

云联壹云 Meetup 10

Part1：新功能介绍

OneCloud核心产品融合云 OneCloud 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

高现起 产品经理

目录

CONTENTS

01 云联壹云产品介绍
Product description

02 v3.4新功能介绍
New features introduction

03 近期功能规划
Product planning

01

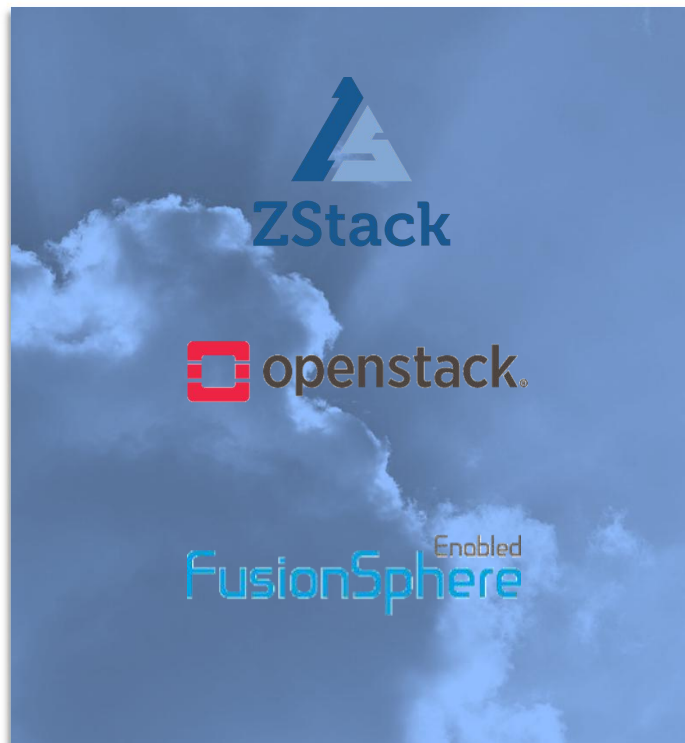
云联壹云产品介绍

企业的IT资源无处不在

据 Flexera 2020云状态报告：93% 的企业实施了多云战略，企业平均使用 7.3 朵云。



Datacenter



Private Cloud



Public Cloud

异构IT基础设施给企业带来了新的挑战

异构IT基础设施在给用户带来更优性能更低成本的同时，也带来了新的问题



IT Admins

如何统一新建和管理所有云计算资源？

如何及时获取所有公有云的账单报表，并且有很好的易读性？



Finance



CTO

如何在保证服务的安全、稳定的前提下，实现成本大幅度降低？



云联壹云是一站式管理云计算资源的解决方案

帮助客户在一个地方管理本地IDC、私有云、公有云等IT资源，整体提高企业IT基础设施的管理效率。



云联壹云平台功能概览

帮助用户在一个地方管理所有云计算资源

OneCloud Cloud Management Platform

统一认证  Microsoft Active Directory  LDAP.com Lightweight Directory Access Protocol  SAML  企业微信  钉钉  飞书

企业应用

 运维工具

统一监控
统一报警
定时任务

 弹性伸缩

告警策略
定时策略
周期策略

 服务编排

虚拟机编排
容器编排
应用市场

 费用管理

账单分析
成本分摊
优化建议

 企业管理

租户管理
权限管理
工单管理

 部署升级

高可用
水平扩展
无缝升级

基础资源管理

计算

网络

块存储

对象存储

数据库

中间件

Kubernetes

 未云化基础设施

 裸机  KVM
 vmware

 私有云

 ZStack  openstack.

 公有云

 阿里云  腾讯云  华为云  天翼云
 UCloud  aws  Azure  Google Cloud

02

v3.4新功能介绍

v3.4主要新功能概览



Web UI界面全面升级



UE交互体验持续迭代



更多多云资源接入



运维工具持续迭代



费用功能丰富



服务编排

UI界面全面升级

给用户提供更好看的页面

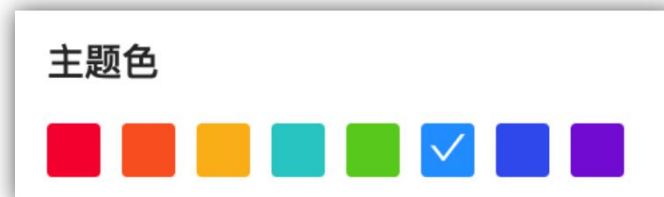
Web控制台支持中英文切换



整体风格设置



8种主题随意切换



系统UI全面升级，清新、简洁、明了、舒服



Next generation unified cloud management platform (CMP)

Simple·Open·Integrated·Smart

Provide one-click deployment and productized solutions for all the needs of enterprises on cloud, cloud use, and multi-cloud management

Select Account

gaoxianqi - Yunion

View: System Manager View

Project: gaoxianqi

 Use another account  Remove Account

Other Login



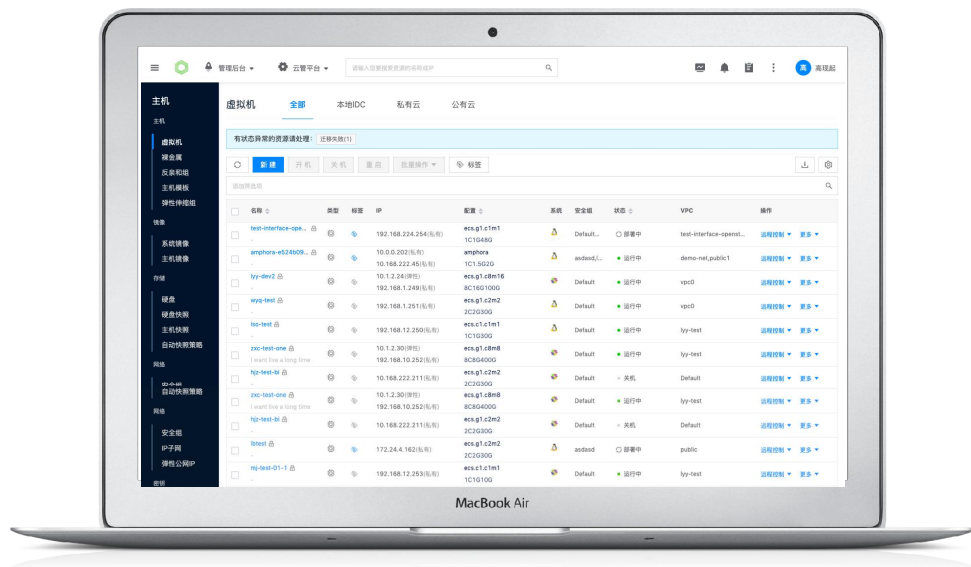
新版监控大屏，实用且科技范十足



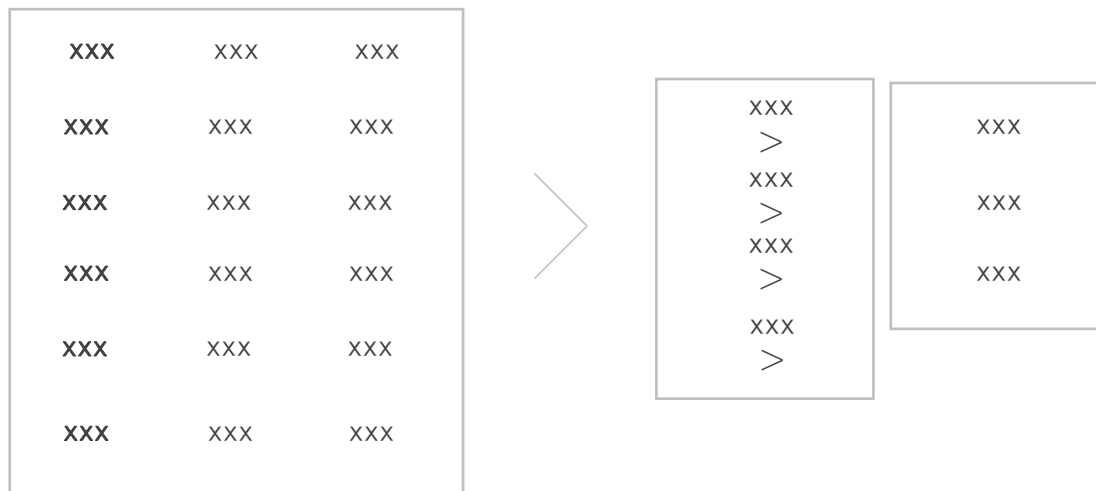
UE交互体验持续迭代

给用户提供更好用的功能

列表默认显示部分字段，兼顾小屏用户操作体验



操作交互先分组再执行目标操作



级联下拉框增加说明

下拉菜单支持加载更多

域: Default

▼

项目: gaoxianqi

▼

区域: Beijing

▼

可用区: YunionHQ

▼

▼

xxx

xxx

...

