP Hana
Archiving	Tape library, off-site data storage	Amazon S3, Amazon Glacier
Email	Email software	Amazon SES
Identity, authoritzation, & authentication	AD/ADFS, LDAP, SAML, third party…	AWS Identity and Access Management/AWS STS, Amazon Cognito, AWS Directory Service, AD & LDAP on Amazon EC2
Deployment & configuration management	Chef, Puppet, Salt, Ansible, PowerShell DSC	AWS CloudFormation, AWS OpsWorks, AWS Elastic Beanstalk, AWS CodeDeploy, Amazon ECS
Management and monitoring	CA, BMC, Rightscale	Amazon CloudWatch, AWS Config, AWS CloudTrail, AWS Trusted Advisor

企业应用向AWS云中迁移的最佳实践

亚马逊 aws

确认计划迁移的应用

迁移独立的应用系统会相对简单

基于SOA设计的松耦合应用系统迁移是个好的选择

紧耦合的系统迁移需要做更多详细的计划

最初迁移的应用系统

开发/测试环境，自包含的网站应用(LAMP)，社交网络的市场活动，培训环境，产品展示与销售网站，软件下载/试用的应用程序。

注意以下场景

32 bit, 非Linux/Windows, 多播 (如：Oracle RAC), 客户端/服务器应用程序, 工程一体机(如：Exadata, Netezza), 垂直扩展/无法分布式的应用系统

预估与规划：最基本的信息

计算： 服务器/虚拟机的数量，包括 内存, CPU, 操作系统, 和启动盘的大小
(Amazon EC2)

存储： 对应交易，备份，归档和日志/文件等不同需求

(Amazon EBS, Amazon Glacier, and Amazon S3)

选择运行的**区域**

通过网络**传出**数据的大小

互联网或专线直连，从**安全和传输效率**两方面考虑 (AWS Direct Connect and VPN)

预估与规划: 最好获得更多信息

每种工作负载的**备份需求**

每种工作负载的**高可用需求**(ELB, Route53, RDS Multi-AZ)

每种工作负载的**扩展需求** (ELB, Route53, Auto Scaling, CloudFront)

每种工作负载的**灾备需求**

每种工作负载的**存储性能需求**(IOPS)

对**管理/监控系统**的要求

预估与规划：如果能获得这些信息就太好了

工作负载分类： 文件服务器，安全，关系型数据库，企业管理软件，大数据分析，管理与监控 等等

每种工作负载对**合规的要求** HIPPA and PCI

每种工作负载对**高性能运算**的需求

超高 **CPU, 内存**的需求

对**第三方打包软件**的需求，
IDS/IPS, WAF, management, monitoring, logging, 等等.

尽早开始PoC，验证计划可行性

PoC会解答你很多**问题和疑虑**，并且让你快速的熟悉AWS

帮助你发现设计与实现的**差距**并找到成功迁移的**关键点**

帮助你做好迁移的成本**预估**

帮助你做好应用系统在AWS运行的成本**预估**

将数据迁移至AWS

- 通过S/FTP, SCP, UDP, Attunity将**文件传输**至Amazon S3或EC2
- 将数据中心的数据通过**NFS**挂载到AWS上
- 配置数据中心的**备份软件**(如 NetBackup, CA, CommVault, Riverbed) 将数据直接备份至Amazon S3
- 通过AWS **Storage Gateway** 将数据异步备份到Amazon S3
- AWS Import/Export 服务/ **Snow Ball**: 将你的磁盘或者Snow Ball寄送给AWS
- 数据库备份工具如 Oracle Secure Backup
- 数据库复制工具如 GoldenGate, Dbvisit
- AWS **专线直连**，100 Mbps 至 10 Gbps

