甜橙金融网络架构演进的分享

--如何应对虚拟化、业务突发增长以及
应用架构变化带来的网络冲击

天翼电子商务有限公司

公司介绍

- 天翼电子商务有限公司（简称“甜橙金融”）是中国电信股份有限公司的全资子公司，作为中国电信旗下唯一的互联网金融平台公司
- 甜橙金融注册资本5亿元，由中国电信股份有限公司（00728.HK）出资
- 甜橙金融是国内首家电信运营商支付公司，是中国人民银行核准的第三方支付机构；作为进军互联网金融领域从事新业态的央企子公司，是兼具“金融、电信、互联网” 特点的创新企业
- 拥有**第三方支付、征信、消费金融、财富管理、保险、网络贷款**等金融牌照

甜橙技术Fintech体系

合作方

SaaS服务输出

- 风控：风险名单服务、信任环境甄别、风险模型计算
- 支付：支付服务、账户服务
- 认证：登录鉴权、实名认证、反欺诈

甜橙云PAAS

- 全局安全服务：众测平台、威胁感知、自动化攻击防护、安全审计
- 平台运维服务
  - 监控管理：业务实时监控、设备基础监控、资源动态监控、定制监控
  - 自动化测试：自动化测试平台、全链路压测
  - 资源调度：环境资源管理、一键式发布
  - 持久化：关系型数据服务、Kv数据服务、分布式缓存、NOSQL
  - 分布式中间件：事务服务、消息服务、数据源服务、动态配置服务
- 智能大数据服务：流式计算、模型算法、流程管理、Hadoop、Spark