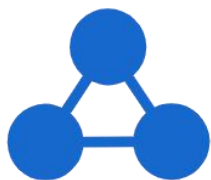
xxx

加载更多

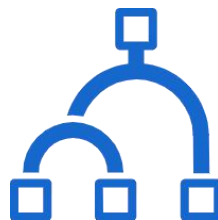
更多多云资源接入

帮助用户统一管理更多的资源

OpenStack 负载均衡对接



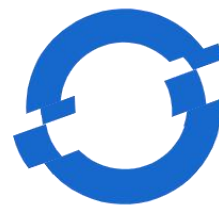
OpenStack 虚拟路由表对接



腾讯云域名服务DNS对接

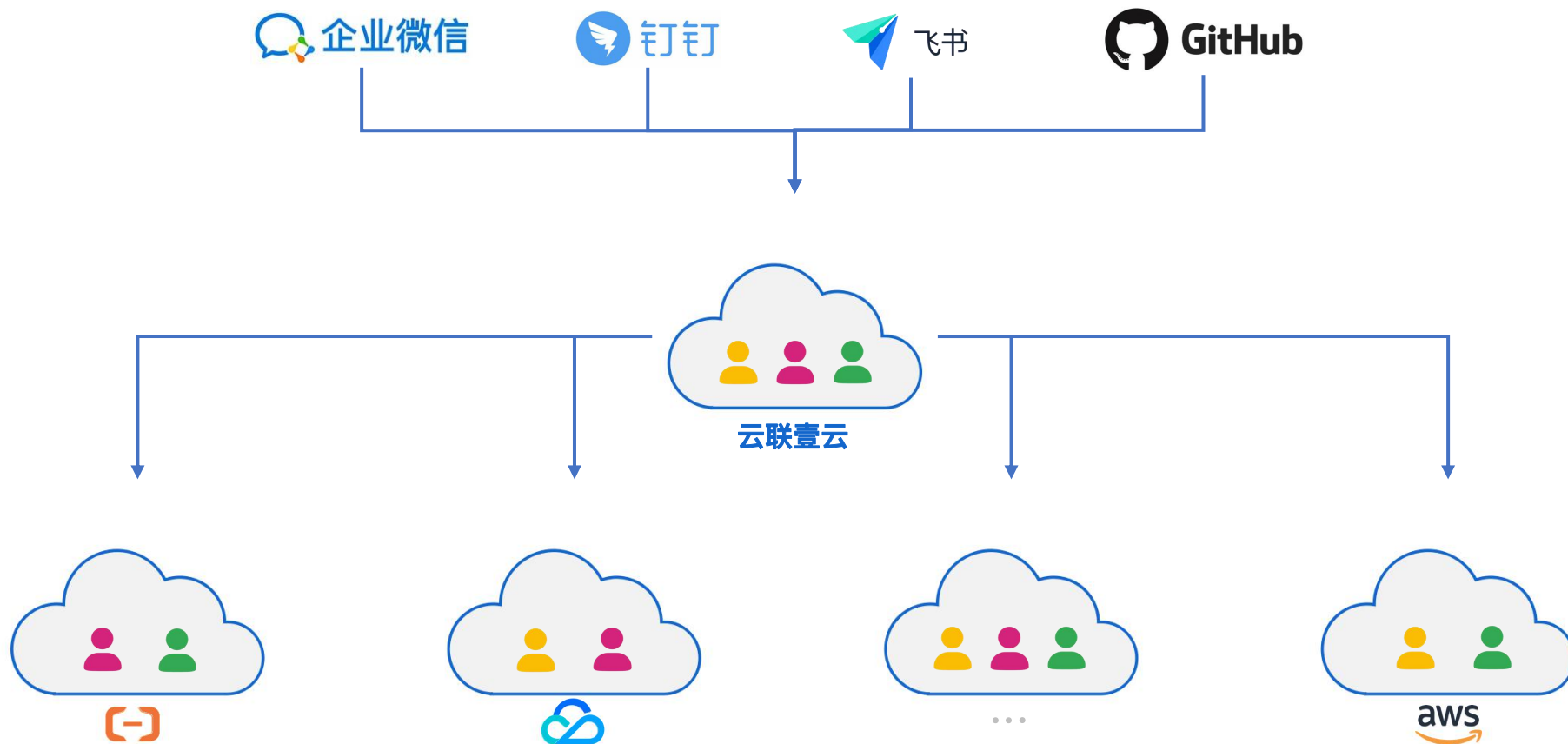


AWS域名服务DNS对接



OpenShift 容器集群对接

在一个地方新建和管理所有公有云的子账号及权限



运维工具持续迭代

给用户更多的一致性运维体验

- ◆ 统一监控
- ◆ 统一报警
- ◆ 通知渠道支持企业微信

通知渠道：



系统



邮件



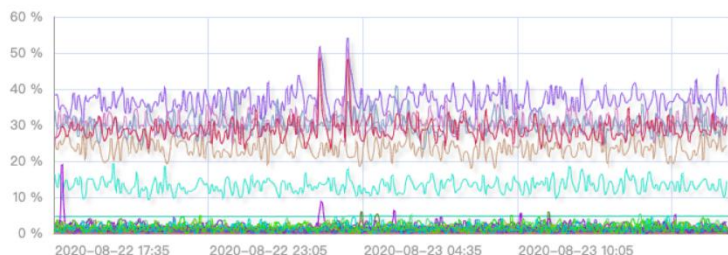
钉钉



飞书



微信



	名称	IP	宿主机	宿主机IP	平台
●	lxj-test	10.168.222.169	office-04-host02	192.168.222.4	🔗
●	dlptest	10.168.222.180	office-04-host02	192.168.222.4	🔗
●	wyq-rook-cluster-node-cliff-1	10.168.222.153	office-04-host02	192.168.222.4	🔗
●	zxc-server-java	10.168.222.237	office-04-host02	192.168.222.4	🔗