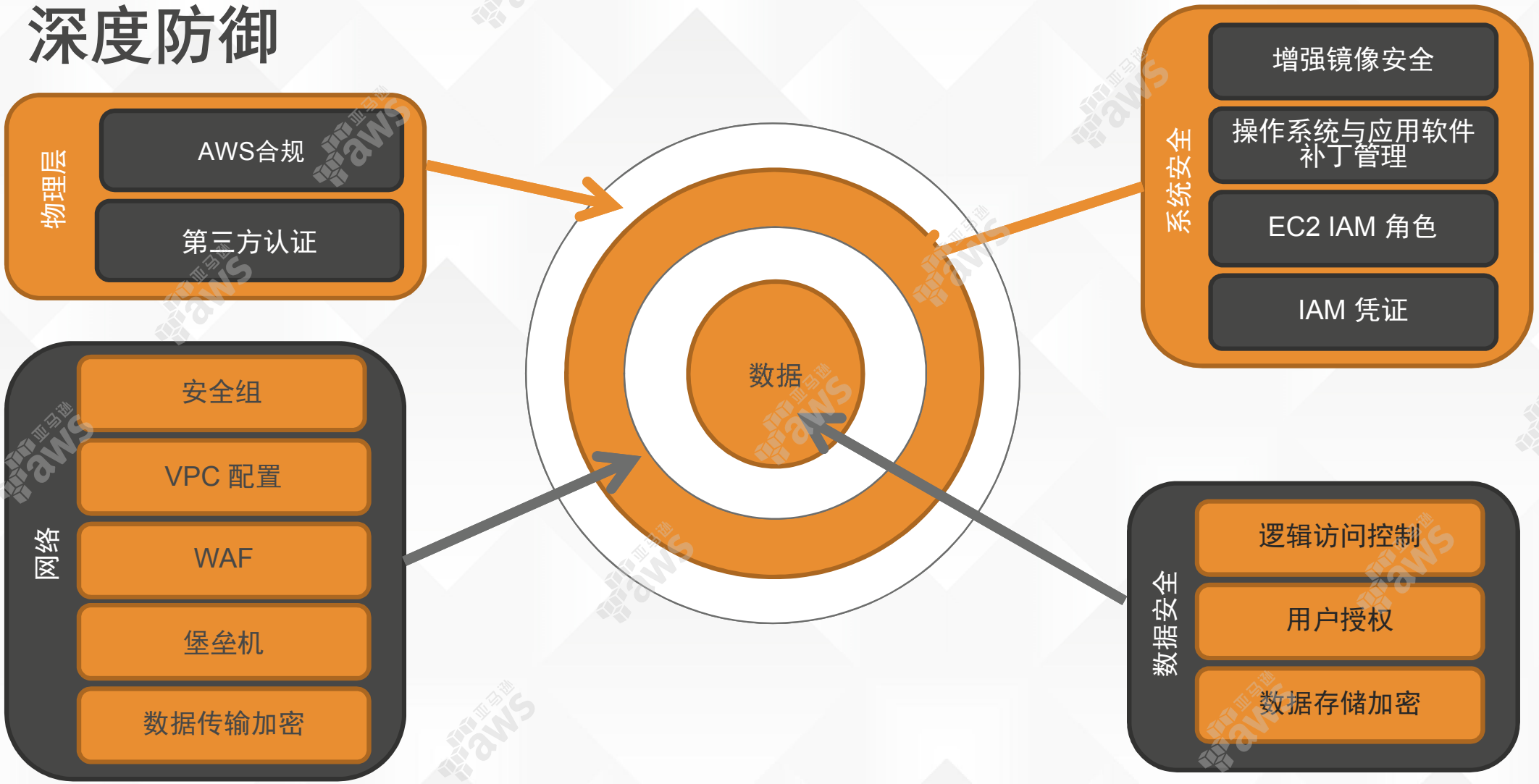
将数据迁移至AWS


GBs
TBs
UDP 传输软件 (如, Tsunami…)
Attunity CloudBeam
AWS Storage Gateway,
Riverbed, NFS
通过专线一次性上传,
并持续同步变化数据
小时
PBs
天
通过互联网传输
AWS Import / Export
Snow Ball
需要快速传输数据
数据容量大小*
* 与网络带宽与延时相关