基础设施

IAAS平台API

- 资源虚拟化：VMWARE、负载均衡、存储、计算资源、DOCKER、SDN

数据服务API

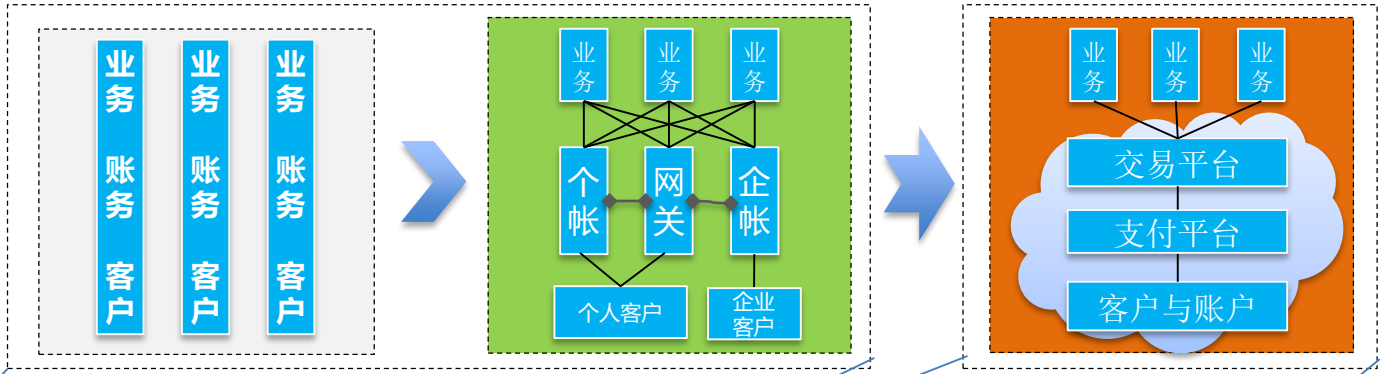
- 资源标准化：容量管理、节点管理、容器管理、版本管理、日志管理、CMDB

甜橙金融-技术架构演进历史

甜橙金融架构演进

1.0：“一把蜡烛“ 2.0：“烛台上的蜡烛“ 3.0：

流水账



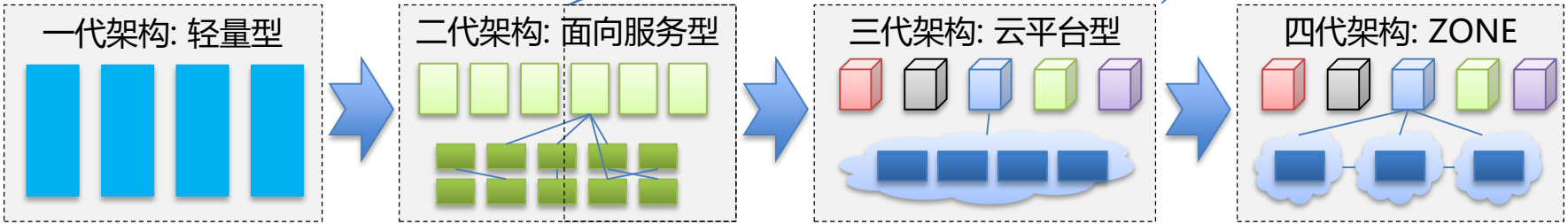
复式记账

单业务条线架构
2011年~2013年

传统非金融业务架构
2014年~2015年

互联网云平台架构
2016年~2017年

支付宝架构演进



2005年~2007年

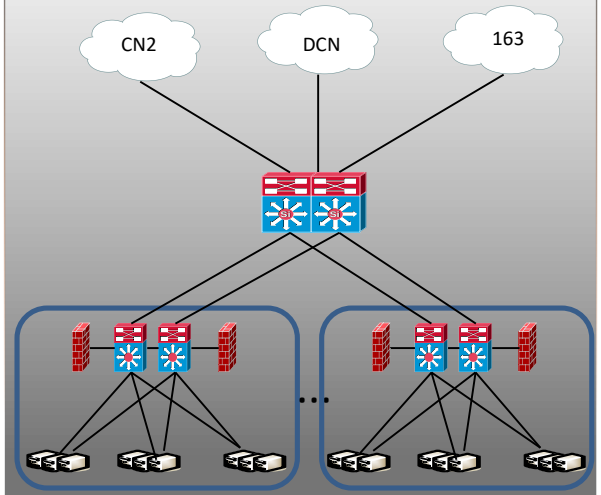
2008年~2010年

2011年~2013年

2014年~2018年

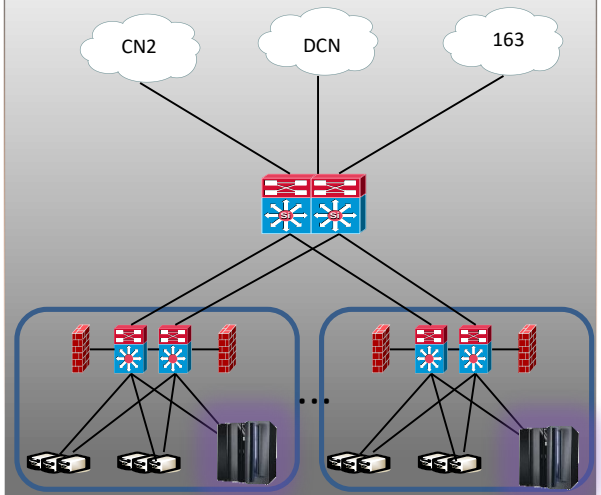
网络随着业务的逐步演进

前期较少业务



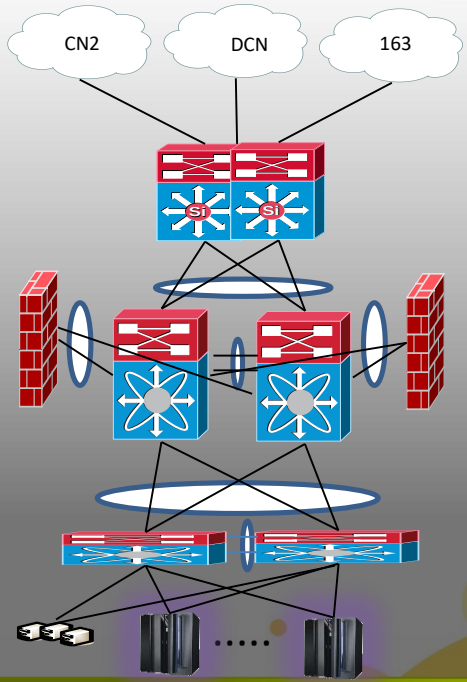