共 45 条记录



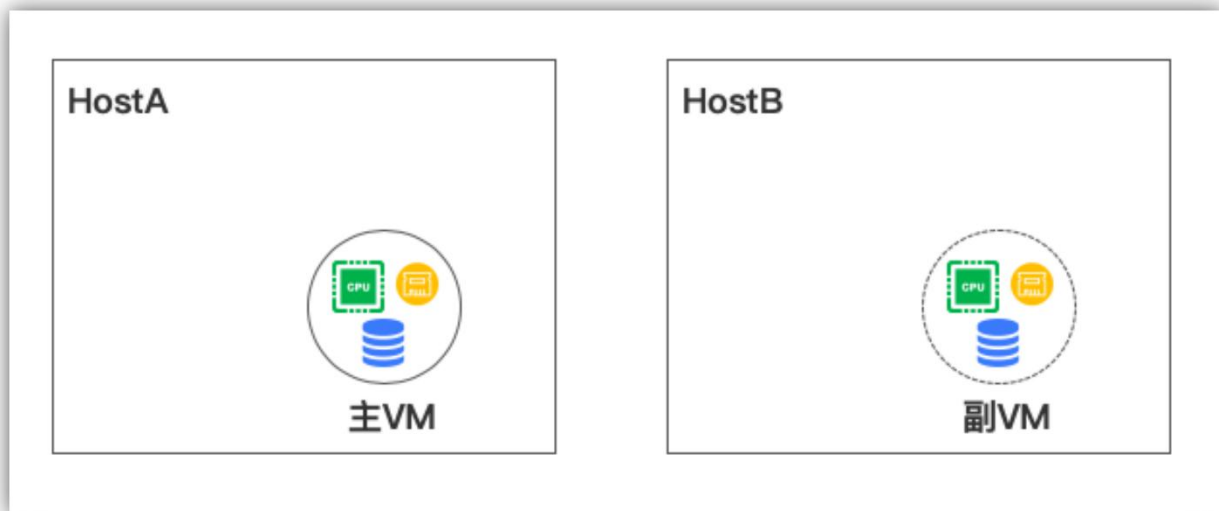
	名称	IP	宿主机	宿主机IP	平台
●	wyq-nfs-allinone	10.168.222.137	office-99-host03	192.168.222.99	-

共 1 条记录

费用功能丰富

为用户算好每一笔账

主备机费用翻倍



调整配置增加费用预估

费用估算: **¥ 0.20/ 时**
(合¥4.80/天 ¥144.00/月)

确定

服务编排

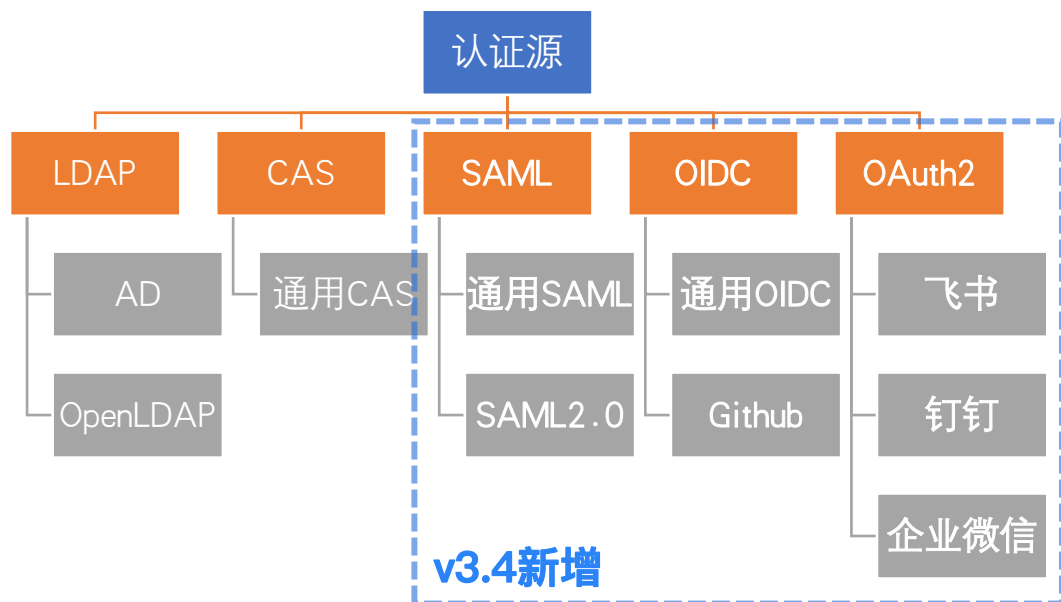
基础设施即代码，快速交付服务



其他

国产化支持、更多认证源支持

更多认证协议支持



私有云支持ARM架构服务



v3.4主要新功能概览



Web UI界面全面升级



UE交互体验持续迭代



更多多云资源接入



运维工具持续迭代



费用功能丰富



服务编排

v3.4新增功能总览（30+）

UI/UE

中英文切换
登录页风格
主题注入
监控大屏
小屏适应
操作显示优化
新建页面样式优化
级联下拉框增加提示
下拉列表支持加载更多

安装部署

负载均衡Agent的部署自动化
新手引导
K8s 共享存储longhorn部署
设置 高可用架构的时间同步

多云管理

OpenStack LBaaS对接
OpenStack 虚拟路表对接
AWS 域名服务对接
腾讯云 域名服务对接
VPC对等连接
AWS VPC 连接

主机

物理机（裸金属）检测GPU
主机套餐和存储类型联动
调度结果优化
宿主机服务启动失败信息展示
快速过滤异常虚拟机
支持ARM虚拟化

系统配置

SAML认证源
OpenID认证源
OAuth2.0认证源
OpenID Connect认证提供者
通知渠道支持企业微信
服务ITSM支持SSL
信息中心和统一方式的接口
发现各个服务 watch endpoint 变化，然后自动 reload auth 信息
指定监听资源类型
发现policy变化，及时加载policy
发现service config变化，及时加载service config
IP子网增加自动分配字段

容器管理

多集群资源管理
服务组件支持查看部署日志
支持通过jsonschema方式创建虚拟机实例

计费管理

ELB 带宽计费
主备机费用double
调整配置增加预估费用

运维工具

系统报警
统一监控
统一报警
服务编排

功能丰富 X 易用性

03

近期功能规划

近期的功能规划



支持在 aliyun 虚拟机
部署K8S



运维工具



公有云子账号SSO



更多多云资源接入

云联壹云 Meetup 10

Part2: 私有云VPC的设计与实现

OneCloud核心产品融合云 OneCloud 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高

运维效率的同时，降低企业运营成本。

周有松 网络开发工程师 2020-08-

26

目录

CONTENTS

- 01 VPC功能概要介绍
- 02 壹云VPC功能演进
- 03 壹云VPC实施细节
- 04 规划和展望

01

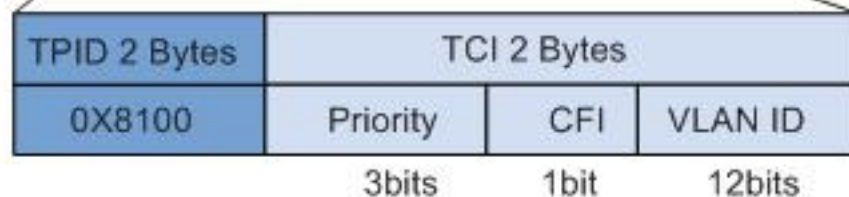
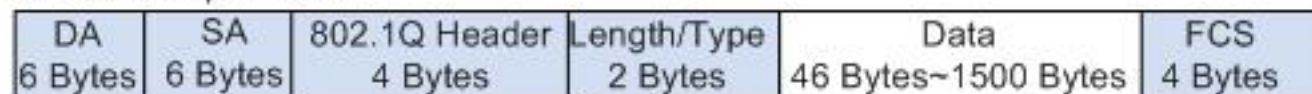
VPC功能概要介绍

