



容器架构下 多云平台的运维实践

何浩祥 Jerry

思杰大中华区高级技术经理

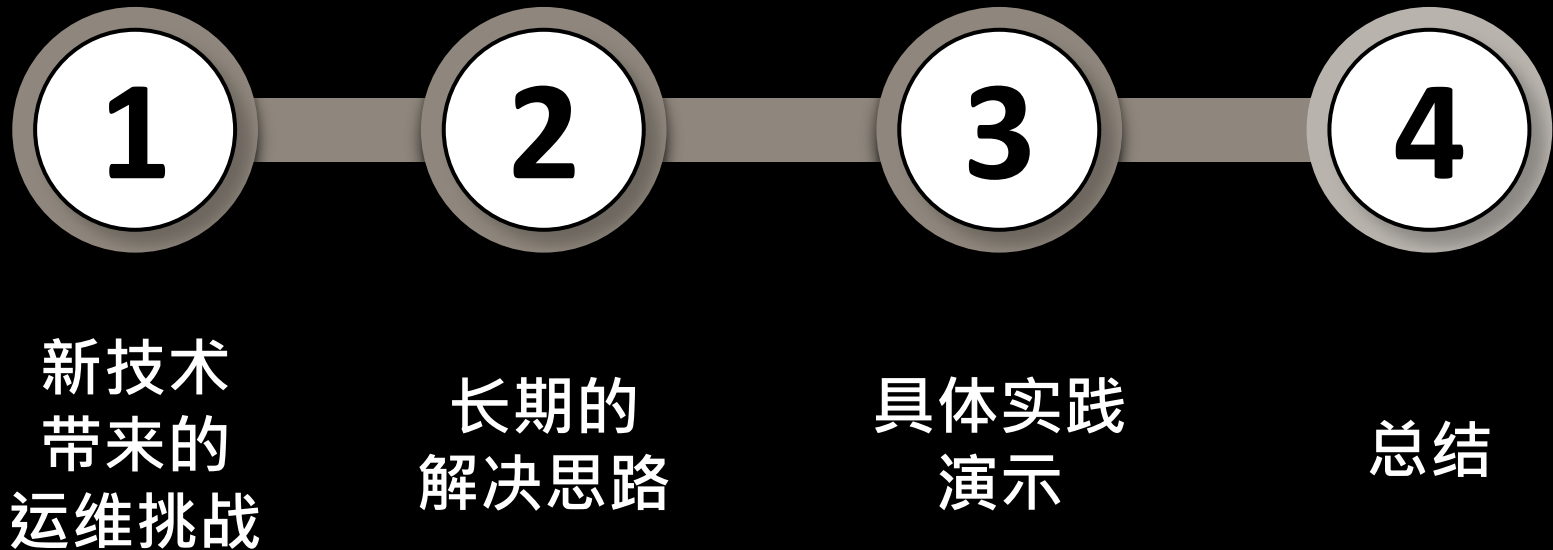
Jerry.ho@citrix.com

MAY 19, 2017

© 2016 Citrix | Confidential



主要内容



容器可跨平台，混合部署多

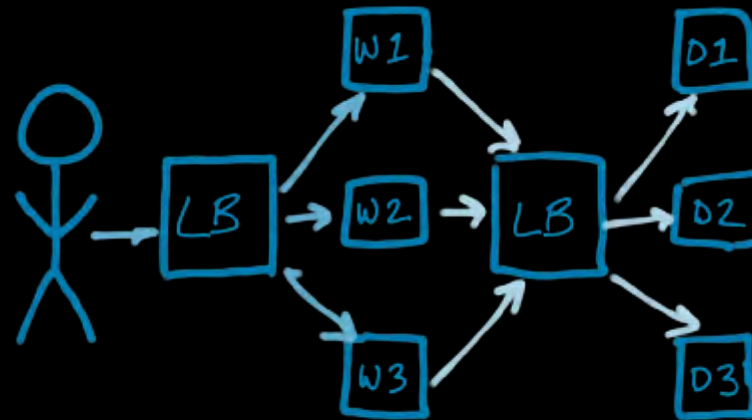
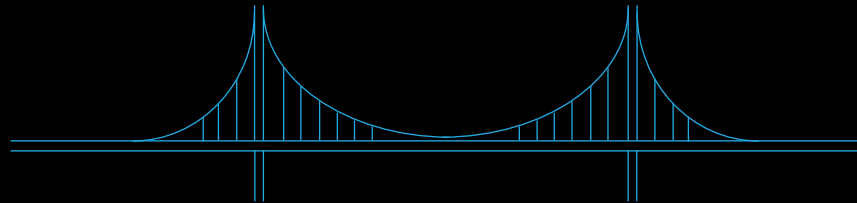


不管公云还是私云，都是为了谁服务？

什么需求都会出现在各种云里，又和应用息息相关??




IT
运维



开发


各平台都有不同的负载均衡

容器服务与编排




The first row features three circular icons. The first icon shows the NGINX logo (a green 'G' on a white background) with a stack of server racks above it. The second icon shows the Kubernetes logo (a ship's wheel) with the text 'kubernetes Kube Proxy' below it. The third icon shows the Mesos logo (a hexagonal grid) with the text 'MESOS' and a network diagram below it.

公云



The second row features three circular icons. The first icon shows the Amazon logo (orange blocks) with the text 'amazon services Elastic Load Balancing' below it. The second icon shows the Azure logo (blue cloud) with the text 'Azure' and a green plus sign below it. The third icon shows the Alibaba Cloud logo (a stylized 'A' in a square) with the text '阿里云 LVS' below it.

私云与SDN



The third row features three circular icons. The first icon shows the VMware logo (blue and green) with the text 'vmware NSX' below it. The second icon shows the Citrix logo (a red square) with the text 'Citrix' and a network diagram below it. The third icon shows the Cisco logo (a diamond shape) with the text 'CISCO APIC 第三方' below it.

PaaS服务



The fourth row features two circular icons. The first icon shows the Pivotal logo (a green cloud) with the text 'CF Pivotal Cloud Foundry' below it. The second icon shows the OpenShift logo (a red circular arrow) with the text 'OPENSHIFT' below it.

但是这都只满足了4层负载均衡，无法解决应用的问题

新型态应用特性



交易量不定

易有瞬间大量
要能确保交易完成



任何地点

车上
分店
行走间



使用者沒耐心

等久了，用別家吧
体验是绝对要求



第三方接入

接不完的平台
上线时程漫长
新协议(MQTT)



安全

安全是信任的
基础
Apple ATS要求

目前主流网站加密模式/Apple ATS

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

传输层加密协议
目前建议是
TLS1.2或TLS1.3

密钥交换
(Key Exchange)
ECDHE:非对称密钥交换
RSA:签名认证(跟凭证公
钥使用的算法有关)

加密算法
(Cipher)
建议是AES_128_GCM
其中128为以上为佳

讯息鉴别码
(MAC: Message
Authentication Code)
建议是SHA256以上

为何使用ECDHE?

ECC

Elliptic Curve Cryptography椭圆曲线加密

- 使用较短的密钥长度
- 对客户端的CPU与Memory消耗较小
- ECC在客户端更快
- ECC 更安全

DH
Key
Exchange

Diffie-Hellman密钥交换算法

- 更安全的密钥交换机制
- 不需交换预置密钥(pre-master secret)
- 目前无已知的弱点

PFS

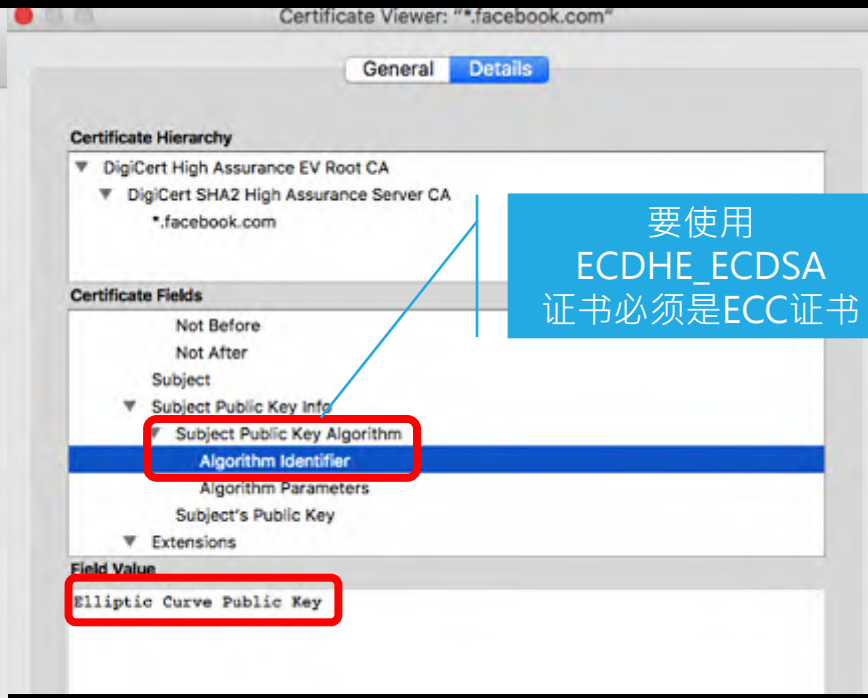
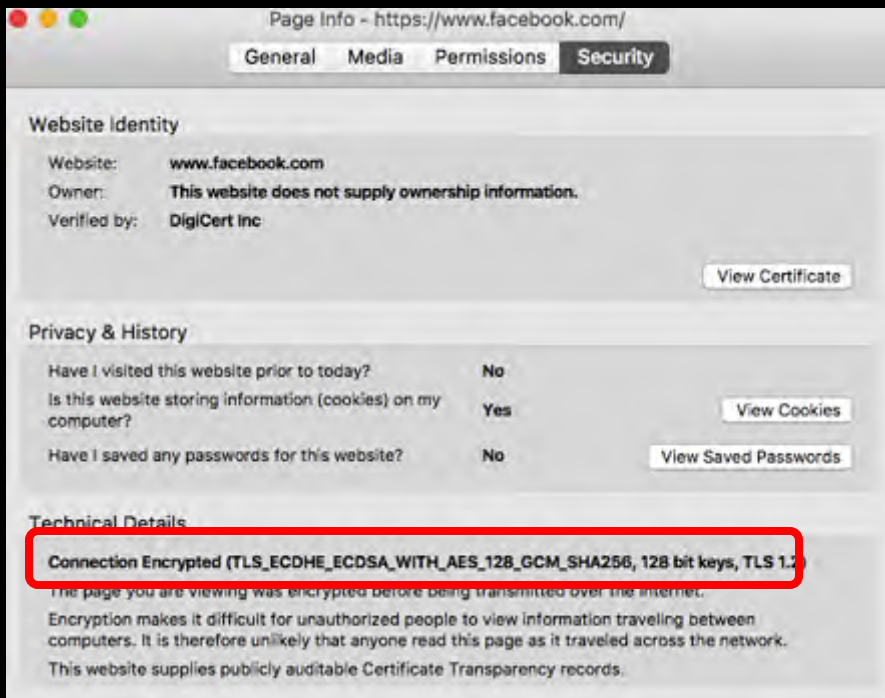
Perfect Forward Secrecy完全前向保密