传统三层架构网络 + X86服务器

中期业务快速发展



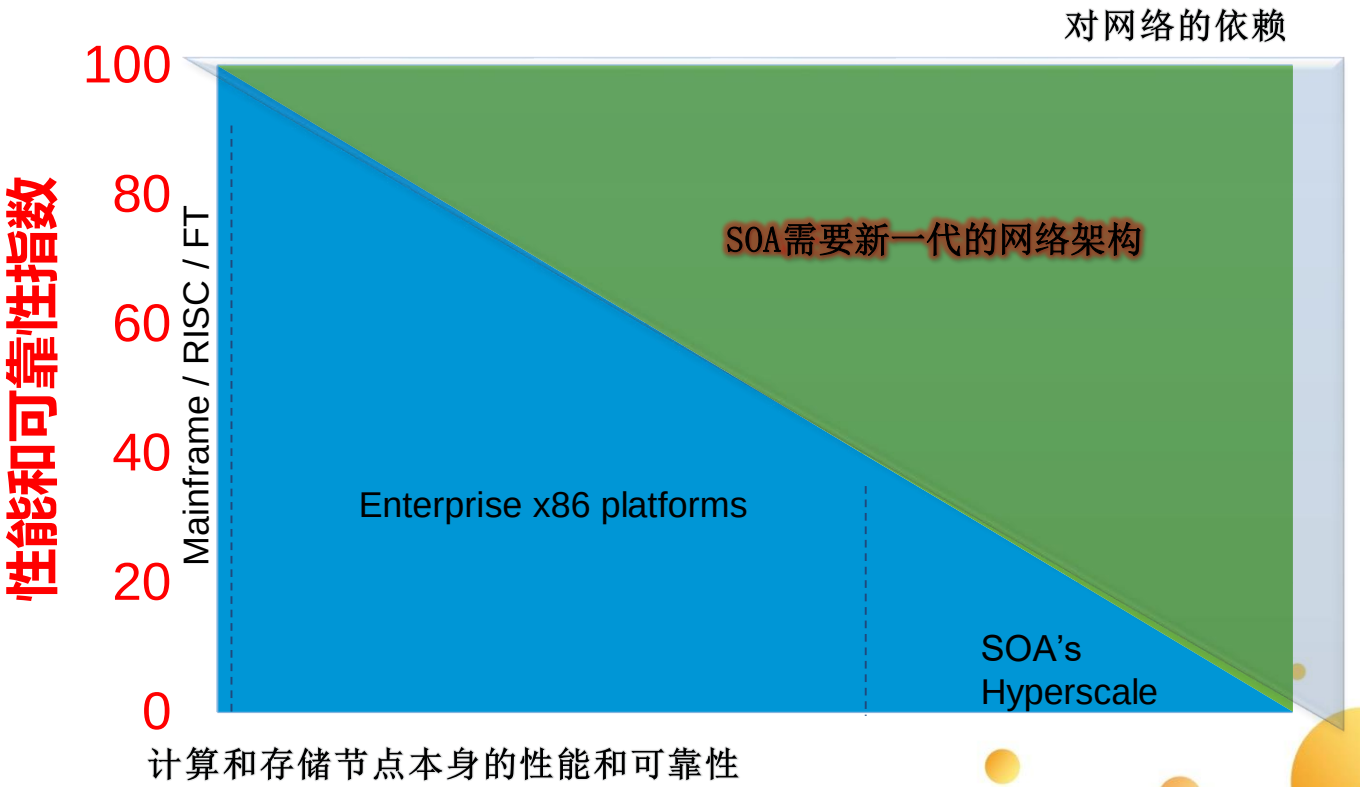
传统三层架构网络 + X86服务器 + 小型机

当前业务增长迅猛

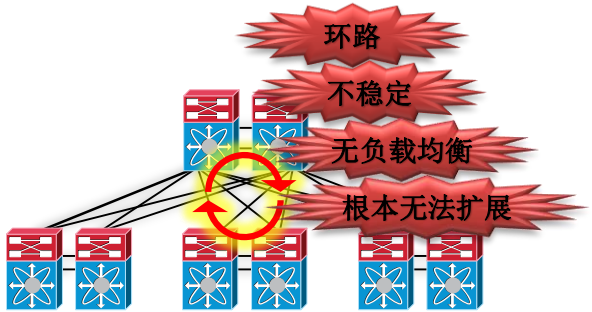


传统网络 + 网络虚拟化 + X86服务器 + 小型机 + 初步SOA

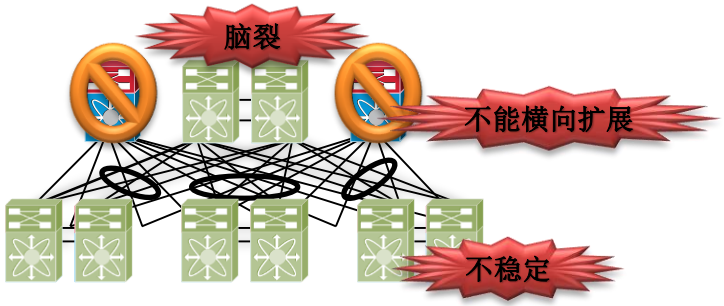
网络更多的参与到计算过程中



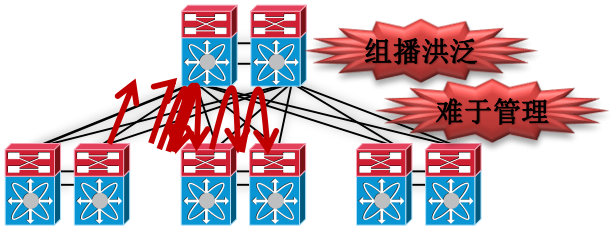
传统设计中遇到过的一些问题分享



传统生成树



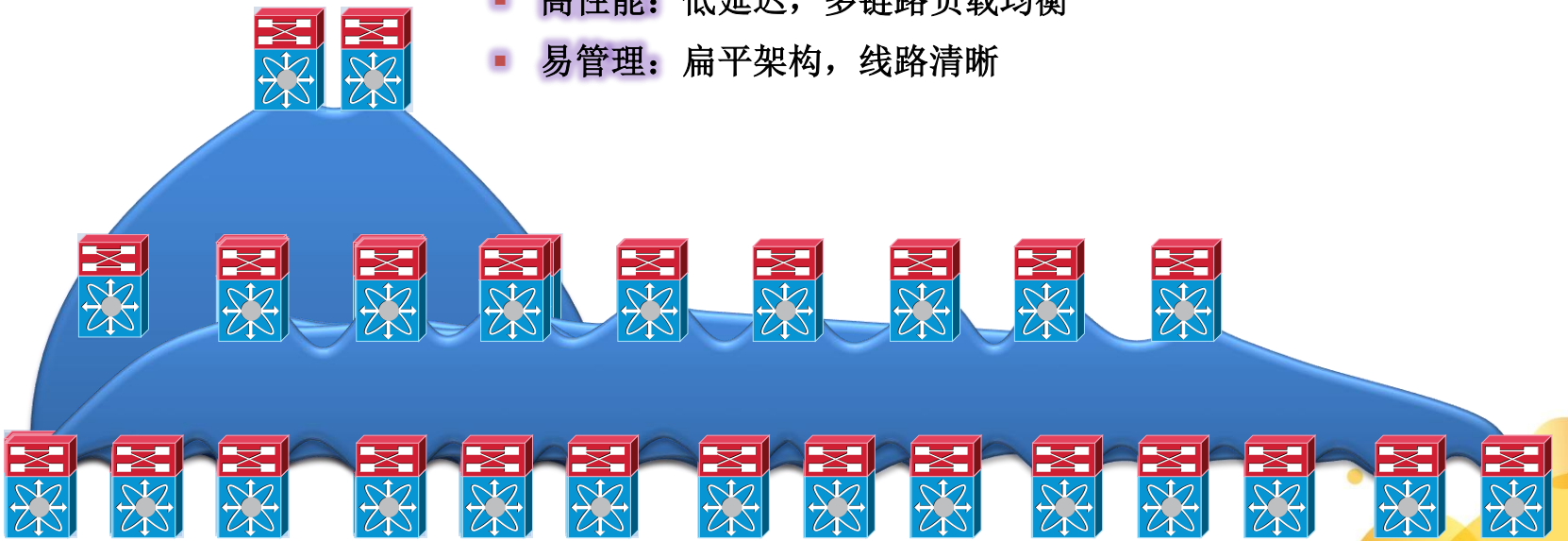
传统跨机箱捆绑



传统VXLAN

全新的弹性网络结构

- **Pay as You Grow：** 动态横向扩展
- **VLAN Anywhere：** 二层处处可达
- **高可靠：** 广播控制、差错隔离、松耦合
- **高性能：** 低延迟，多链路负载均衡
- **易管理：** 扁平架构，线路清晰