- 解决什么问题
- VPC的功能和内容
- OVS与OVN

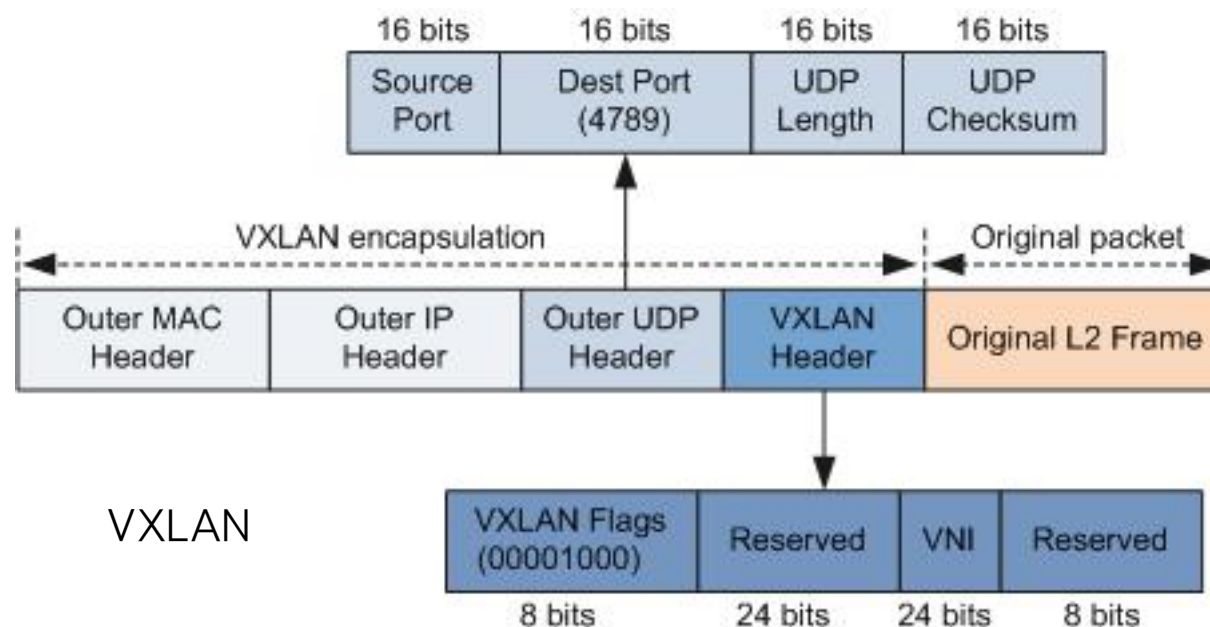
VPC解决的问题

- 链路复用: Multiplexing
- VLAN
 - 局域网
 - 约 2^{12} , 2093
- VPC
 - 跨机房、跨地域
 - 租户概念: 时效、管理
 - VXLAN为例, 2^{24}

802.1 Q Encapsulation



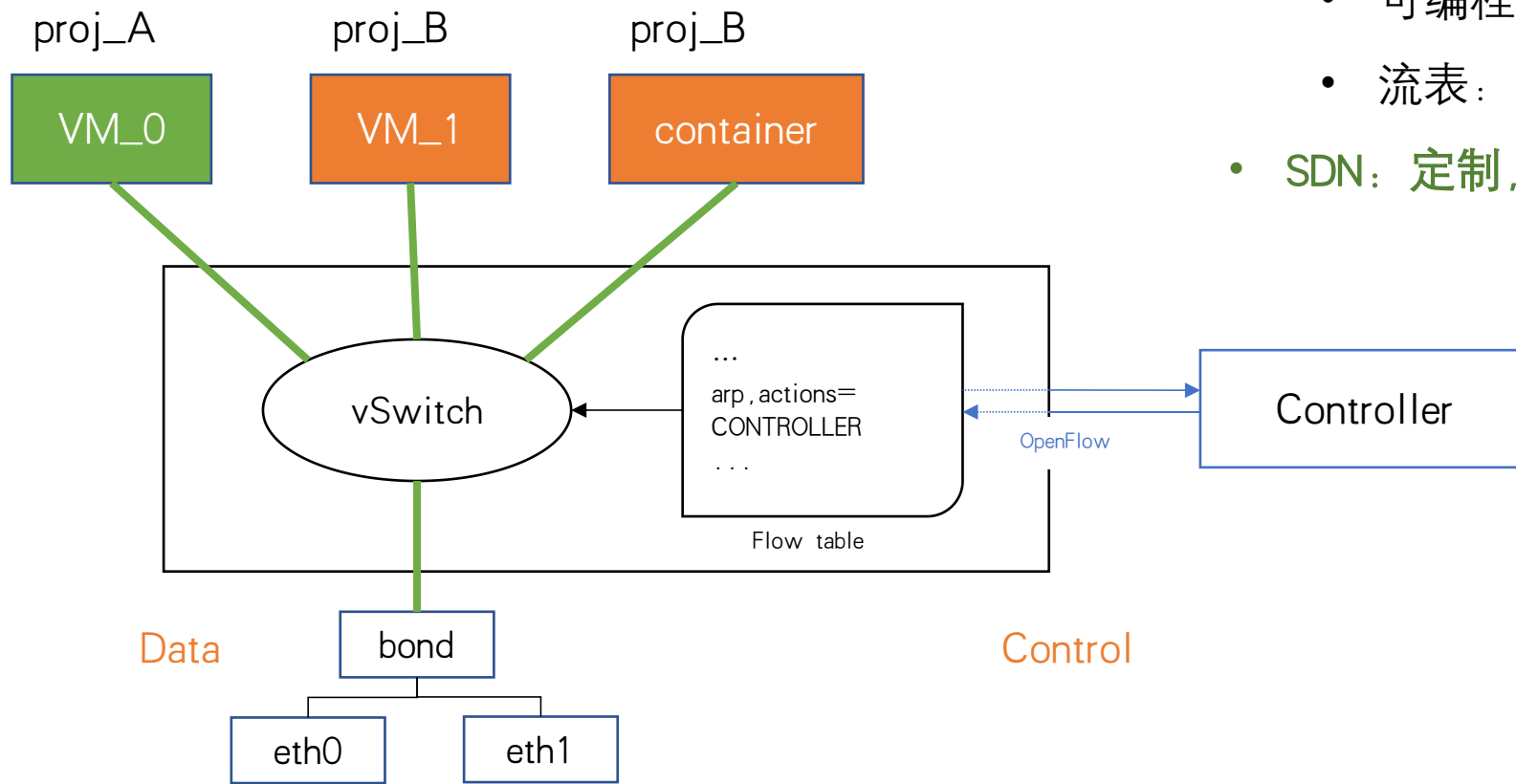
VLAN



VPC的功能和内容

- 功能层面
 - VLAN：二层隔离
 - VPC：包含地址分配，路由管理，防火墙等功能
- 产品化
 - VPC内不同子网通信
 - VPC访问外部网络
 - 向外提供服务：外部网络访问VPC
- 与平台其它产品整合
 - 负载均衡
 - DNS
 - 监控采集与告警
 - 自动发布与部署