企业应用在AWS云中的安全最佳实践

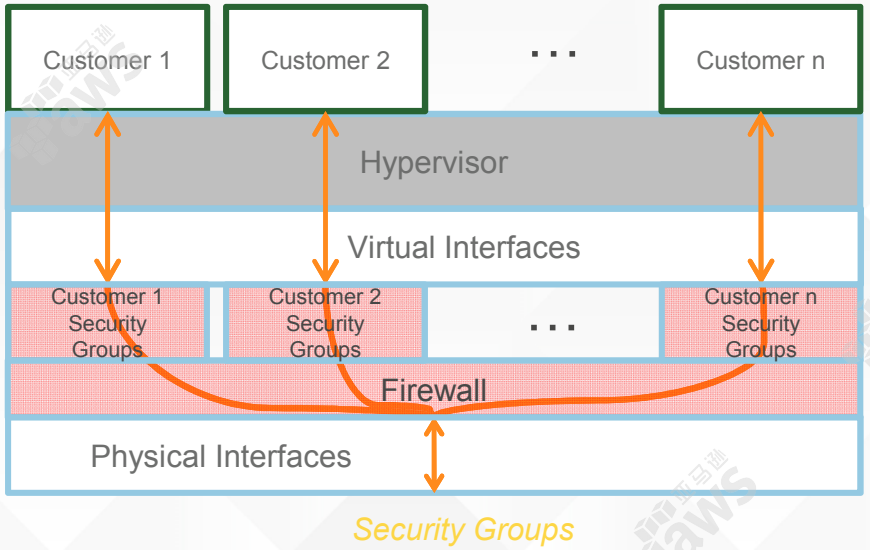
亚马逊 aws

深度防御


物理层
AWS合规
第三方认证
网络
安全组
VPC 配置
WAF
堡垒机
数据传输加密
数据
系统安全
增强镜像安全
操作系统与应用软件补丁管理
EC2 IAM 角色
IAM 凭证
数据安全
逻辑访问控制
用户授权
数据存储加密

云中防火墙: 安全组以及网络访问控制列表

- **VPC 安全组(必选)**
  - 实例级别，有状态
  - 仅支持 允许 条件
  - 默认拒绝入站，允许出站
  - 最小权限，类似”白名单”
- **VPC 网络访问控制列表 (可选)**
  - 子网级别，无状态
  - 同时支持允许和拒绝
  - 默认允许所有
  - 类似使用”黑名单”



- 任何更改都会被Cloud Trail记录
- 无需为安全组以及网络访问控制列表付任何额外费用

数据存储加密

卷加密

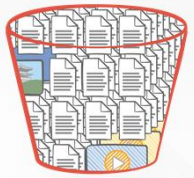
- EBS encryption
- OS tools
- AWS marketplace/partner

对象加密

- S3 server side encryption (SSE)
- S3 SSE w/ customer provided keys
- Client-side encryption