目录

智能化之前的困境（一）

瓶颈
有状态
延迟增加
SOA高并发场景下选型困难

VS

监管要求
隔离
管控

一次访问操作3套防火墙，配置超过50行

智能化之前的困境（二）

A

设备规划散乱

配置不一；网络不一，内部网络架构复杂；属于烟囱式平台管理方式

B

资源池规划散乱

无法对资源进行统一的生命周期管理

C

开通准备周期长

研发与运维之间沟通成本高

D

缺乏统一策略管控

协查困难，缺少知识传承

E

分布式的业务特性

带来高并发场景下的高失败率

惨痛经历血泪史分享

目录

智能化之后的效果（一）

ACI

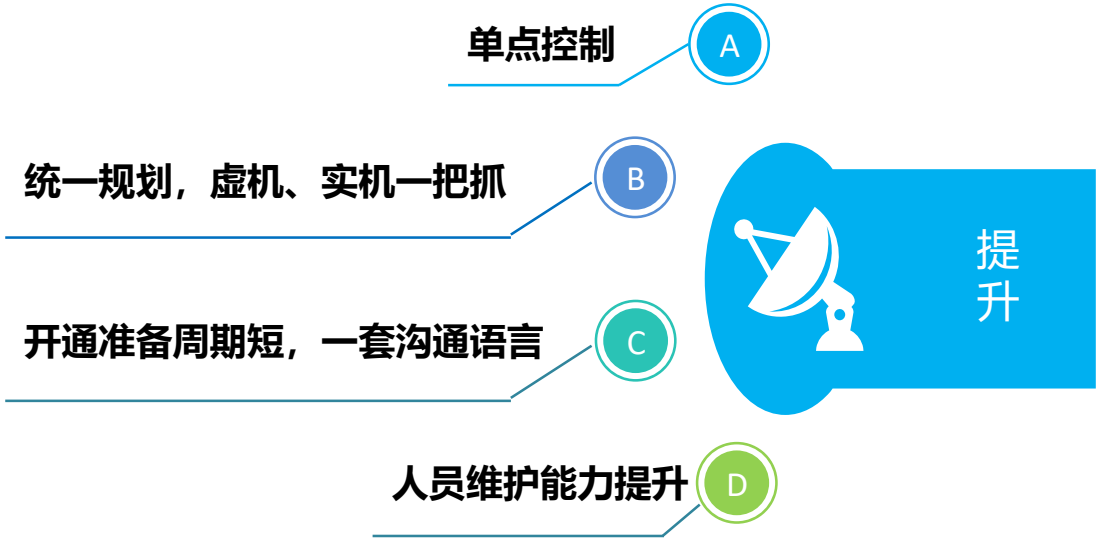
低延迟
无状态（切换不断长链接）
无瓶颈可扩展
适合SOA场景，适合分布式场景

&

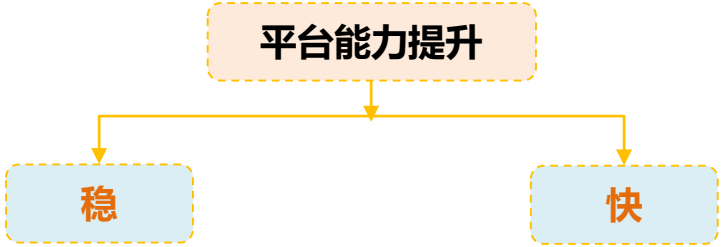
监管要求
隔离
管控

一次访问操作，一分钟搞定

智能化以后带来的提升（二）



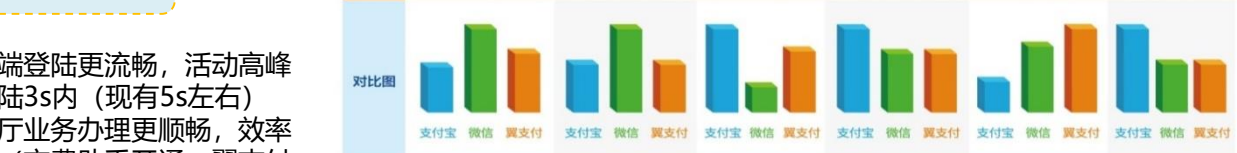
智能化以后带来的提升(三)