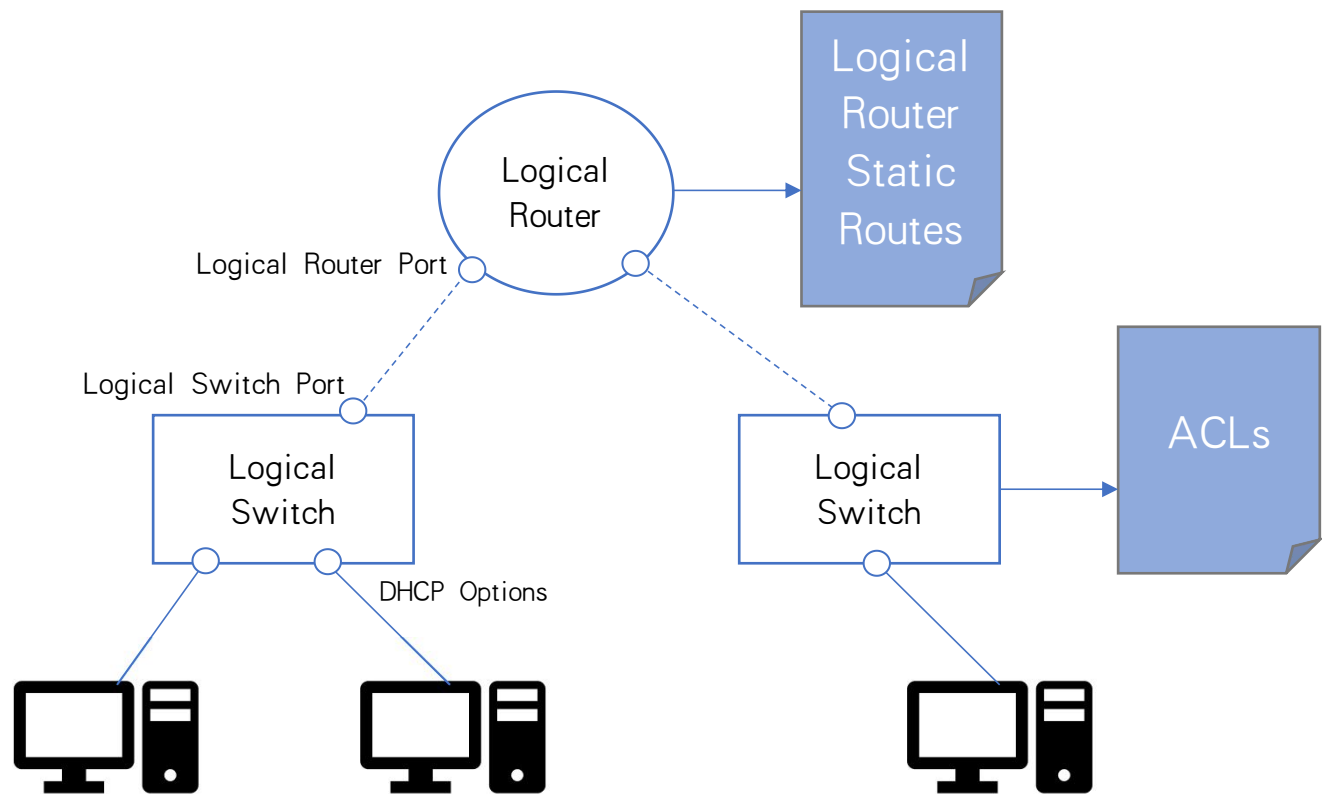
公共组件：OVS与OVN



- Open vSwitch
 - 可编程的控制面
 - 流表: 〈match, action〉
- SDN: 定制, 定义

公共组件： OVS与OVN （续）

- Open Virtual Network
- 以OVS为基础，实现虚拟的网络功能
 - Logical Switch
 - Logical Router
 - DHCP
 - ACL
 - ...
- 云管SDN组网



02

壹云VPC功能演进

- 模型介绍
- 分布式外网访问
- 弹性IP

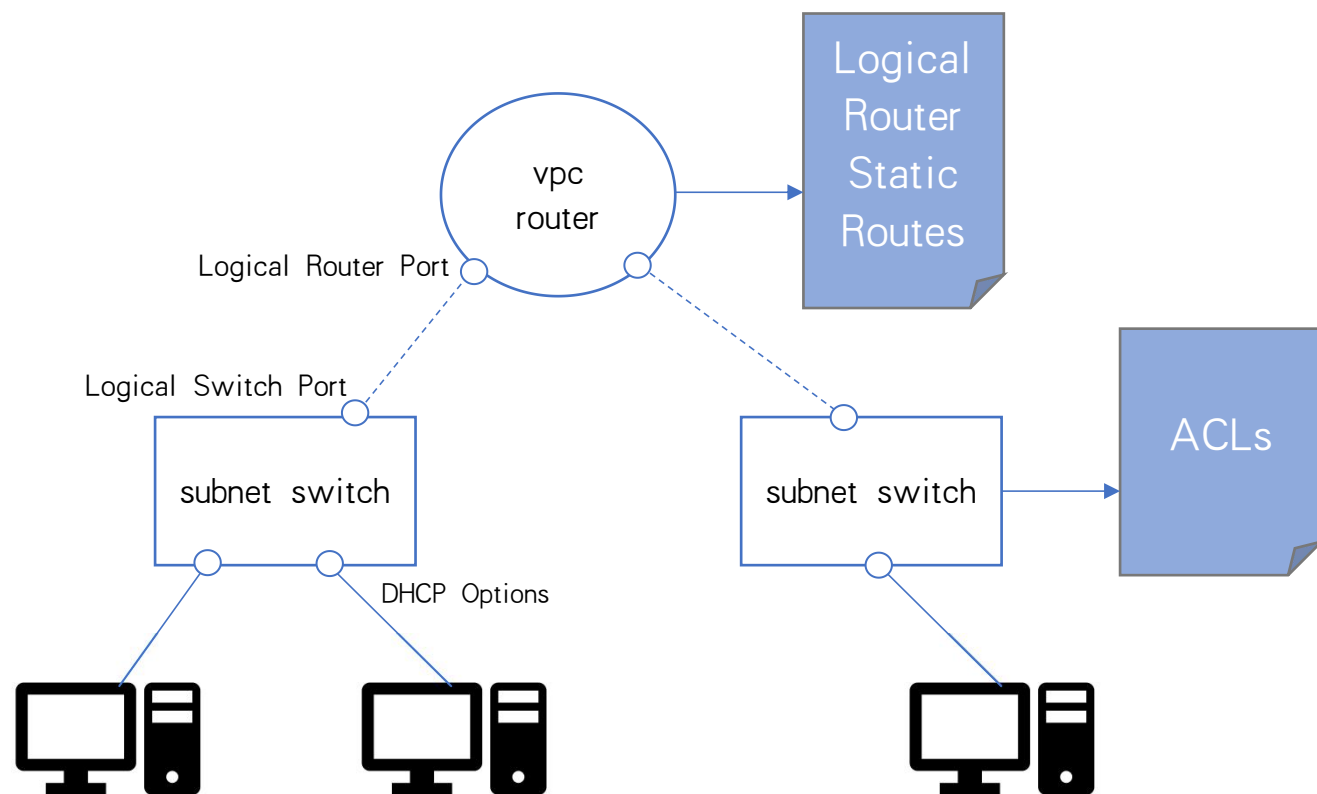
壹云VPC的功能演进

- 3.1
 - VPC功能上线
- 3.2
 - 分布式网关，允许VPC内虚拟机访问传统网络
- 3.3
 - EIP功能上线，EIP地址管理、网关、限速
 - DNS
 - 安全组
 - VPC虚拟机网卡限速

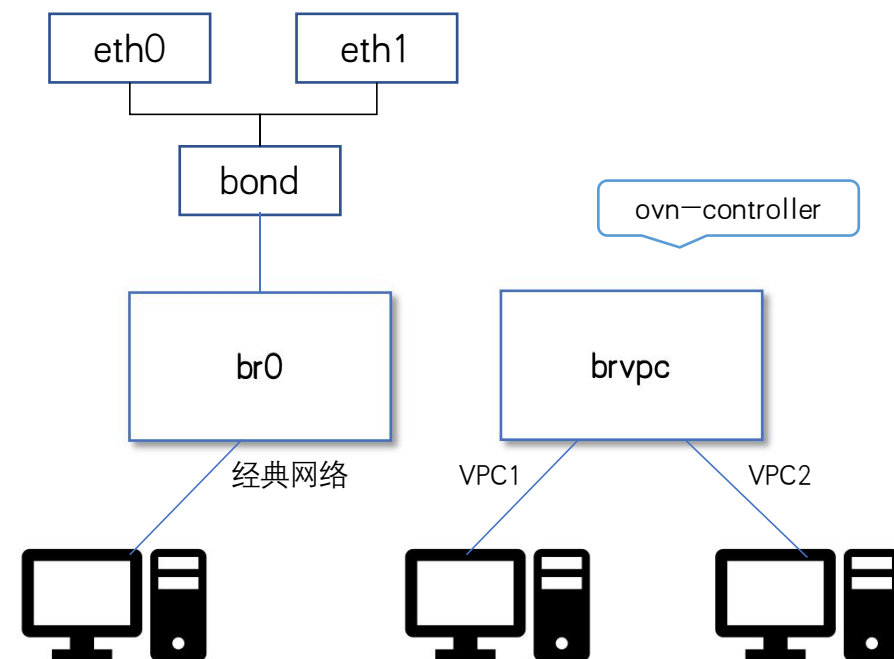
壹云VPC的功能模型 — 3.1

- VPC可使用3个私有段
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/24
- VPC子网
 - 预留第1个地址：网关
 - 预留最后1个地址：广播地址
 - 预留倒数第2个地址：保留
- 经典网络作为一个特殊VPC存在
- 虚机、子网间的API未改变
 - 允许同一虚机同时绑定经典网络子网、VPC子网
 - 允许同一虚机同时绑定不同VPC子网