- 在密钥泄漏时也能确保数据安全
- ECDHE下，支持PFS

*ECDHE无法防止中间人攻击，需加入签名认证机制，如RSA,ECDSA来防止

*ECDHE产生的是Session Key，就算拿到凭证的私钥，也不能将截取的封包解开

ECC证书



要使用
ECDHE_ECDSA
证书必须是ECC证书

RSA还是ECDSA



ECDHE_RSA

- 目前签发最多的证书方式
- 满足现况最多的需求



ECDHE_ECDSA

- 较ECDHE_RSA省资源
- 建议未来采用的证书方式
- 目前使用较少

大部份的网站还是用RSA证书

Website: **www.apple.com**
Owner: **Apple Inc.**
Verified by: **Symantec Corporation**



View Certificate

... prior to today? **Yes, 2 times**

... information (cookies) on my computer? **Yes**

View Cookies

... for this website? **No**


View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

Website Identity

Website: **www.baidu.com**
Owner: **This website does not supply ownership information.**
Verified by: **GlobalSign nv-sa**



View Certificate

... my computer? **No**

... information (cookies) on my computer? **Yes**

View Cookies

... for this website? **No**

View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

Website: **world.taobao.com**
Owner: **This website does not supply ownership information.**
Verified by: **GlobalSign nv-sa**



View Certificate

... my computer? **No**

... information (cookies) on my computer? **Yes**

View Cookies


... for this website? **No**

View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

Website: **aws.amazon.com**
Owner: **This website does not supply ownership information.**
Verified by: **Amazon**



View Certificate

... my computer? **No**

... information (cookies) on my computer? **Yes**

View Cookies

... for this website? **No**

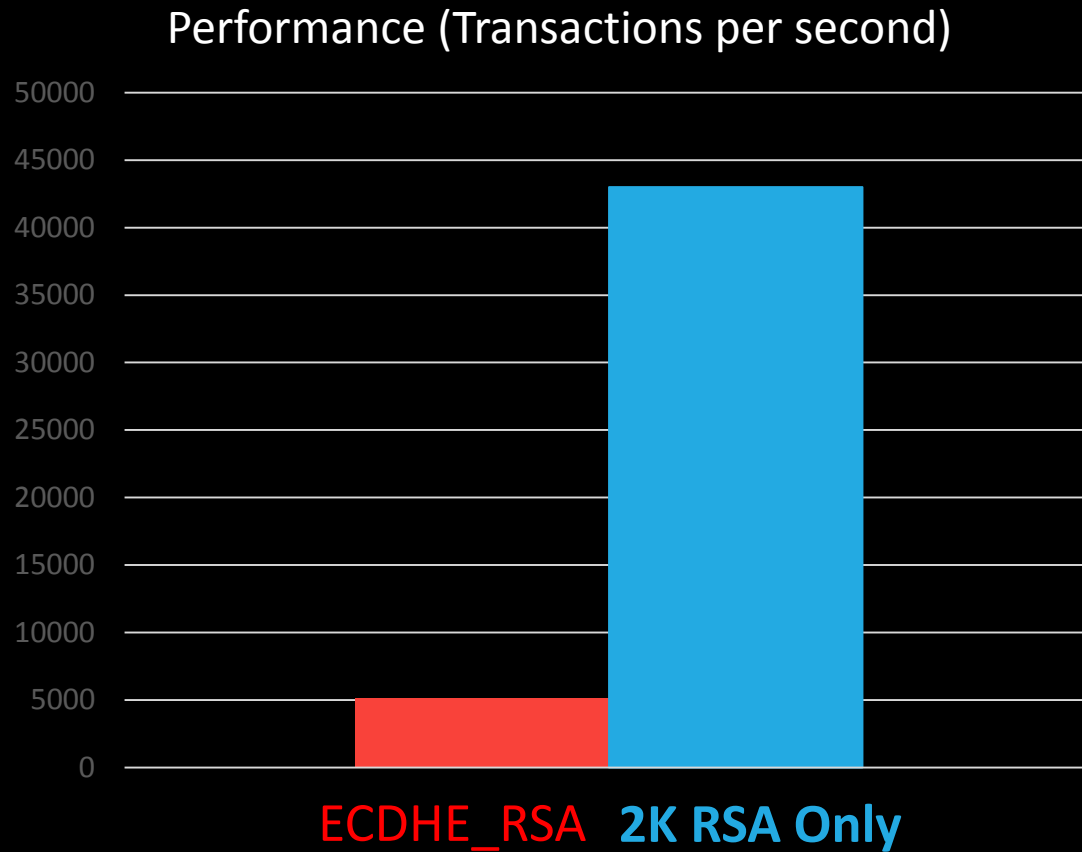
View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the internet.

ECDHE_RSA 性能问题



90%



CITRIX

长期的解决思路

负载均衡需能解决新型态应用与部署需求



高可用

交易不中断
本地高可用
多云高可用



安全

SSL加密
API安全



管理

多平台下应用
管理
一致性
分权管理



自动

多云平台下自动化
服务发现
自动扩展
自动配置



分析

多平台下应用
分析



一套走天下



ONE
to
ANY

硬件
虚拟
多租户
虚拟隔离
容器

OpenStack
NSX
OpenDaylight
Cisco
Nuage

...

ESX
Xen
> 形态
Hyper-V
> 虚拟化
KVM
> 云
> 编排
> 架构

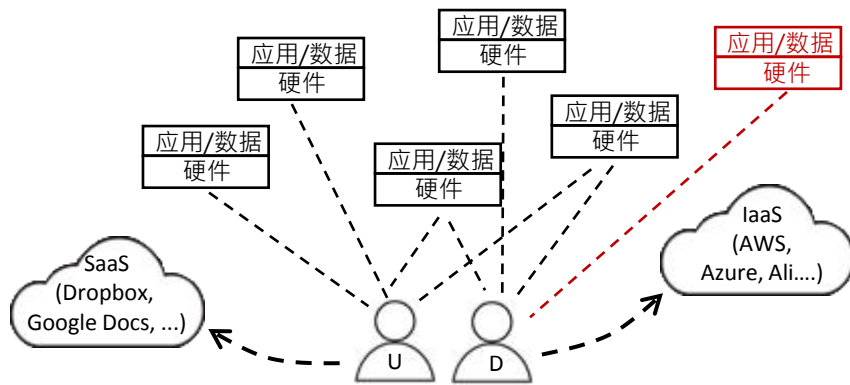
分散式架构
微分段架构
Hyperscale 超大规模
依应用架构
集中式架构

...