1. 后续系统升级服务不中断，用户无感知（现在部分业务有影响）
2. 平台服务可用率大幅提升（98.6%→99.99%）
3. 运维可用率提升到99.996%
4. 水电煤、话费充值、理财等业务系统故障发生后恢复效率提升30%（平均70分钟→50分钟）

1. 客户端登陆更流畅，活动高峰期登陆3s内（现有5s左右）
2. 营业厅业务办理更顺畅，效率更高（交费助手开通、翼支付开户）
3. 全国业务(营业厅、pos)并发受理能力大幅提升（1000笔/s→3000笔/s，还可以持续提升）
4. 套餐红包返利更快、高效（1小时→10分钟内）
5. 单机处理能力和支付宝、微信等水平一致

3.0 平台整体性能目标一览表

各支付平台	账务处理能力				交易处理能力	
	单个会计事件的事务处理时长(ms/笔)	单次余额更新的事务处理时长(ms/笔)	单机并发会计事件目标数(台)	单机并发余额更新事务处理目标数(台)	单个交易处理时长(ms/笔)	单机并发交易处理数(ms/笔)
支付宝	9	8	3500	7000	30	7000
微 信	12	10	2200	5000	40	5000
翼支付	10	8	3000	5000	50	5000
对比图						

各支付平台	客户平台能力		风控平台能力	中间件统一服务能力		登录状态
	单次客户信息查询处理时长(ms/笔)	单次客户信息查询并发处理数(W/台)	风控事件的单次判断处理能力(ms/笔)	单次消息通信速度(ms/条)	单机并发处理消息数(ms/笔)	同时登录保持在线数(W/台)
支付宝	15	10	10	4	4	5
微 信	15	10	20	8	7	8
翼支付	15	10	15	5	5	5
对比图						

备注：整体性能指标阐述按单台标准机器的处理能力进行列示，单台标准机器的配置为（双核8G内存），这个配置后面将作为信息技术部的唯一标准进行衡量。

通过建规范及推行应用改造、权限把控、自动化平台搭建等解决问题

YunShan Networks | IT大咖说 知识共享平台

问题

- 部分应用仅支持单点部署
- 集群的节点隐藏着差异：比如定时任务
- 对本地环境依赖
- 个性化的应用
- 无法准确判断节点的健康状态，特别假死
- 难以快速复制的网络

一 建规范；推改造

1. 统一架构
2. 健康检查页面
3. 会话共享
4. 文件存储规范

1. 涉及改造应用：413个
2. 剩余95个应用为非标或者厂商应用

二 试迁移；爆问题

1. 通过迁移应用，提前暴露各种不规范问题。通过试迁移100多个应用，提前发现各种问题

三 控权限，避免二次不规范

1. 严格控制服务器权限，避免二次不规范的产生，回收了消费金融、征信、预付卡等的权限

四 通过EPG管理应用及网络

1. 内部调用：标准端口网络互通
2. 对外提供的地址：全部通过NGINX，有据可查；网络关系更清晰
3. 网络开通按照epg开通，快速扩容中的网络卡点将不复存在

