APSARA 云栖大会

深度用云 网络先行
云网络卓越架构设计

常 磊

阿里云智能集团资深产品解决方案架构师

2024/09/19

为什么网络需要卓越架构

总结深度用云中遇到的问题，沉淀出优秀的架构

忽视网络规划和设计，为业务的长期发展埋下隐患

应用未实现跨可用区容灾

客户1：直播回源业务单可用区部署，花费3周时间做多可用区容灾改造

服务之间无法有效隔离

客户2：业务部署在单VPC，隔离通过ECS安全组(规则上千条)，运维复杂度非常高

IP地址冲突，无法互相通信

客户3：IP地址冲突无法构建全球一张网，5次停机割接才完成改造

专线主备不生效

客户4：专线主备配置不生效，导致主线中断后，业务中断

疯狂点控制台批量交付

客户5：业务要求单ECS绑定300EIP，控制台操作数小时

稳定	设计网络容灾，构建高可靠架构
安全	正确使用VPC，构建安全隔离的网络
性能	构建弹性网络保障业务可持续扩展
可观测	巡检架构缺陷并告警持续优化网络架构
自服务	提供自动化交付能力实现高效交付

深度用云，网络先行，构建卓越的网络架构

云网络卓越架构五大支柱

The Five Pillars of the Well-Architected Framework

稳定 Reliability

多机房容灾	**同地域多可用区部署设计**
	跨地域容灾网络设计
	NAT网关多可用区容灾设计
	TR多可用区部署设计
多线路容灾	多专线多点接入高可用
	专线与VPN容灾设计
	冗灾快速倒换

安全 Security

安全隔离	安全组
	网络ACL
	TR路由策略
	TR多路由表
流量安全	**东西向流量安全**
	南北向流量安全
	混合云流量安全

性能 Elasticity Performance

弹性设计	ALB/NLB替换CLB提升弹性能力
QoS设计	跨地域QoS设计
	专线接入QoS设计
时延设计	**公网最短时延设计**
	跨地域最短时延设计
	专线上云最短时延设计
带宽管理	公网带宽选型

可观测 Deep Observability

流量观测	公网流量分析与监测
	VPC间流量分析与监测
	混合云流量分析与监测
	跨地域流量分析与监测
运维监测	**网络巡检**
	告警感知

自服务 Efficient Automation

自动化	**通过IaC自动化部署**
	结合FC自动化运维

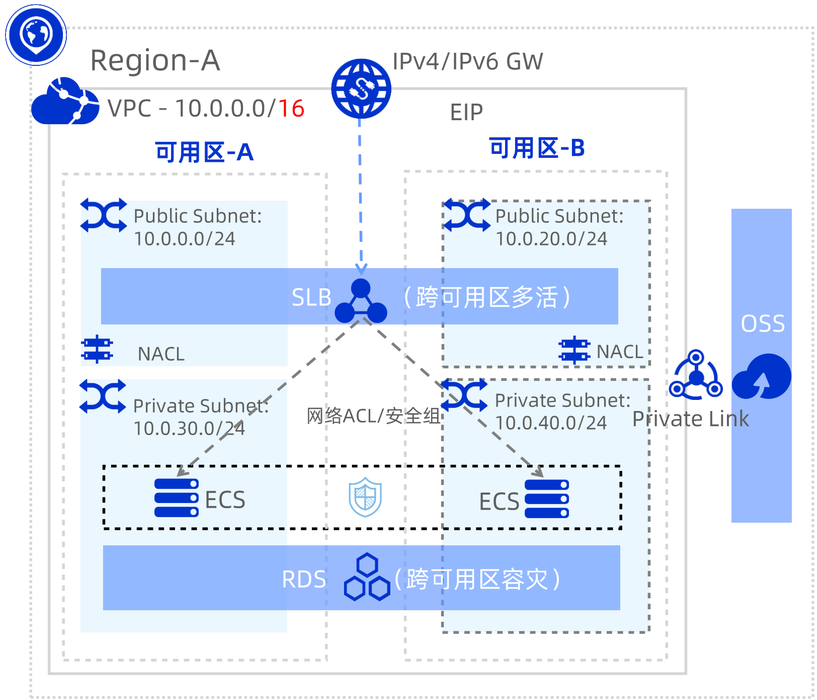
稳定 - 同地域多可用区部署设计

单地域多可用区部署+SLB多活架构，快速构建同城双活网络

业务场景

- **应用双活/灾备：**业务系统多可用区(AZ，Available Zone)部署，避免单可用区内网络故障，提升系统服务连续性
- **业务入口灾备：**业务入口的负载均衡需要支持同城灾备，避免单机房网络故障

方案设计



- ✓ **IP地址规划：**考虑到未来扩展，选择一个足够大的CIDR，为未来业务发展预留足够的空间，推荐使用/16掩码，同时要避免跟现有网络地址冲突
- ✓ **多可用区规划：**考虑到容灾诉求，至少需要双可用区规划vSwitch部署ECS
- ✓ **负载均衡规划：**利用SLB产品多活能力，加载不同可用区的ECS构建应用池，解决应用单节点问题