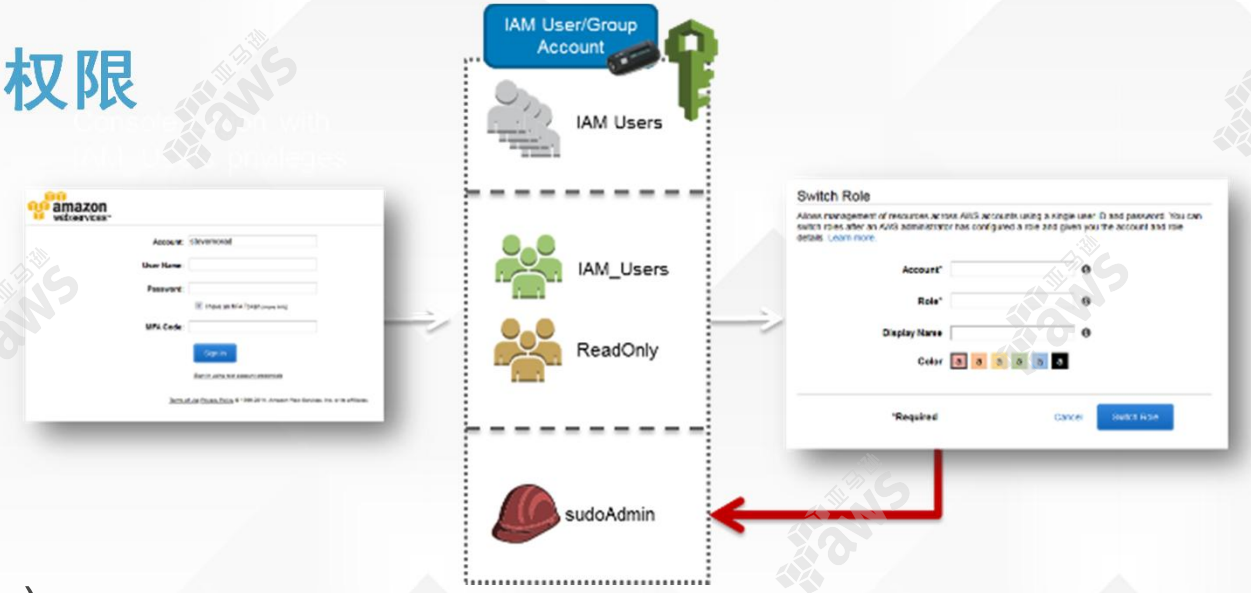
数据库加密

- RDS MSSQL TDE
- RDS ORACLE TDE/HSM
- RDS MYSQL KMS
- RDS PostgreSQL KMS
- Amazon Redshift encryption



最低用户权限原则

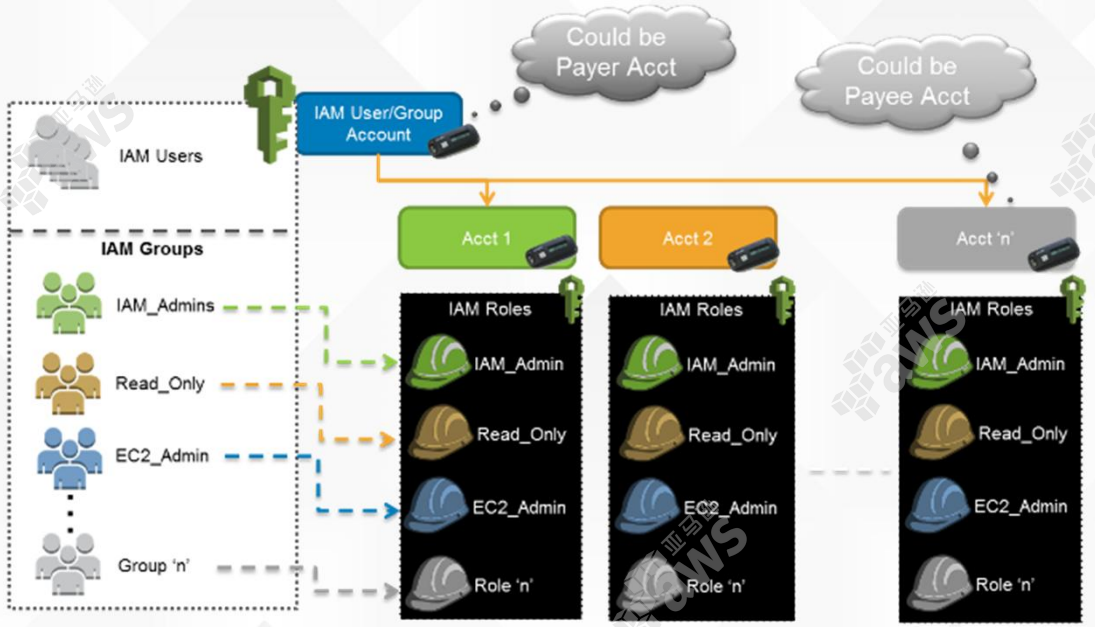
- **使用尽量低权限的用户登录AWS**
  - Read-only
  - EC2 launch-only
- **通过转换角色来获得操作权限**
  - 管理 IAM
  - 删除实例
  - 删除快照