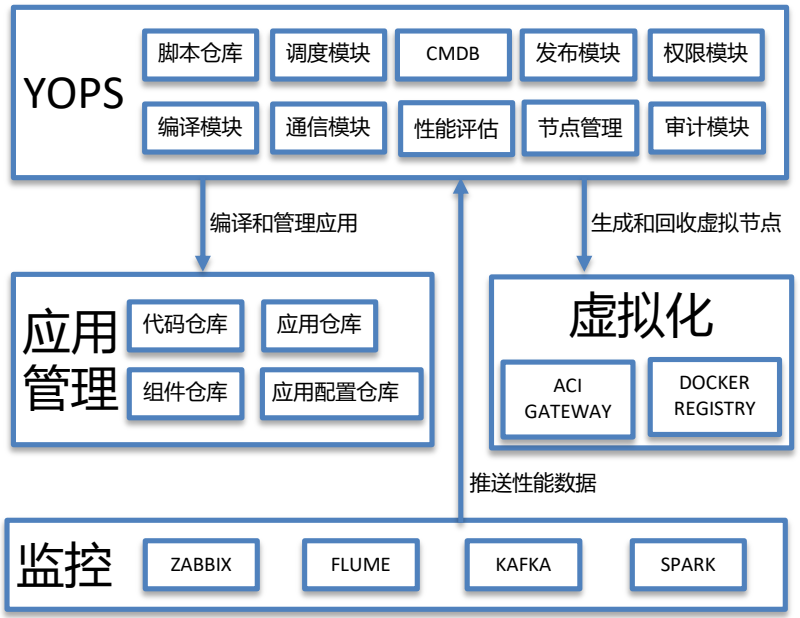
五 梳理了网络和dns

1. 梳理完成：1100条网络
2. Dns迁移：209条

后续所有应用信息以及网络信息均会维护在自动化运维平台里

目录

自动化运维架构



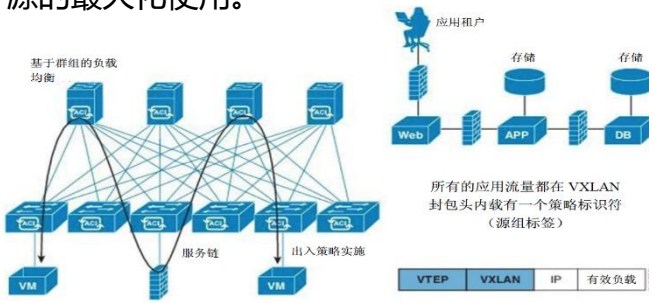
- 全平台采用PYTHON自主研发，并结合了MAVEN、GIT、ZABBIX等业界实践过的优秀开源组件
- 通信模块采用主流的自动化配置管理工具SALTSTACK，高效稳定且集群易于扩展
- 主机虚拟化采用轻量化容器DOCKER并做了定制化，在实现应用有效隔离的同时最大化利用主机资源
- 网络虚拟化采用行业领先的CICSO ACI技术，完全实现SDN
- 系统监控采用老牌组件ZABBIX，应用监控采用最新的FLUME+KAFKA+SPARK，实时感知应用压力变化，并通过自主开发的智能学习模型感知扩容阈值，实现弹性计算
- 权限和审计模块做到每次线上操作事前有管控，事后可回溯，保证线上生产环境安全稳定

基于全局资源虚拟化的自动化运维平台以及SDN建设

智能化运维的解决基石

基于全局资源虚拟化的自动化运维平台

1. 甜橙云引入了**全局资源虚拟化的体系**，对计算、存储、网络资源分别进行统一的池化，在统一资源调度平台的融合下形成全局的弹性。
2. 通过对运行时状态下的应用在Load、IO、流量等数据的动态监控，弹性地增减资源使用情况，达成在低运维成本情况下对设备资源的最大化使用。



SDN建设

SDN的价值

- 提升运维效率
- 降低运维成本
- 快速自动化部署

近期成果

- 工单模板调研及目标制定
- 部署安装TOOLKIT及SDK
- 编写PYTHON SDN程序V1.0及配置下发验证

SDN建设的近期成果-工单模板调研及目标制定

YunShan Networks | IT大咖说 知识共享平台

ACI环境SDN工单模板调研及模板制定完成

H19

	A	B	C	D	E	F	G	H	I	J	K	L
1	Tenant	Contract	Provide_EPG	P_AppPrf	Consume_EPG	C_AppPrf	FilterEntry	Protocol	sFromPort	sToPort	dFromPort	dToPort
2	sunzhibin	APP_CON	APP_EPG	APP_PRF	WEB_EPG	APP_PRF	TCP_25	TCP	1	65535	25	25
3	sunzhibin	DB_CON	DB_EPG	APP_PRF	APP_EPG	APP_PRF	TCP_1433	tcp	1	65535	1433	1433
4	sunzhibin	DB_CON	DB_EPG	APP_PRF	APP_EPG	APP_PRF	UDP_3306	Udp	1	65535	3306	3306
5	sunzhibin	WEB_CON	DB_EPG	APP_PRF	WEB_EPG	APP_PRF	ICMP	icmp	unspecified	unspecified	unspecified	unspecified
6												

	A	B	C	D	E	F	G
1	Tenant	Context	BD	Subnets	Subnets_Scope	AppProfile	EPG
2	sunzhibin	sunzhibin_VRF	APP_BD	192.168.10.254/24	private	APP_PRF	APP_EPG
3	sunzhibin	sunzhibin_VRF	APP_BD	192.168.15.254/24	public	APP_PRF	APP_EPG
4	sunzhibin	sunzhibin_VRF	WEB_BD	192.168.20.254/24	private,shared	APP_PRF	WEB_EPG
5	sunzhibin	sunzhibin_VRF	DB_BD	192.168.30.254/24	private	APP_PRF	DB_EPG
6	sunzhibin	other_VRF	other_BD	10.10.10.254/24	private	other_PRF	other_EPG
7	test	test_vrf	test_bd	1.1.1.1/24	public,shared	test_prf	test_epg
8							
9							

SDN建设的近期成果-TOOLKIT及SDK部署安装

- **完成ACI环境SDN的SDK部署与安装；**
- **完成ACI环境SDN的Toolkit部署；**

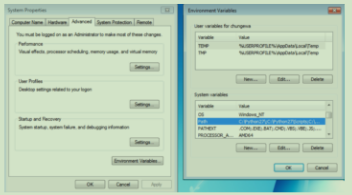
APIC Python SDK – cobra

https://developer.cisco.com/media/apicDcPythonAPI_v0.1/install.html

Python环境

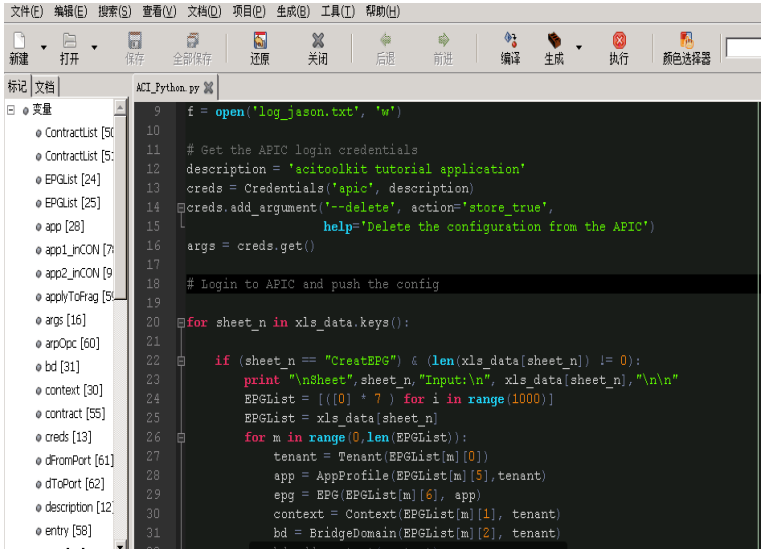
https://developer.cisco.com/media/apicDcPythonAPI_v0.1/install.html