壹云VPC的功能模型 — 3.1 (续)



OVN逻辑模型

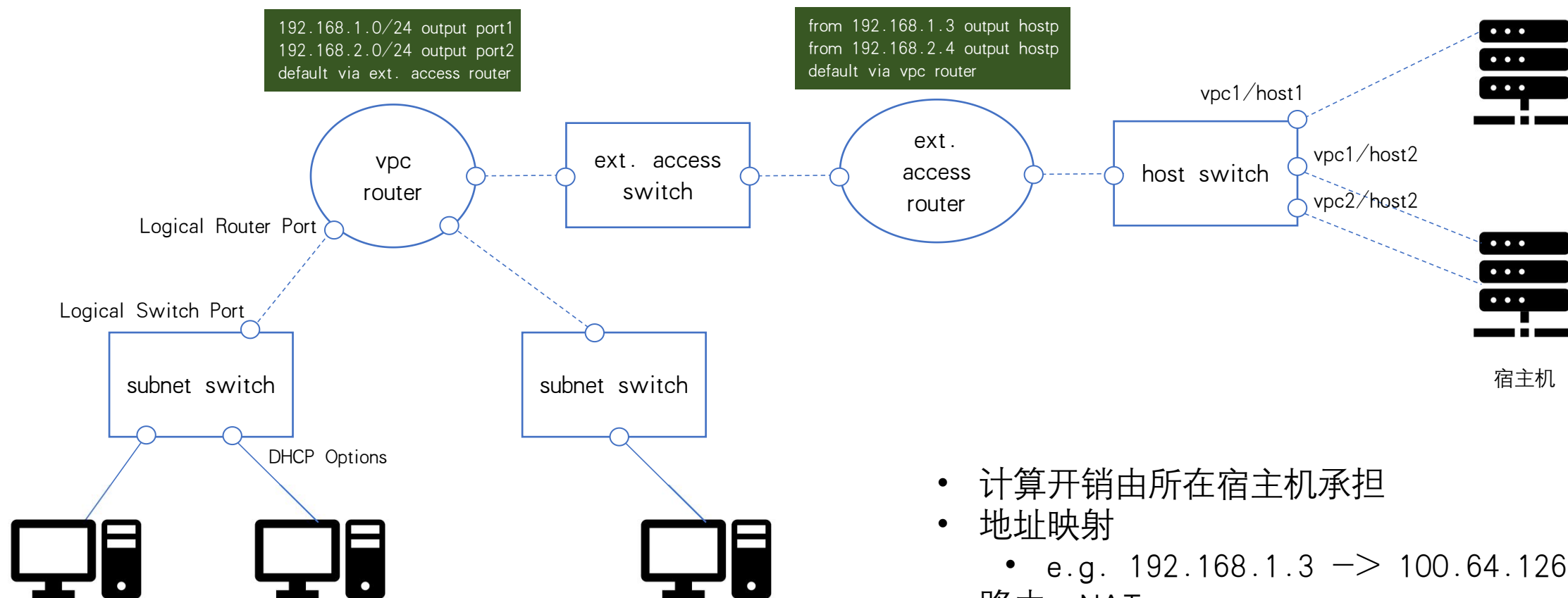


计算节点网络设备

访问外部网络 — 3.2

- 如果网络与外界不通，VPC是一座孤岛
- 3.1版本如何实现VPC与外部通信?
 - 创建一台虚机vm0
 - vm0连接经典网络
 - vm0连接VPC网络
 - vm0配置路由转发
 - VPC中其它虚机将路由指向vm0
- 3.2实现分布式网关
 - 开箱即用
 - 水平扩展
 - 无单点故障
- 不同VPC内IP地址可重复
 - 在外部网络需要唯一的身份
- 映射段100.64.0.0/17
 - 为宿主机预留约2000个
 - 为VPC IP预留约30000个

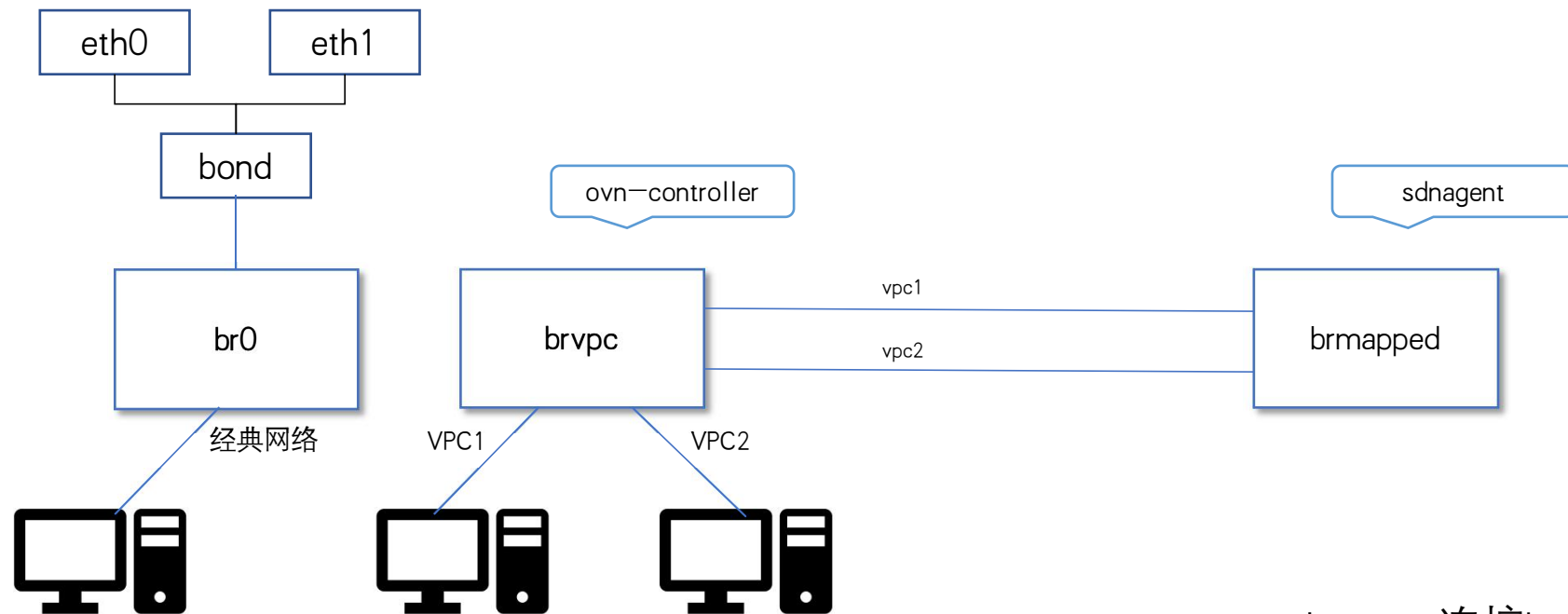
访问外部网络 — 3.2 (续)



OVN逻辑模型

- 计算开销由所在宿主机承担
- 地址映射
 - e.g. 192.168.1.3 → 100.64.126.254
- 路由、NAT
- 允许从宿主机直达VPC中虚机