Amazon
Azure
Softlayer
...
私云

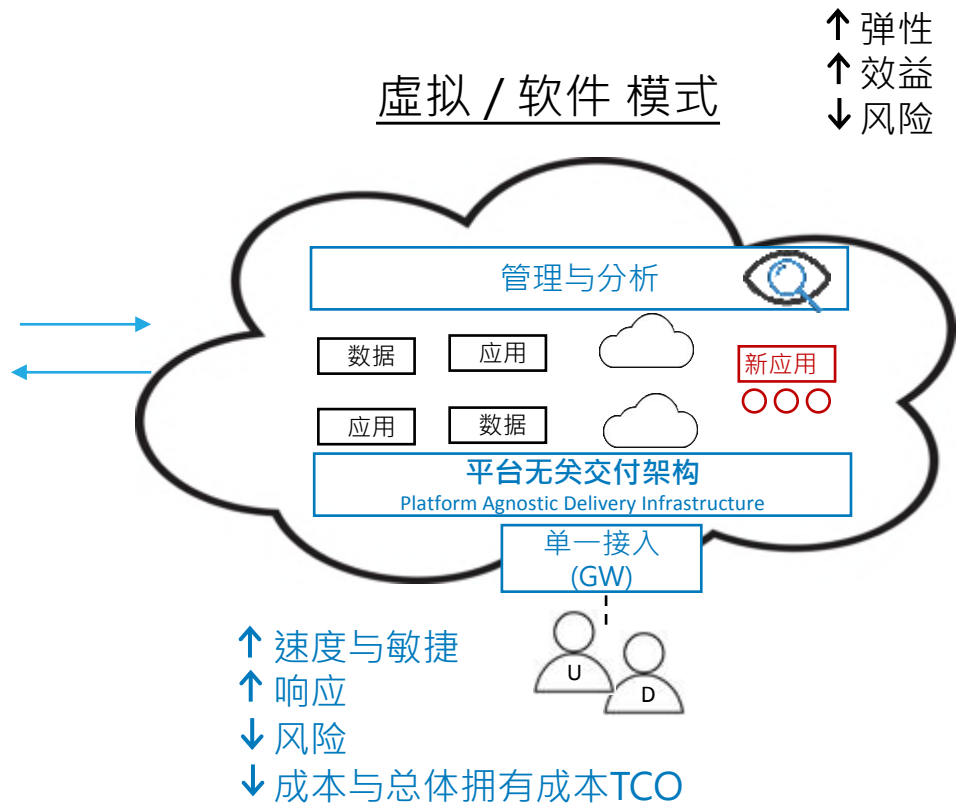
打造无边界数据中心

实体/硬件模式



- ↓ 弹性
- ↑ 复杂度
- ↑ 成本
- ↓ 安全

虚拟/软件模式



- ↑ 弹性
- ↑ 效益
- ↓ 风险

- ↑ 速度与敏捷
- ↑ 响应
- ↓ 风险
- ↓ 成本与总体拥有成本TCO

CITRIX

具体实践与演示

功能一致



NetScaler 部署于任何环境



功能一致

硬件
高性价比

=

虚拟
任何平台

=

共享
多租户

MPX



VPX
虚拟化



CPX
容器



SDX

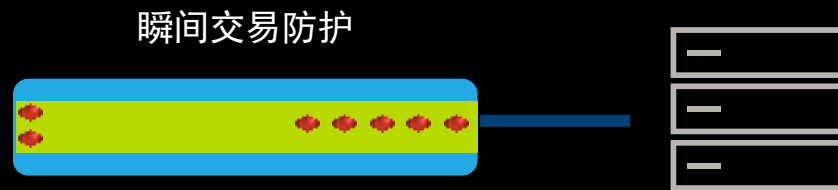


NetScaler解决新应用挑战



确保交易完成

Surge Protection技术，确保交易完成



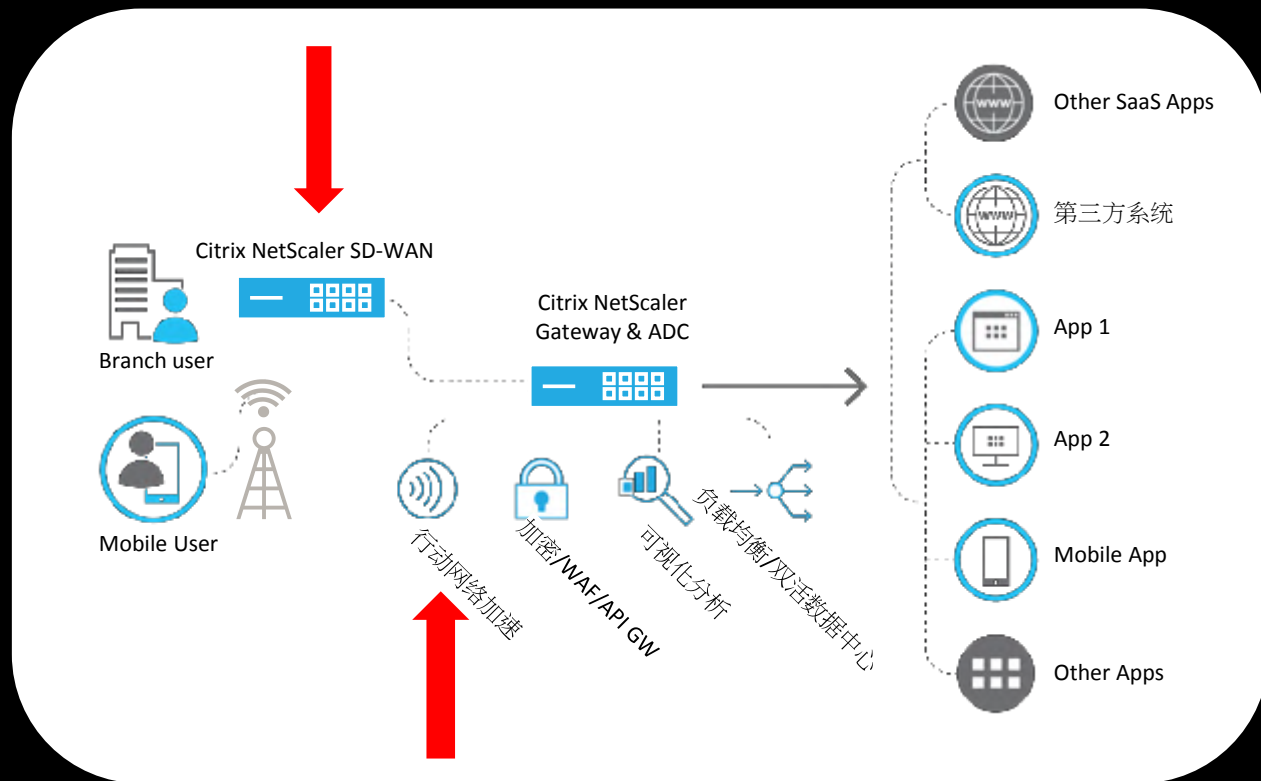
NetScaler解决新应用挑战



任何地点

SDWAN确保分店交易不中断

NetScaler加速行动网络



NetScaler解决新应用挑战



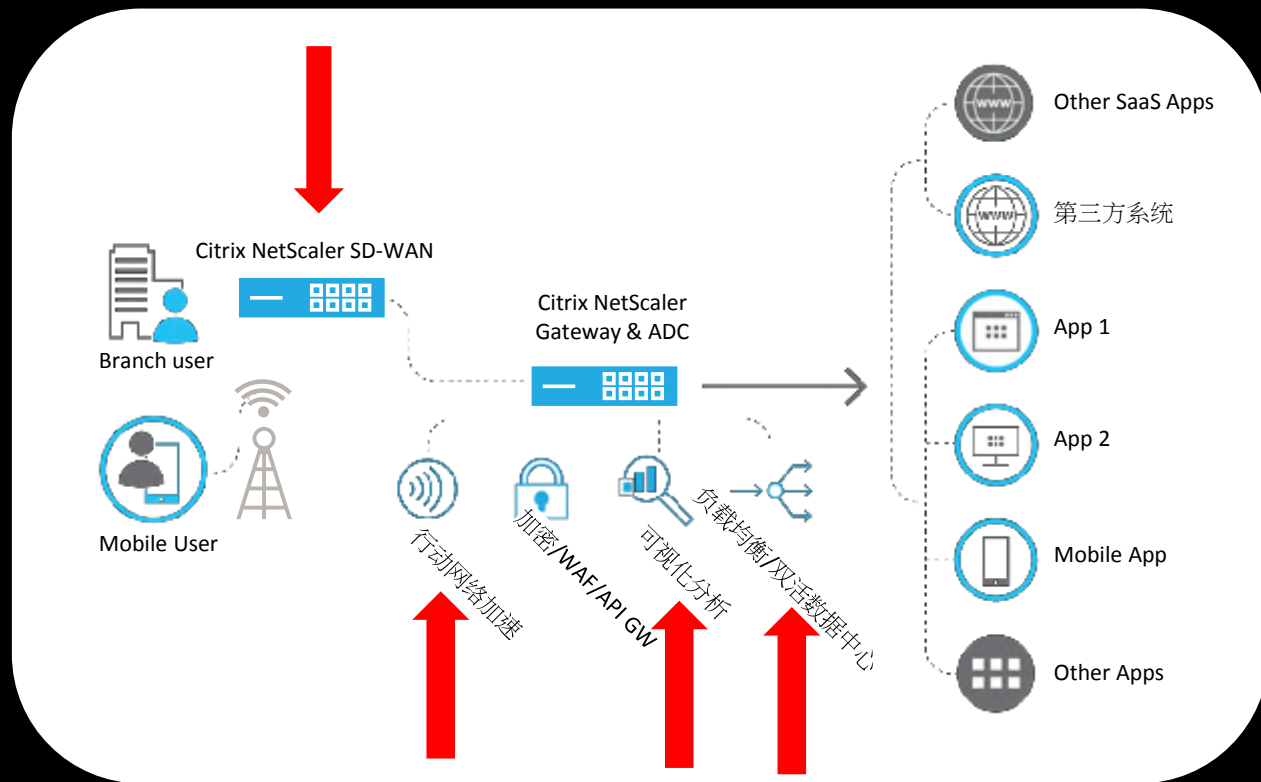
加快响应速度

SDWAN确保分店交易不中断

NetScaler加速行动网络

最佳负载分发

使用者体验分析



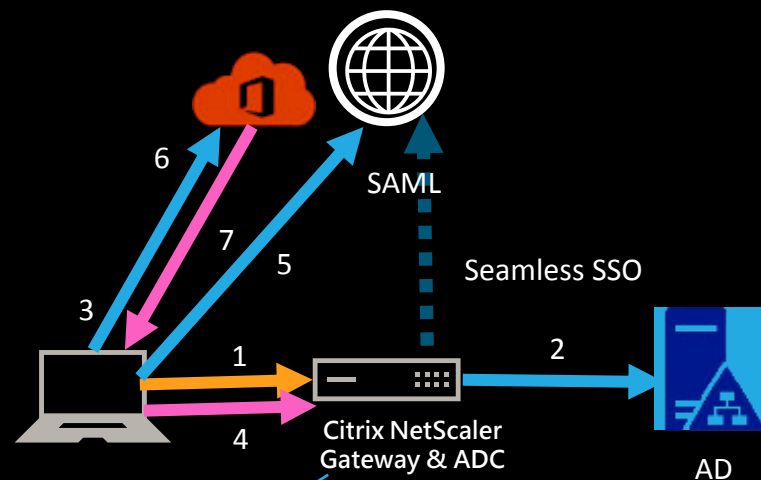
NetScaler解决新应用挑战



第三方接入

NetScaler提供
多种认证方式，
快速接入