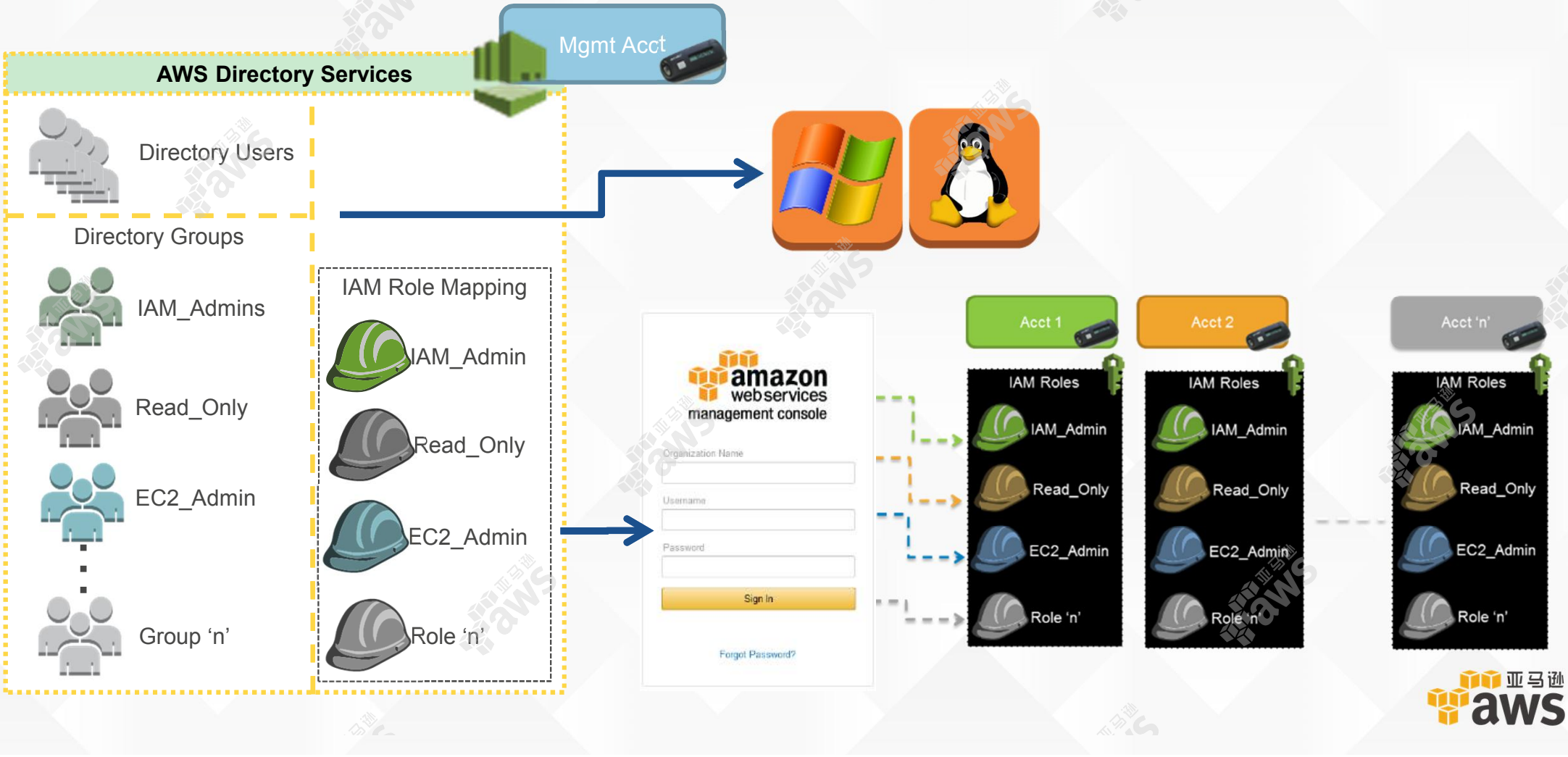
防止误操作
(类似于 DisableApiTermination=true)

整合你的AWS IAM用户

- 在企业层面，采用整合帐单(consolidated billing)
- 不同Account之间允许通过转换角色(assume roles)的方法切换帐号
- 管理与计费Account不产生服务费用



与AWS Directory Service 和 IAM进行权限联盟



Thank You