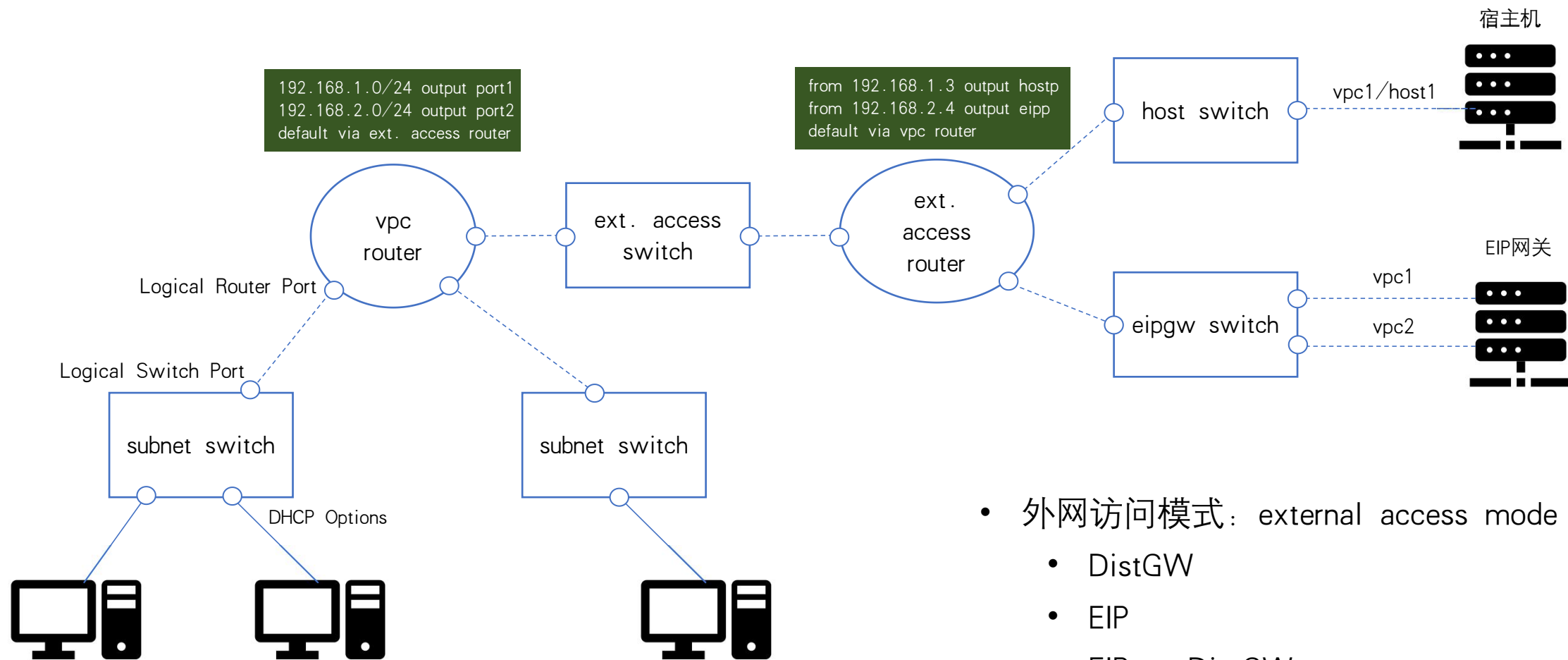
访问外部网络 — 3.2 (续)



计算节点网络设备

- patch ports连接brvpc、brmapped
- sdnagent组件管理brmapped网桥
 - ARP应答
 - 地址转换
 - NAT配置下发

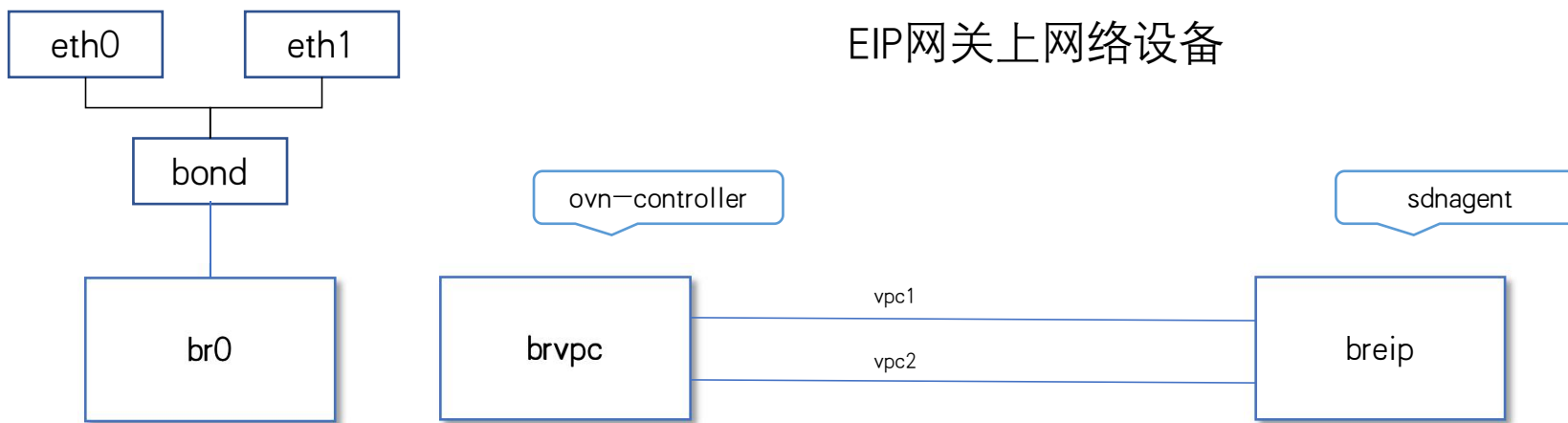
壹云VPC与弹性IP — 3.3



OVN逻辑模型

- 外网访问模式: external access mode
 - DistGW
 - EIP
 - EIP or DistGW
- VPC间共享EIP网关集群

壹云VPC与弹性IP — 3.3 (续)



- `brvpc`与计算节点建立隧道
- `patch ports`连接`brvpc`、`breip`
- `sdnagent`管理`breip`
 - VPC IP与EIP映射
 - 路由
 - ARP应答管理
- 部署灵活
 - 可与分布式网关同时存在
 - 可与计算节点分离部署在不同级别安全区域
- 高可用
 - 主备高可用
 - 无状态切换