登录行为监控

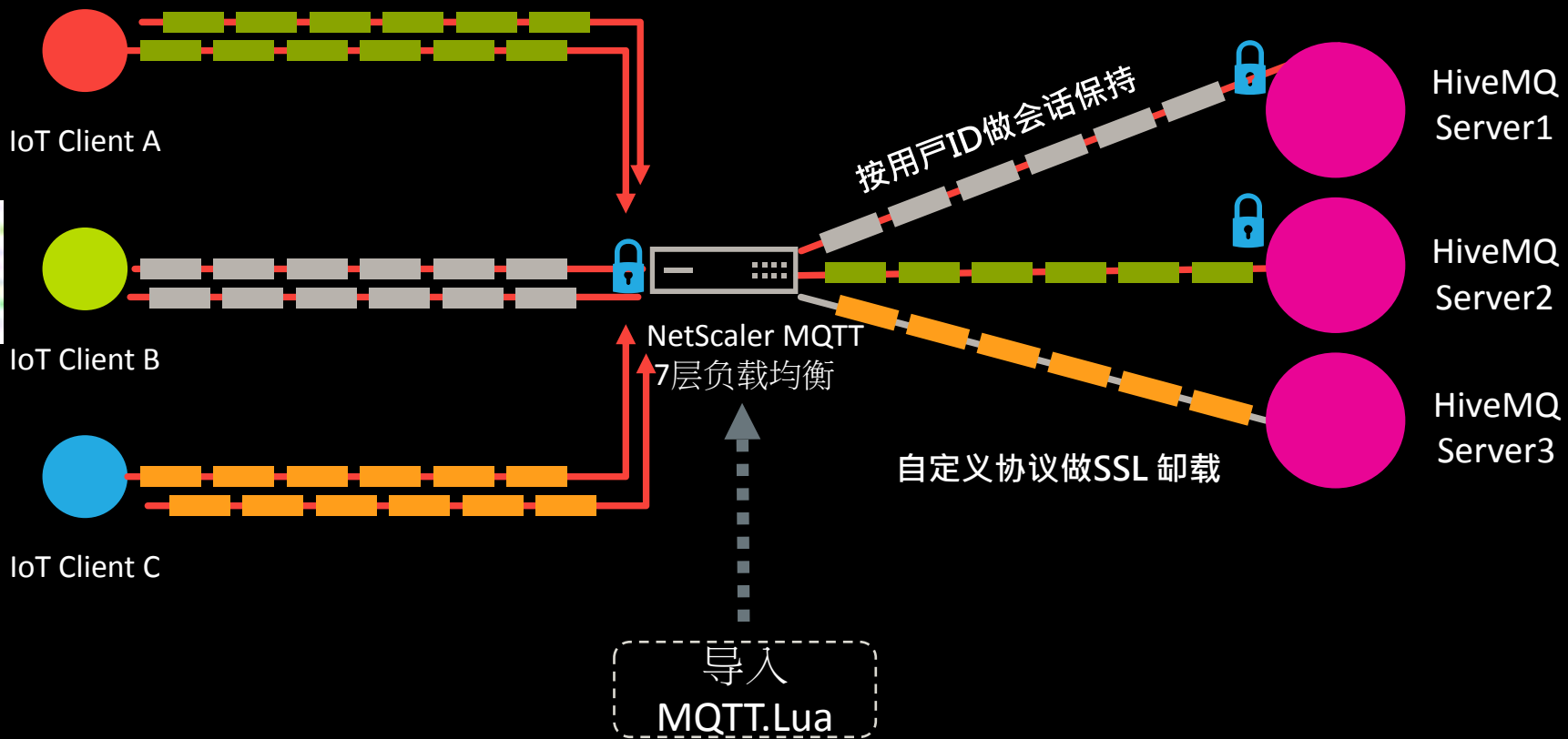


- NetScaler是SAML IDP 或 SP
- 支持SAML/Oauth/Form Base/LDAP/Radius/TACAS

自定义协议7层负载与加密

物联网时代，自定义协议降低安全风险

Microservice



NetScaler解决新应用挑战



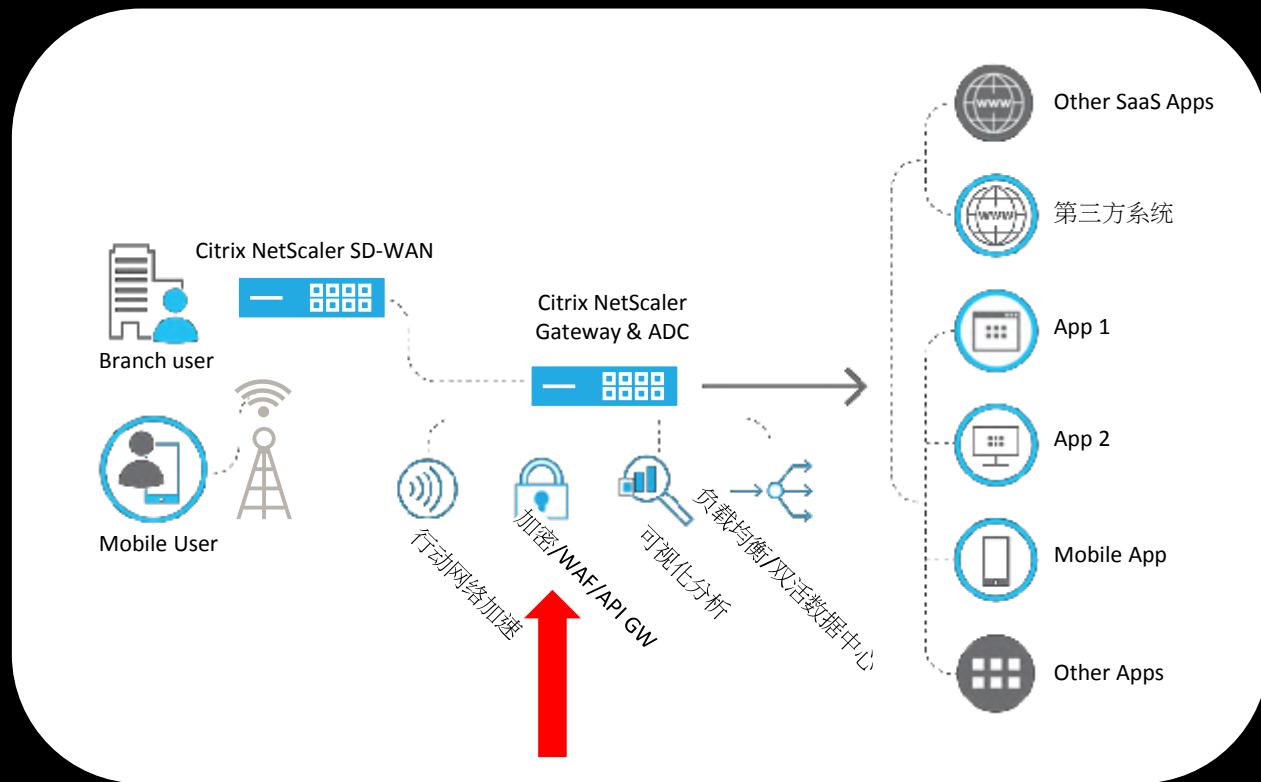
安全

满足Apple ATS
要求

最快SSL速度

WAF/API GW

DDoS防护



NetScaler 不换硬件下，ECDHE性能提升



NetScaler



~~硬件升级~~

8X

虚拟化支持



虚拟化支持



云平台支持

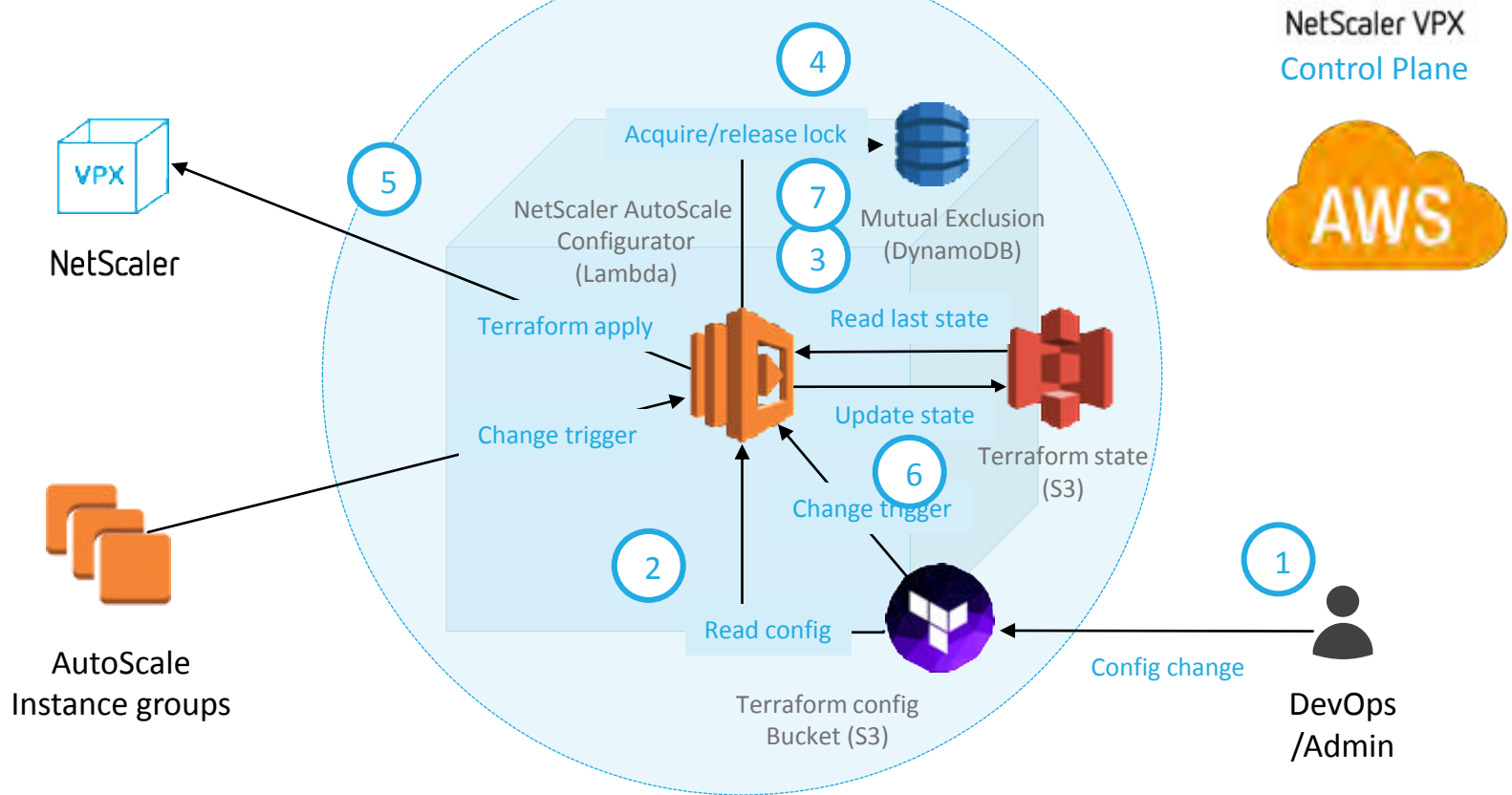


性能

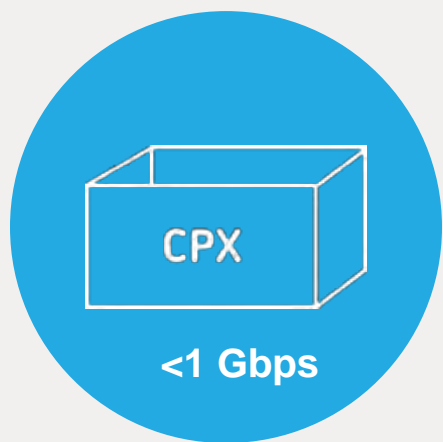
最高达

100 Gbps

计算资源自动扩展



容器原生支持



容器下部署



容器管理支持



MESOS



kubernetes
by Google

性能

可达

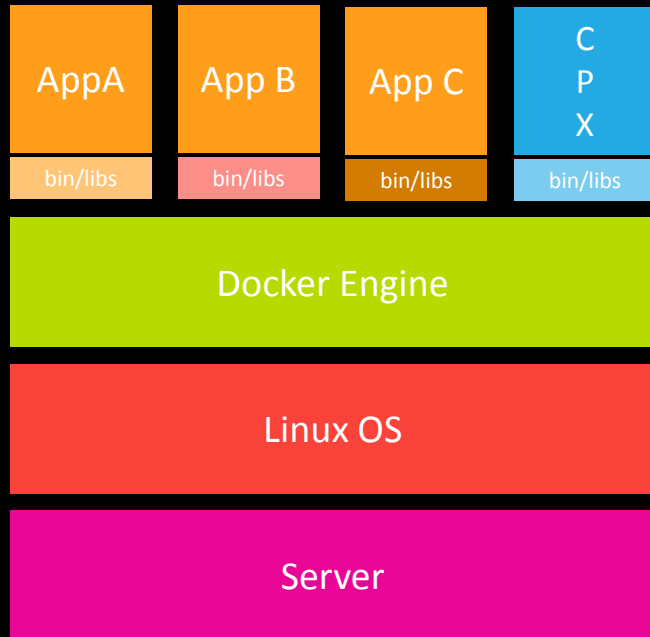
1 Gbps

Citrix NetScaler CPX Express

免费开发版

NetScaler CPX 原生容器负载均衡器

秒级部署



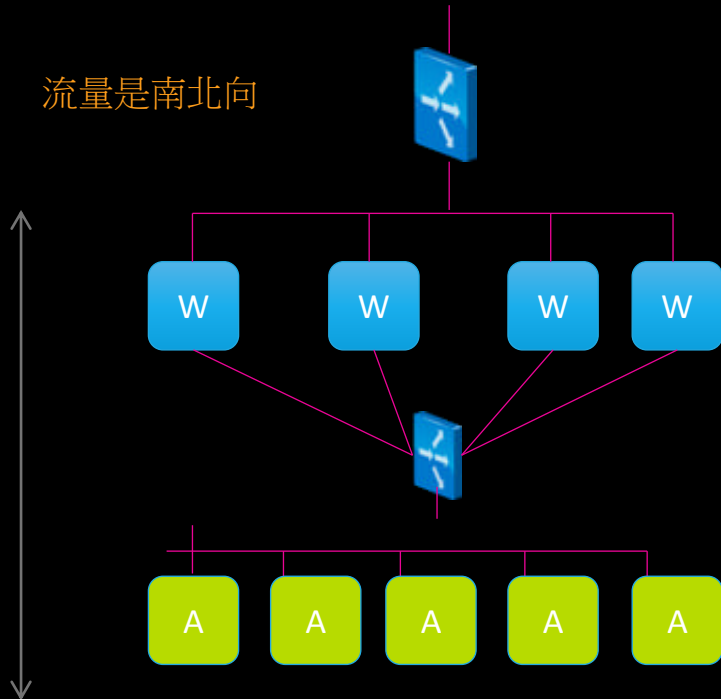
• CPX提供容器应用交付L4-L7服务:

- Content Switching
 - Responder
 - Redirect
 - Rewrite
 - TCP Optimization
 - SSL Offloading
 - DDoS
 - DNS load balancing
- 仅需 1 CPU core 和 1 GB 内存
- 免费版：NetScaler CPX Express (<https://www.microloadbalancer.com/>)



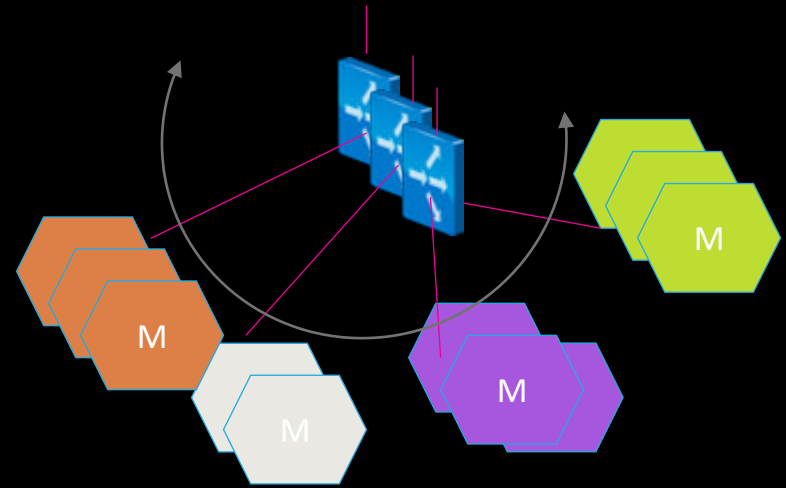
在容器世界中的负载均衡：传统vs微服务

流量是南北向



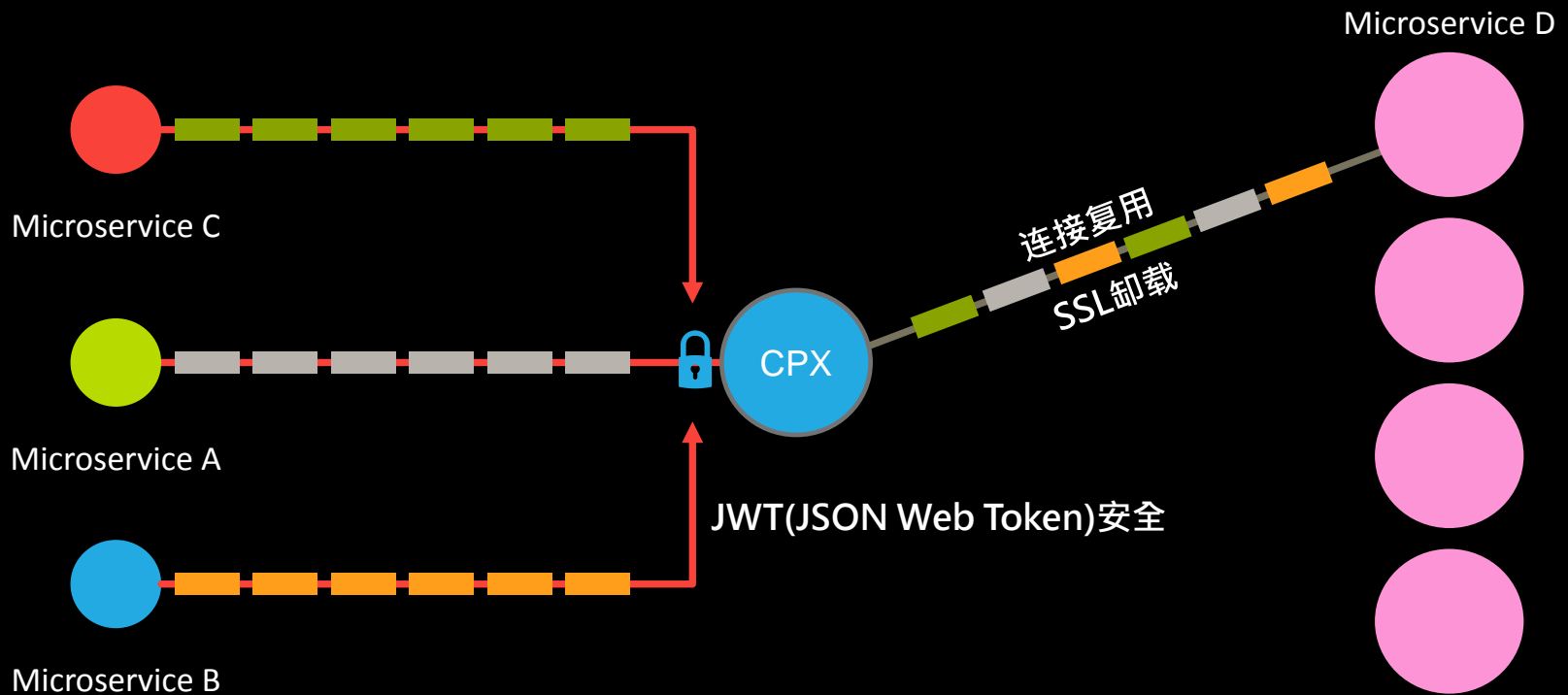
静态应用服务，定义良好的服务架构，但缺乏弹性

流量是混合南北向与东西向架构

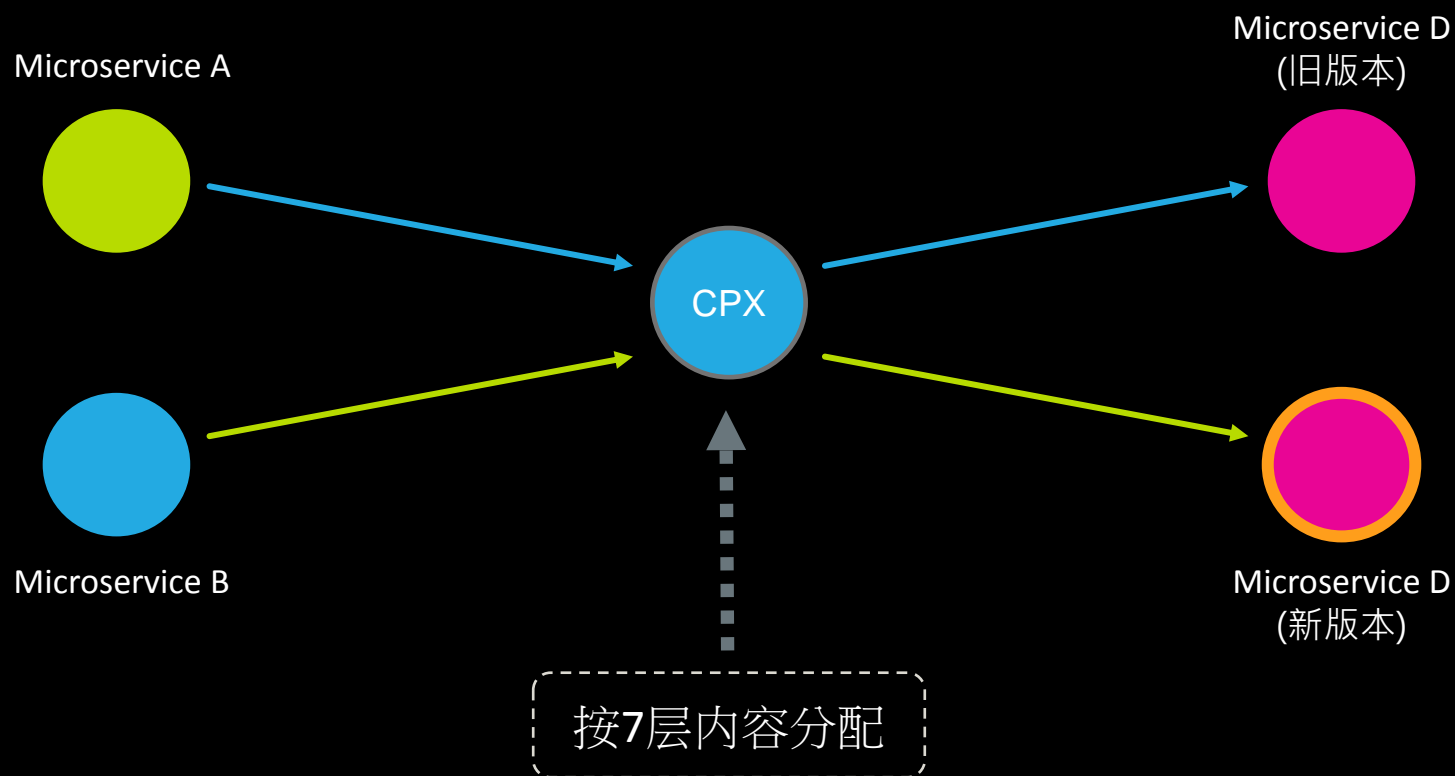


动态微服务，应用服务改变
敏捷高效自动化

典型场景：性能与安全提升



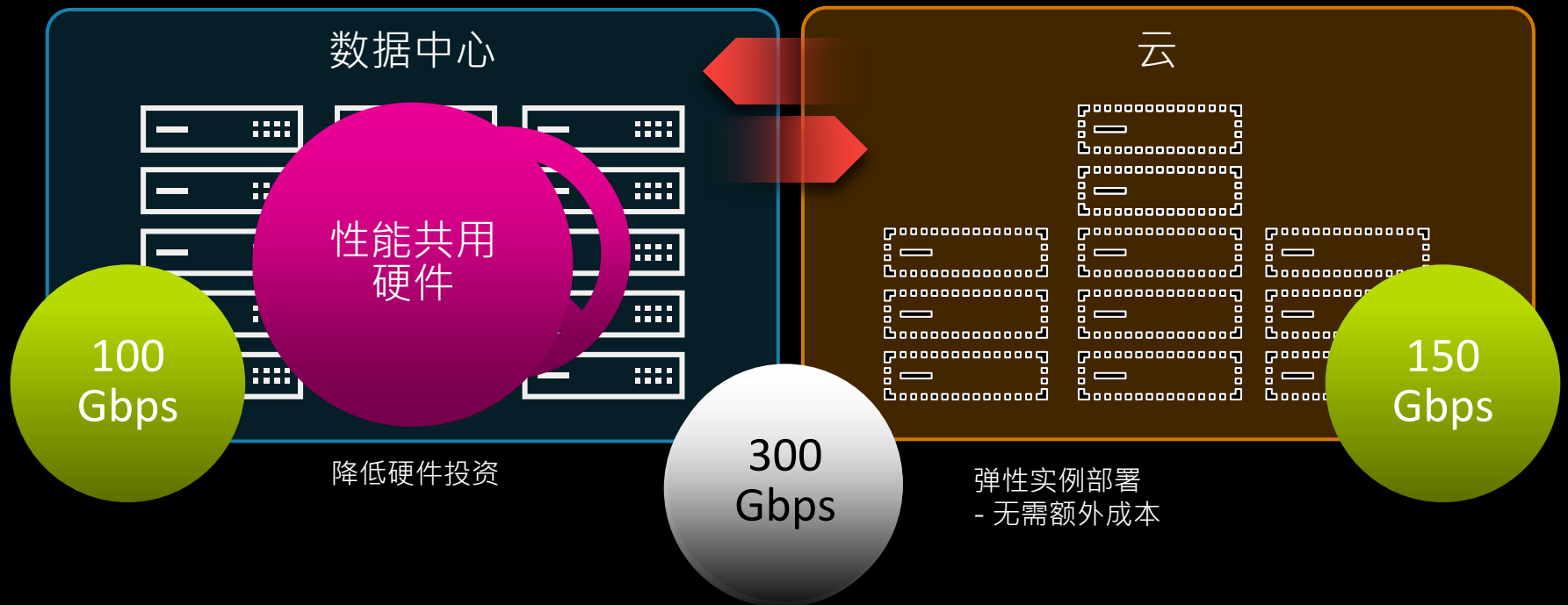
典型场景：灰度发布



开源对比

	NetScaler CPX	NetScaler CPX Express	HA Proxy	NGINX
负载均衡算法	16种以上及多种会话保持方法	16种以上及多种会话保持方法	有限	有限
UDP 协议支持	有	有	无	有
在线升级不中断	可	可	可	否
TCP 优化加速	有	有	无	无
连线分析与统计	有	有	有限	有限
管理与分析	NetScaler MAS 整体方案	NetScaler MAS 整体方案	无	仅云平台应用
客制化协议7层负载与加密	可	可	无	无
瞬间交易防护	可	可	无	无