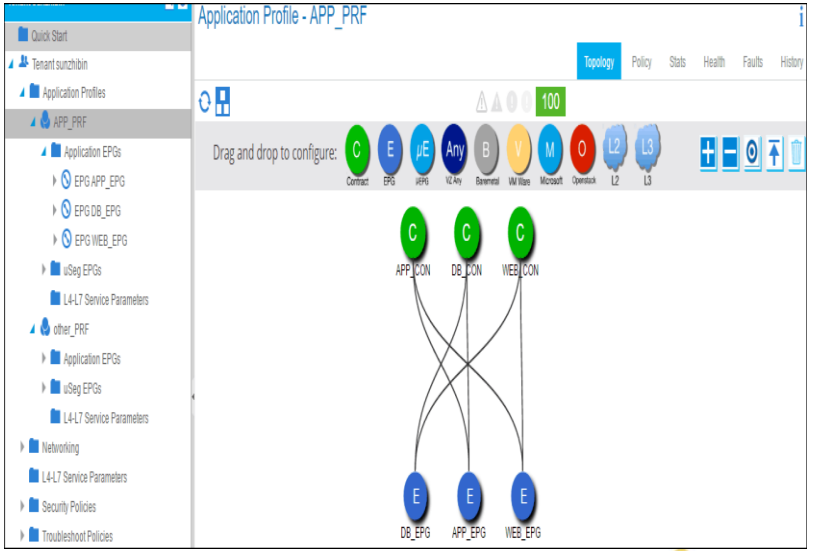
- 目前为止，Python2.7版本依然是ACI编程的不二选择
  - 目前: 不要试图选择高版本 ^-^
  - 确保安装姿势正确!!! ☺ 否则，就没有然后鸟.....
  - Python2.7、 easy_install、 pip是必备安装包；没有install难度，只有安装过程是否正确
  - Virtualenv用虚拟空间跑不同的APIC SDK版本环境；不是必须
  - Python: https://www.python.org/
  - Easy_install: https://pypi.python.org/pypi/setuptools
  - PIP: https://pypi.python.org/pypi/pip
  - Virtualenv: https://pypi.python.org/pypi/virtualenv
- *Pyopenssl*
  - SSL support for connecting to the APIC and fabric nodes
  - *不是必须安装工具*
- Python脚本编写工具：
  - 参考：JetBrains PyCharm Community Edition 5.0.3
  - 工具不唯一，各有所爱
- 针对Windows，修改环境变量:
  - 增加 ;C:\Python27;C:\Python27\Scripts (以安装目录为c:\Python27为例)



SDN建设的近期成果- PYTHON SDN程序V1.0编写及配置下

- 调用ACI API接口的Python SDN程序v1.0编写完成；
- 工单的一键实施，配置自动下发及验证完成；

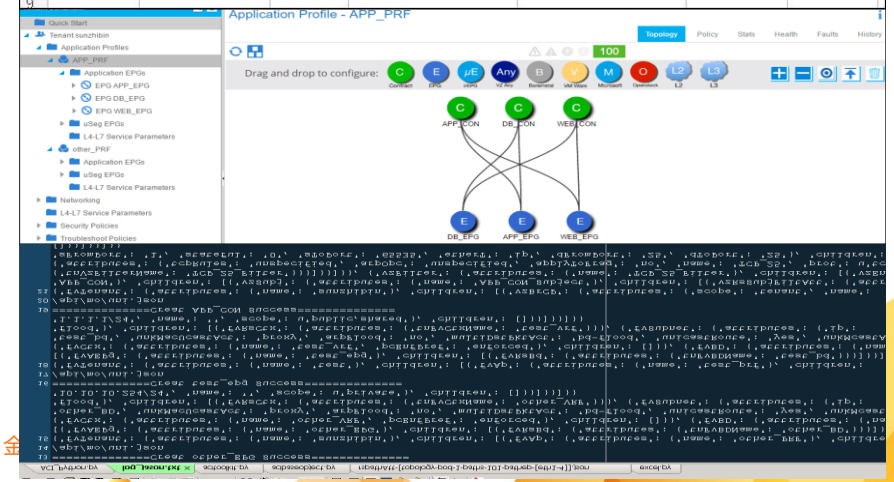




SDN的价值-提升运维效率

	现状	未来
运维人员角色	工单实施人员（人工写配置）	工单审核人员（定义好的工单模板格式和内容）
实施人	运维工程师	通过工单模板输入到调用SDN API接口的Python程序
工单时长	2个工作日	瞬间完成配置推送，缩短到分钟级别