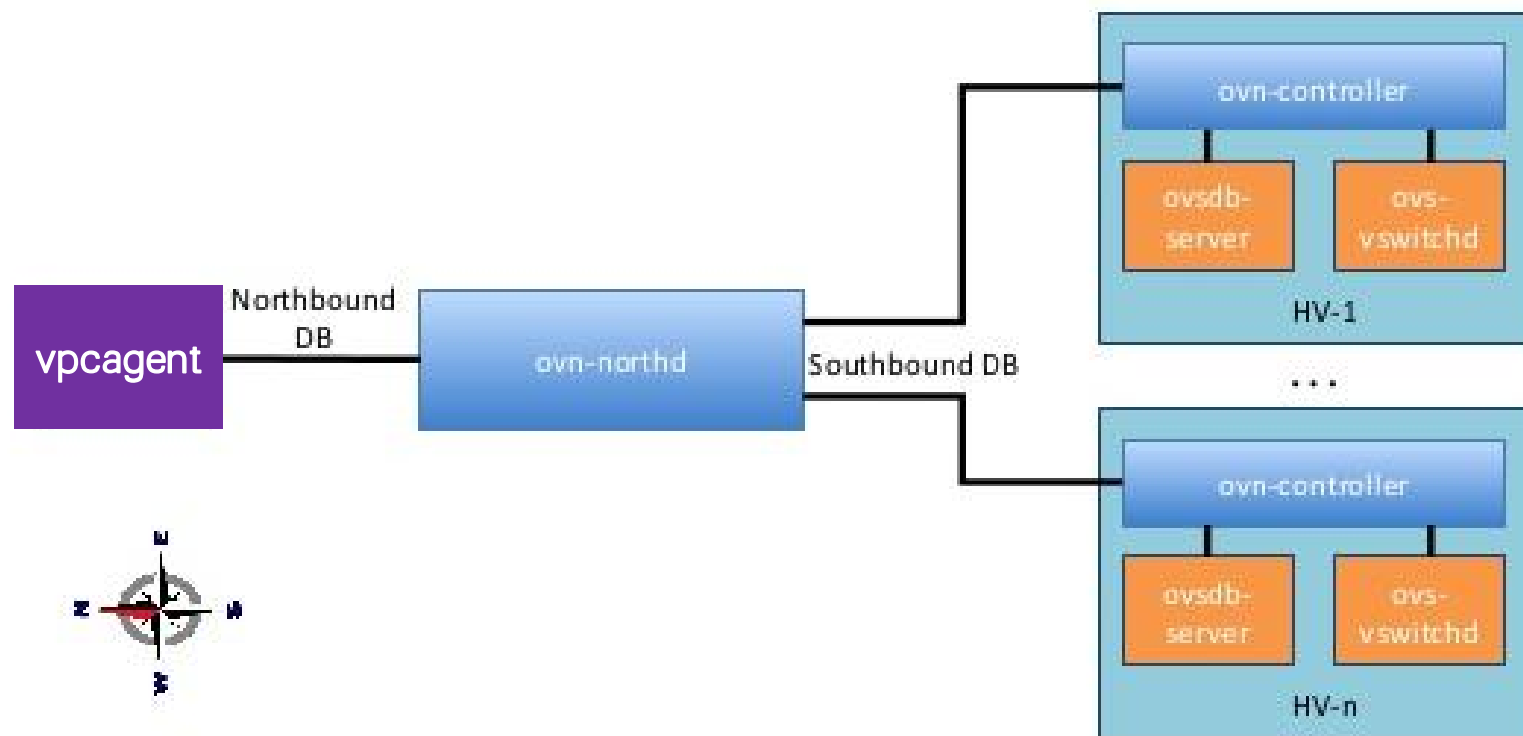
03

壹云VPC实施细节

- 架构和组件
- 高可用、可扩展性
- 链路MTU

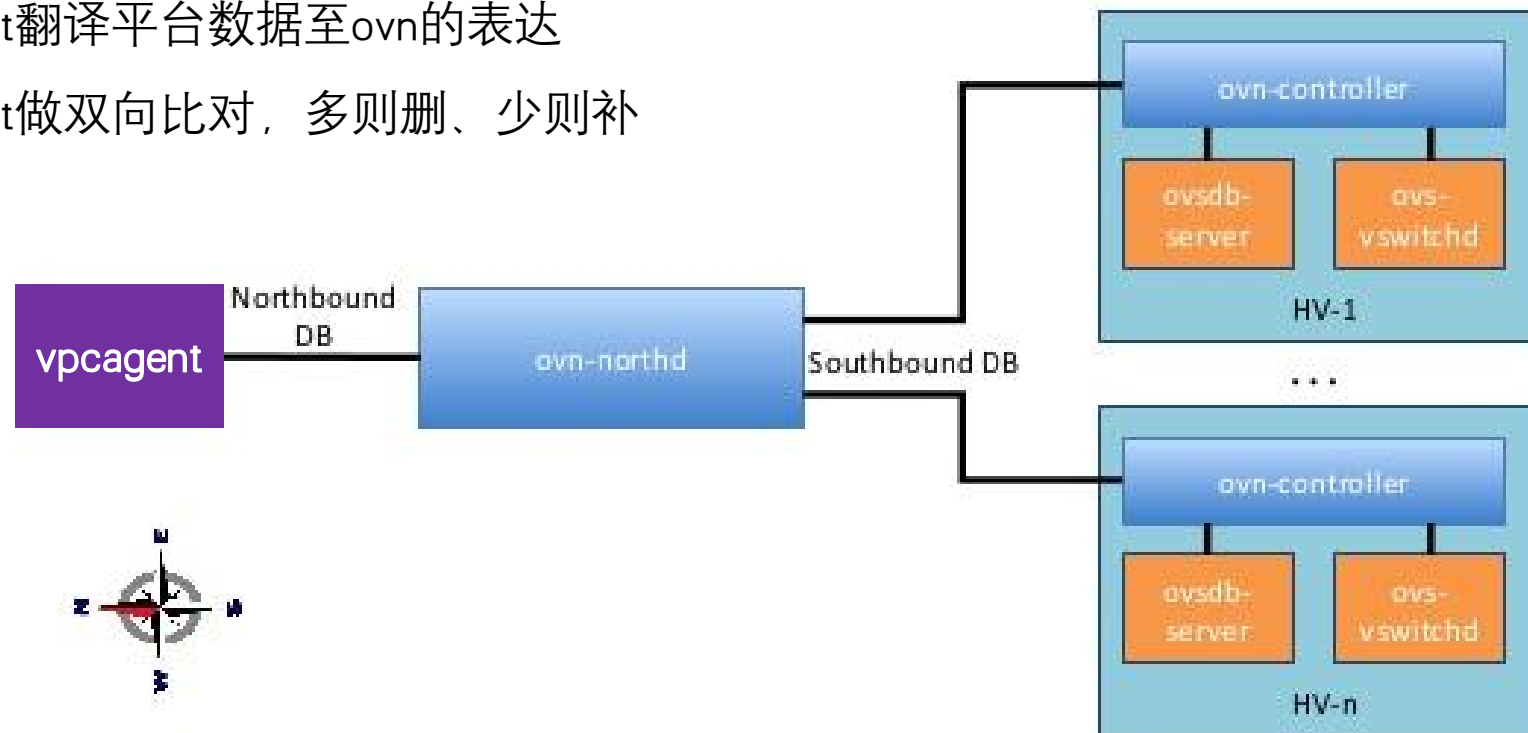
壹云VPC相关的架构和组件

- 1个cms插件
 - Vpcagent
- 2个ovsdb数据库
 - northbound db
 - southbound db
- 1+n个进程
 - ovn-northd
 - ovn-controller
- n个sdnagent
 - 分布式网关
 - eip网关集群
- 数据中心内：Geneve



壹云VPC组件间访问关系

- vpcagent需要访问north-ovsdb
- 宿主机需要访问south-ovsdb
- 2个ovsdb是平台数据的衍生物
 - Vpcagent翻译平台数据至ovn的表达
 - Vpcagent做双向比对，多则删、少则补



壹云VPC — 高可用和扩展性

- 相关组件已容器化至k8s
 - vpcagent
 - ovn northd, 2 ovsdb
 - 宿主机sdnagent
- ovn组件离线不影响存量网络
- vpcagent管理、重建ovn拓扑
- 隧道协议：Geneve
 - UDP，目标端口6081
 - OVN开销58字节，对应虚拟机网卡MTU 1442
- OVN原生分布式结构
 - Logical Switch
 - Logical Router
- 分布式网关提供默认的外部访问能力
- 主备高可用的EIP网关集群
 - 无状态切换
 - 可实现水平扩展

04

规划和展望

规划和展望

- 单网卡多IP，支持容器使用VPC网络
- VPC网络中虚机作为负载均衡服务后端
- 开放路由规则配置
- VPC对等连接
- OVS性能
 - xdp
 - dpdk

- 开源
 - yunionio/onecloud
 - yunionio/sdnagent



2020 THANK YOU

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

高现起 & 周有松 2020-08-26



扫码进技术交流群



更多资讯关注我