TriScale²: 弹性性能转移



单一管理



NetScaler MAS 核心理念

1 自动化

- 敏捷专注
- 自动扩展
- 自动部署
- 自动管理
- 驱动成本降低

2 数据驱动

- 业务专注
- 交易可视(客户)
- 网络可视(运维)
- 流程可视(业务)
- 驱动成长

3 平台不受限

- 进入市场时间缩短
- 任何云平台
- 任何应用管理平台
- 任何形态
- 驱动时间竞争力

微服务架构支持模式

1

服务发现



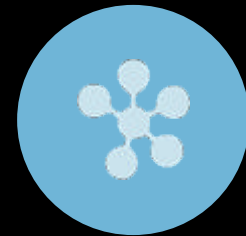
可扩展架构



服务代理



网络重配置



容器实例化,
容器注册

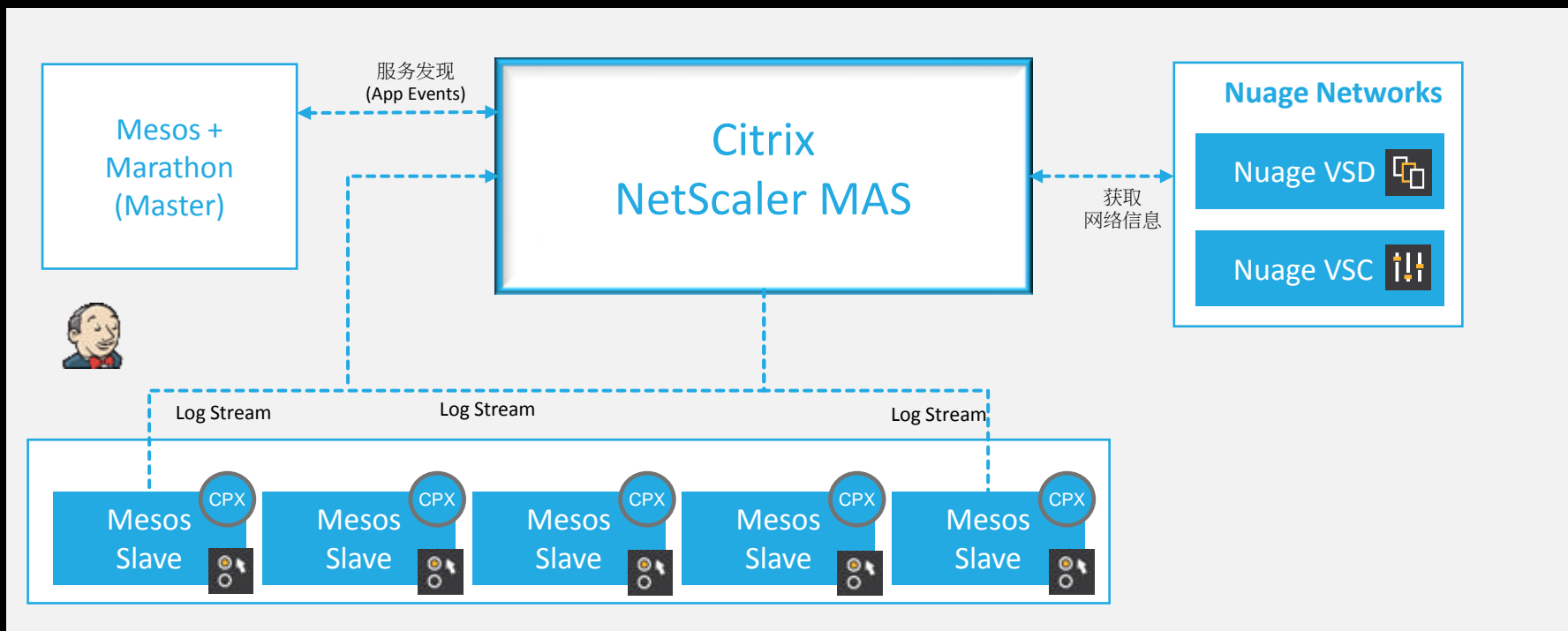


配置,
扩展

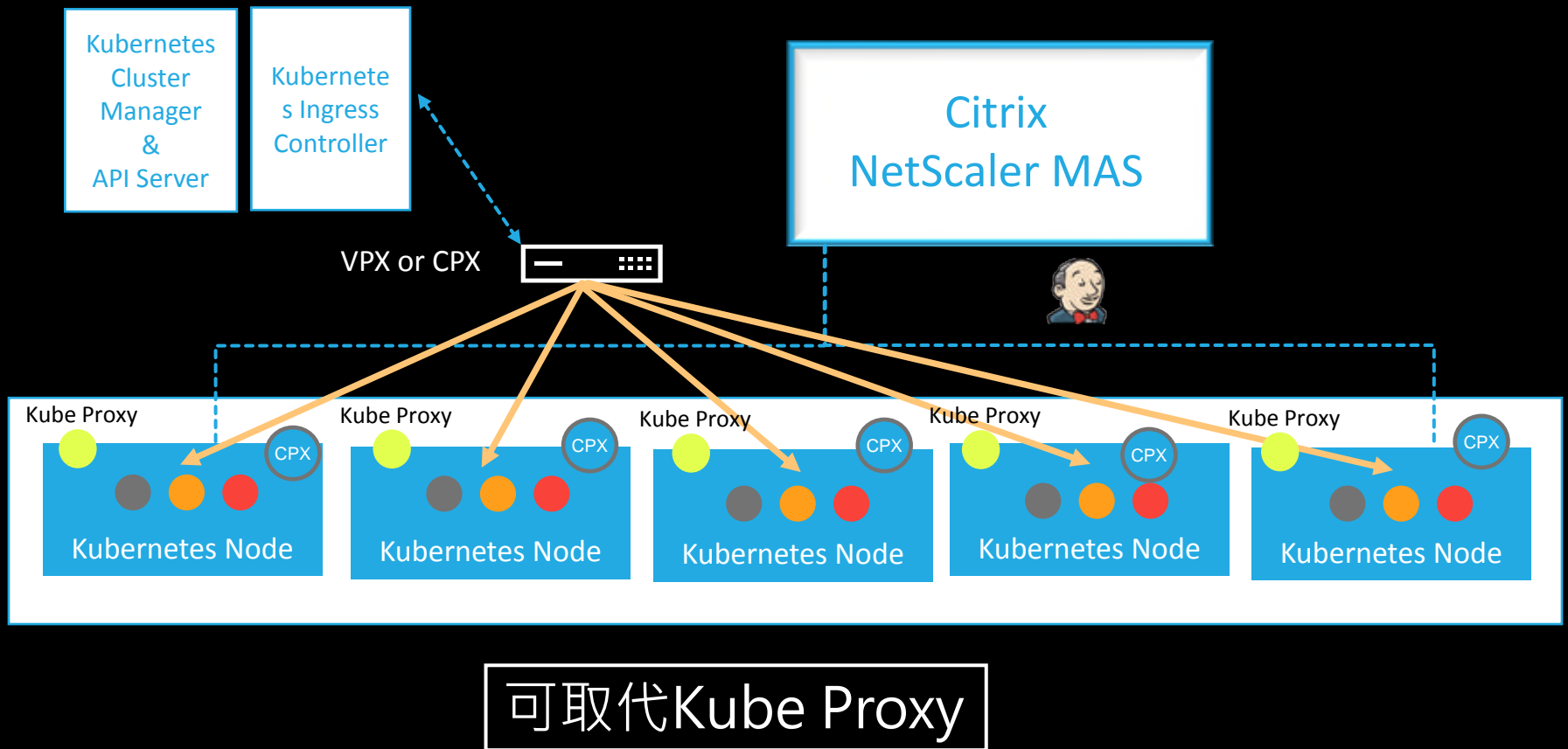
云原生支持

NetScaler CPX 在 Mesos 容器环境

与 Nuage Networks SDN整合

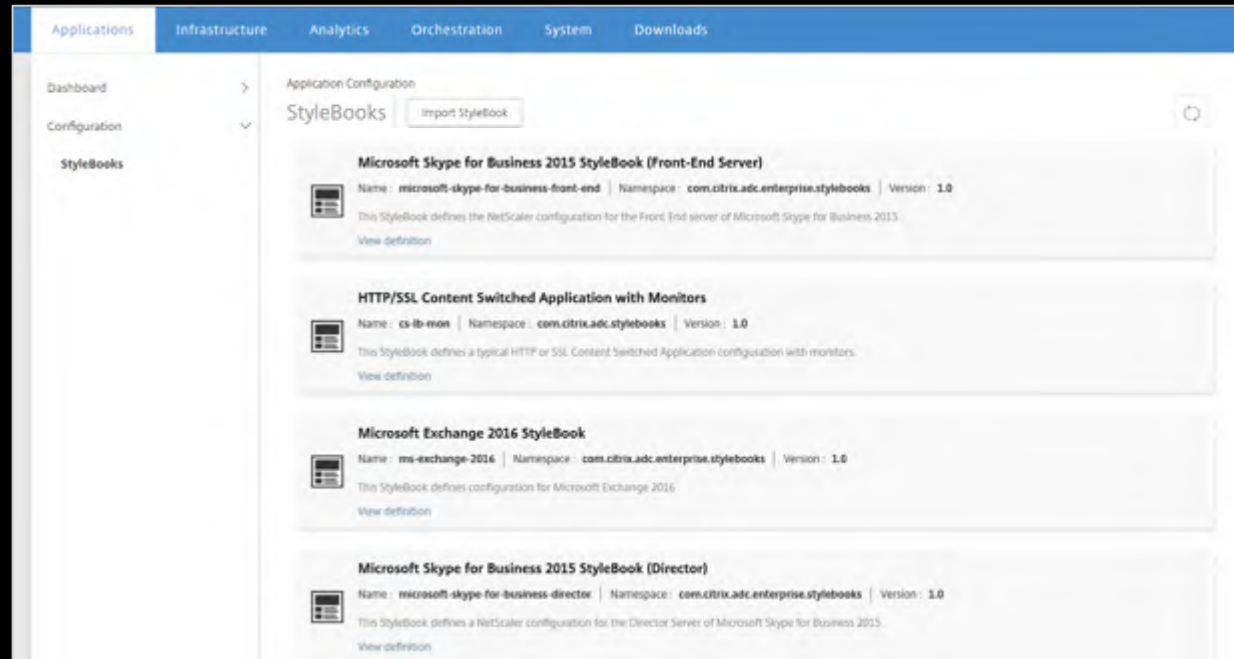