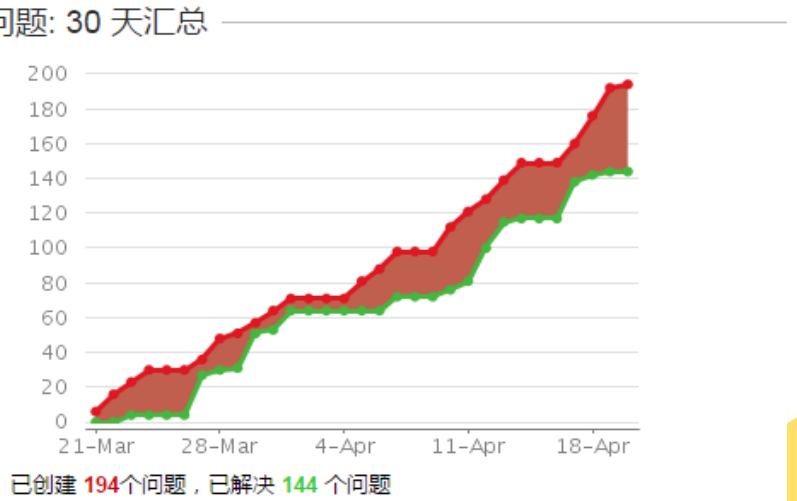
	A	B	C	D	E	F	G
1	Tenant	Context	BD	Subnets	Subnets_Scope	AppProfile	EPG
2	sunzhibin	sunzhibin_VRF	APP_BD	192.168.10.254/24	private	APP_PRF	APP_EPG
3	sunzhibin	sunzhibin_VRF	APP_BD	192.168.15.254/24	public	APP_PRF	APP_EPG
4	sunzhibin	sunzhibin_VRF	WEB_BD	192.168.20.254/24	private, shared	APP_PRF	WEB_EPG
5	sunzhibin	sunzhibin_VRF	DB_BD	192.168.30.254/24	private	APP_PRF	DB_EPG
6	sunzhibin	other_VRF	other_BD	10.10.10.254/24	private	other_PRF	other_EPG
7	test	test_vrf	test_bd	1.1.1.1/24	public, shared	test_prf	test_epg
8							
9							



SDN的价值-降低运维成本

1. 随着公司数据中心不断扩充和工单不断增加（人员未增加），目前面临**人人都需要参与到工单实施**的工作当中。
2. 采用SDN技术后可大大降低运维成本，以工单为例： 目前日均工单10张，每人至少1-2张工单（30日工单量统计）。SDN使用后可单人即可完成日均所有工单审查与复核，可**提升网络运维效率50%。**

NETWORK-365	光大--outerbank准生产机器开通光大银行网络工单	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-364	燃气专线开通南京网络	曾锦华	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-363	征信添加综测白名单	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-362	商户宣城云海-南京网络开通-刘超-	孙志斌	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-361	打通开发环境与外网（支付宝，微信，翼支付个人客户端）的网络	张元辉	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-360	outerbank开通光大专线	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17	
NETWORK-359	办公网访问上海综测，鉴权中心	张怀志	吴佳琦	已解决	验证通过	13/四月/17	17/四月/17	17/四月/17	
NETWORK-357	准生产中间件F5内负载地址申请	薛啸松	陈芳强	已解决	验证通过	13/四月/17	19/四月/17	17/四月/17	
NETWORK-356	通联综测网络开通	薛啸松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17	
NETWORK-355	陕西综测环境网络开通	薛啸松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17	
NETWORK-354	电子货币手机充值业务联调	薛啸松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17	
NETWORK-353	生产中间件F5内负载地址申请	李伊仁	陈芳强	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17	
NETWORK-351	梳理172.17.49.121的专线入向表格	刘涛	张长双	已解决	验证通过	13/四月/17	14/四月/17	17/四月/17	
NETWORK-350	开通商户调用账单应用网络白名单	刘涛	吴佳琦	已解决	验证通过	13/四月/17	17/四月/17	14/四	




DeepFlow
接入网络 / 回溯分析
时间范围： 2018-05-14 10:19 - 2018-05-14 11:19
流量总览
回溯分析
流量特征
会话回溯
服务记录
回溯分析（多维图）是用来检索历史数据，并展示出Flow数据在相邻两个维度的映射关系。 每个维度坐标按照线性排列（如时间）或该维度的TOP排序，您也可以自定义维度展示顺序。
目的IP地址=172.28.49.16
回溯过滤规则，以回车结束
搜索
保存
打开
维度
目前共回溯到 158213 条 Flow 数据， 耗时 12.614 秒
时间
源端口
源IP地址
目的IP地址
状态
目的端口
协议
总包数目
总字节数
连接时间
网络时延
重传比例
tcp-fin
tcp-rst
timeout
half-close
other
1081
0-100
100-200
200-300
300-400
400-500
500-600
600-700
700-800
800-900
900-1000
>=1000
<1秒
<10秒
<30分钟
>=30分钟
<50毫秒
<100毫秒
<150毫秒
<200毫秒
<250毫秒
<300毫秒
<350毫秒
<400毫秒
<450毫秒
<500毫秒
>=500毫秒
5.0-10.0
10.0-15.0
15.0-20.0
20.0-25.0
25.0-30.0
30.0-*

Thank you!

天翼电子商务有限公司

北京：西城区复兴门南大街乙2号天银大厦A东座
上海：虹口区四川北路859号中信广场6F
广州：珠江新城花城大道18号建滔广场20F