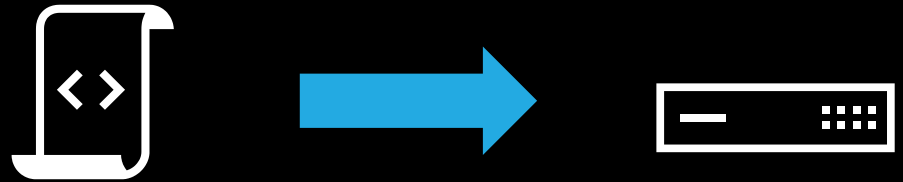


NetScaler CPX 在 Kubernetes 容器环境



MAS Stylebooks 自服务模版

- 可定制化的模板
- 用户脚本可修改
- 由IT认可的自助服务功能
- YAML语言
- REST API支持
- 版本控制
- 可透過URI生成



从分布式服务管理到可编程基础架构

可编程基础架构元素



演示

NetScaler CPX 整合在 Mesos Marathon

应用分析和网络分析

2

Network Reporting

容量和
使用率数据

SSL
vServer
ICMP
TCP
HTTP
Compression
UDP

INSIGHTS (Analytics)

应用层数据
容量规划，性能，威胁

HDX

Web

Security

TCP

SSL

Gate-
Way

Advanced Analytics

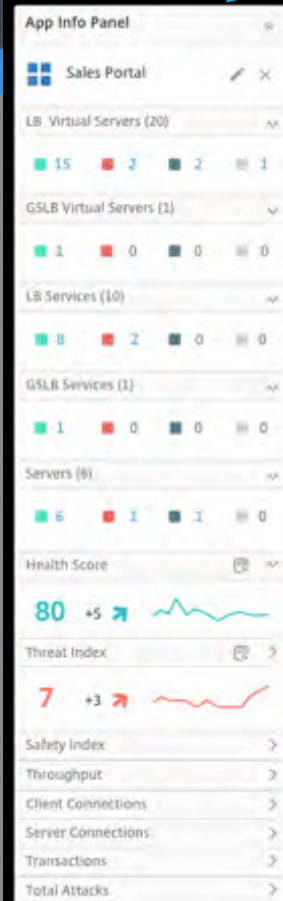
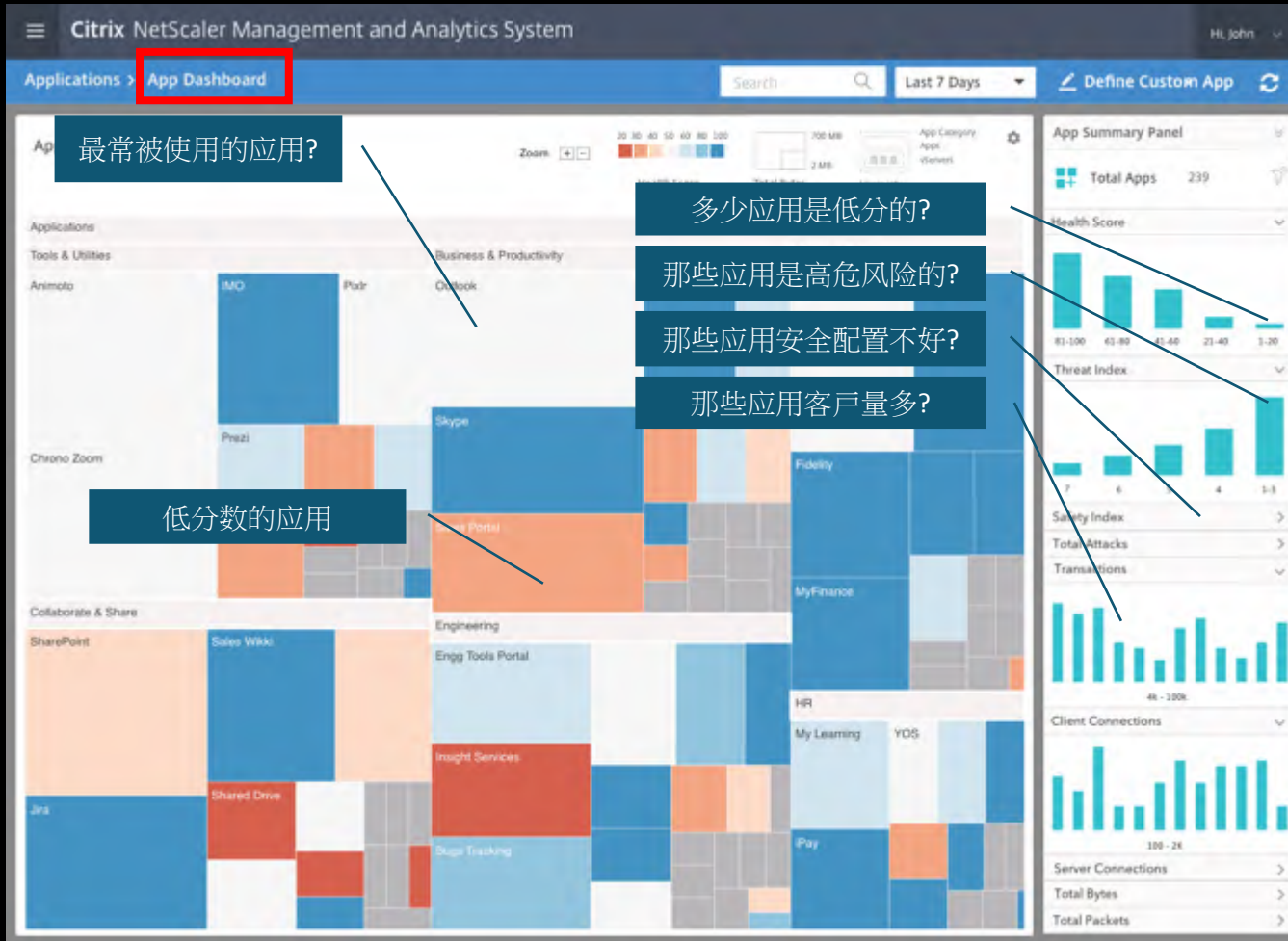
数据+其他高价值数据
用户影响场景

自动化
排错

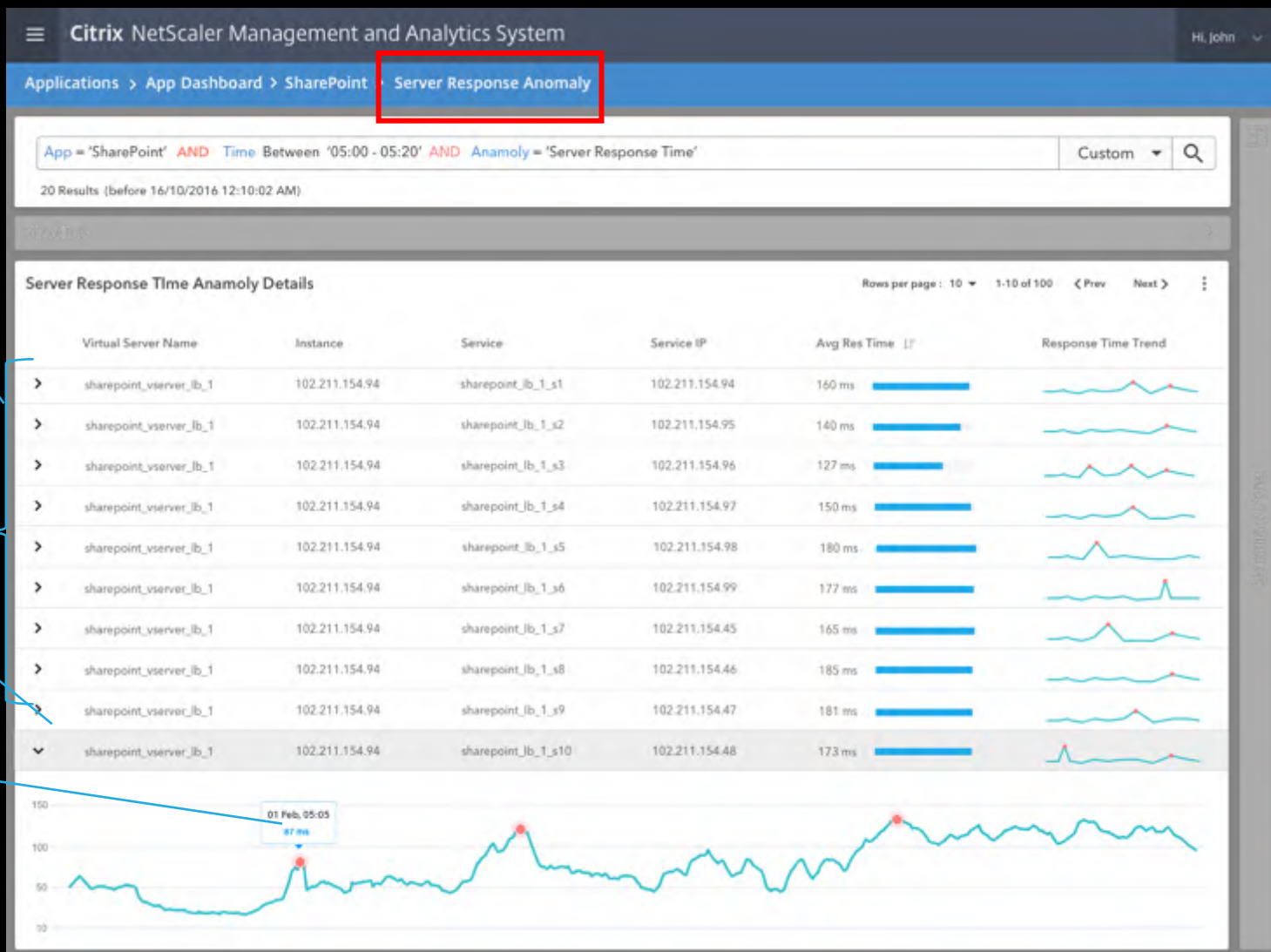
自动化
威胁检测

应用状态即时监控

管理者点击任何应用



服务品质异常监控



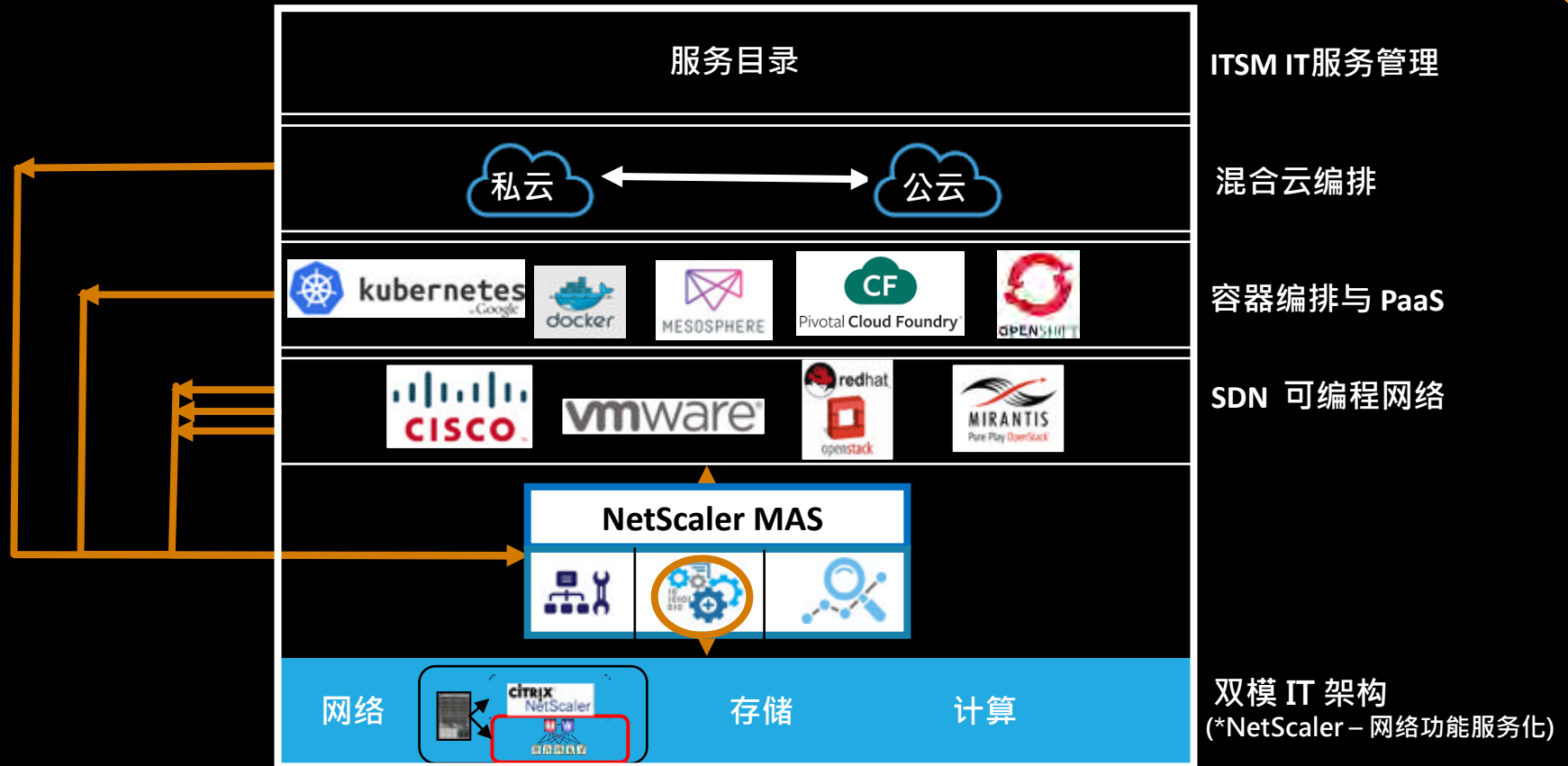
那一个后台服务器造成回应时间异常?

这台服务器的历史回应状况?

那个时间点侦测到异常?

Citrix NetScaler MAS 加速多平台下 应用自动化管理

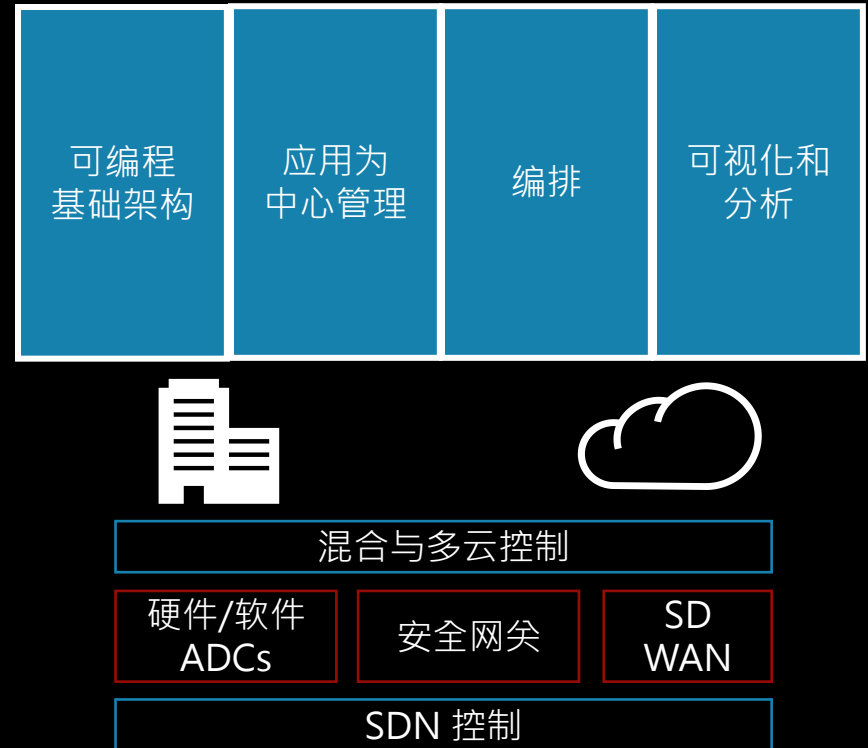
3



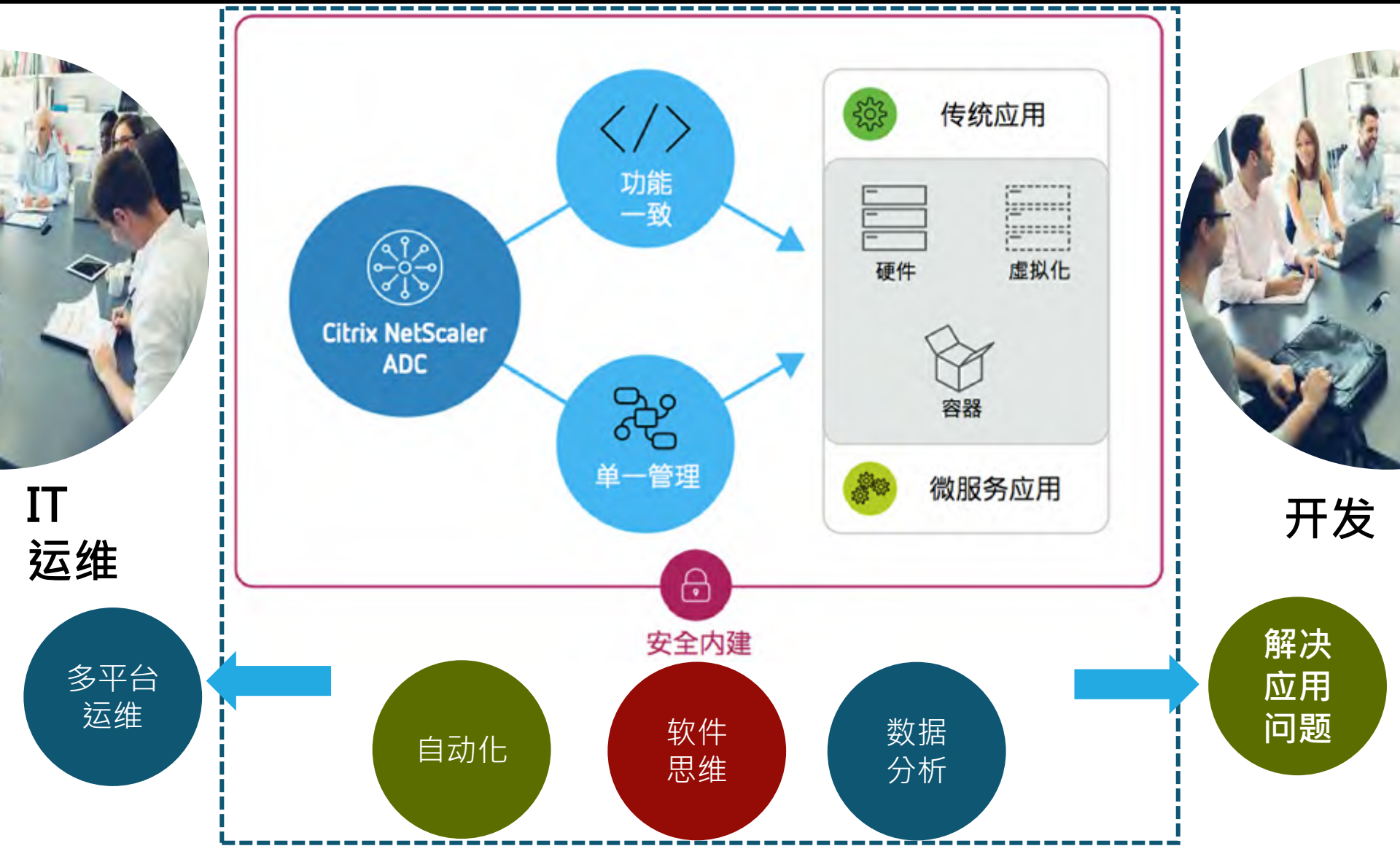
NetScaler MAS管理传统到新一代无边界数据中心中的ADC

新一代·无边界数据中心 管理

传统数据中心管理



新一代负载均衡加速DevOps/ITOps转型



全球超过40万企业部署思杰解决方案

100%

世界100强

99%

世界500强



感谢参与



CITRIX[®]

NetScaler MAS workflow