携程旅行 业务多可用区部署，通过NLB挂载多可用区ECS，轻松实现同城双活架构

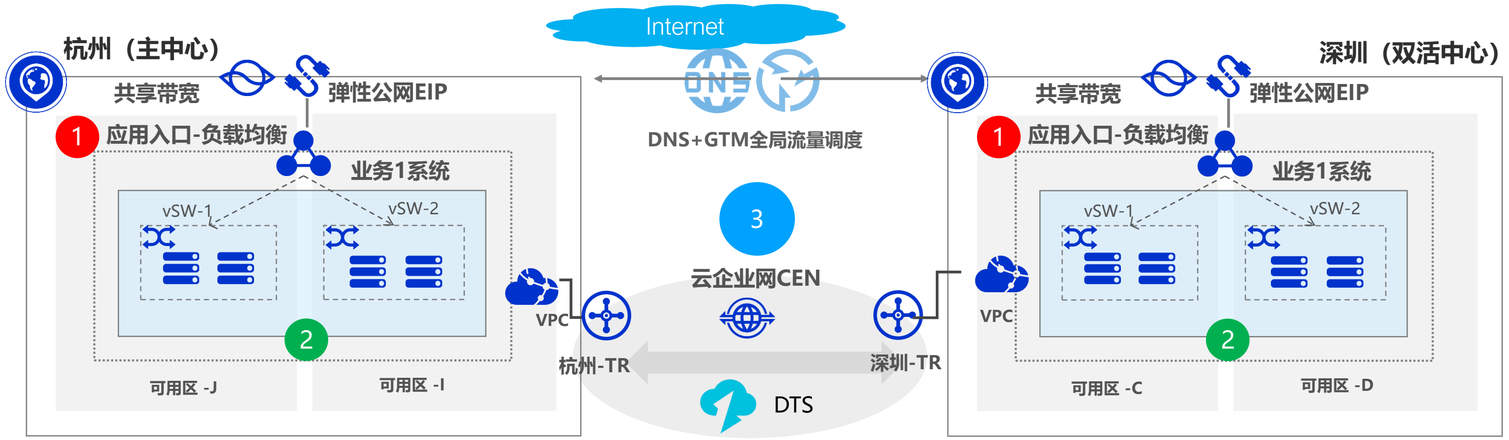
稳定 - 跨地域容灾网络设计

全局流量管理GTM+DNS，实现业务跨地域灾备多活，提升服务连续性

业务场景

- **应用多活/灾备：**业务多地域部署，避免单地域网络故障，提升服务连续性
- **访问优化：**业务多地域就近部署，提升用户访问体验

方案设计



- **多中心部署：**业务同城双可用区部署，跨地域容灾多活部署
- **数据双向实时同步：**CEN和TR构建全局一张网，支持DTS跨地域数据同步
- **服务可用性实时探测：**GTM健康检测探测服务可用性，服务一旦不可用快速切换至双活节点，实现两地三中心应用级容灾

国泰产险 Cathay Insurance

基于GTM和DNS构建了应用的访问入口异地灾备多活，基于CEN和TR实现了跨地域内网数据的实时同步，大幅提升了业务的连续性

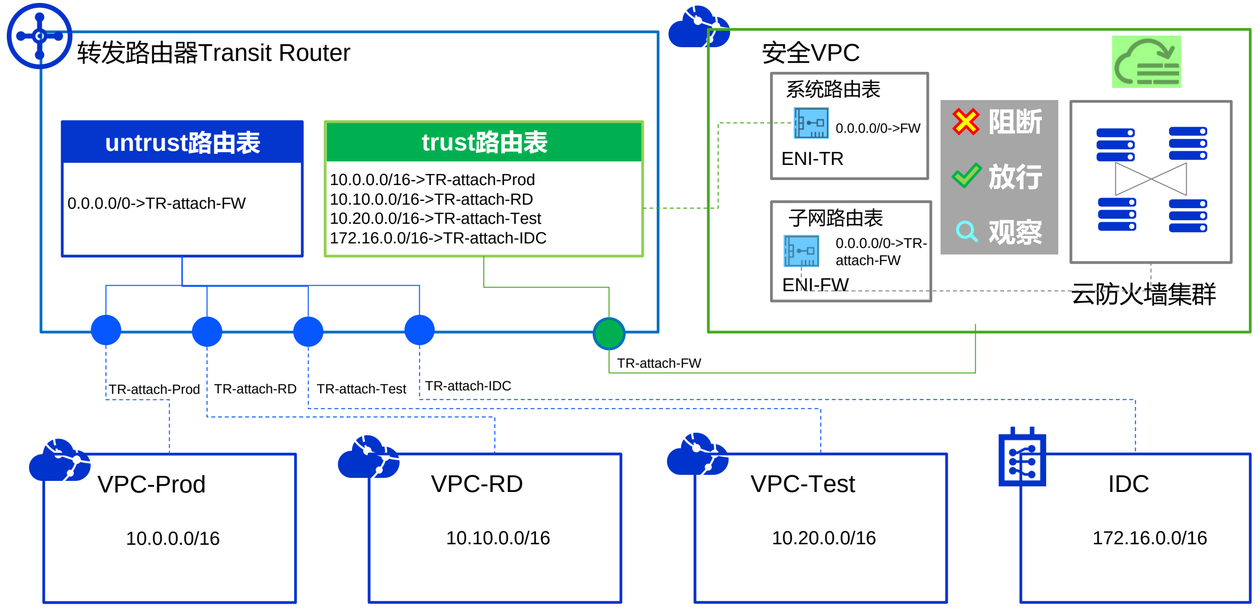
安全 - 东西向流量安全设计

使用TR转发路由器多路由表能力+云防火墙，构建企业内网的安全服务链

业务场景

- **内网安全威胁防控：**内网间通信流量较大，一旦攻击者突破Internet边界防御后，对内网安全造成较大安全威胁
- **内部安全管控要求：**企业内的部分重要业务数据相对敏感，不可随意访问，需增加不同层级的安全访问控制
- **审计、回溯：**企业需要针对网络安全进行定期的审计、回溯，满足网络安全自查及合规的要求。

方案设计



- ✓ **多平面的安全隔离：**安全VPC绑定TR的Trust路由表，业务VPC绑定TR的Untrust路由表，通过该路由表引流至安全VPC；待云防火墙进行检测和观察后，放通可信的访问流量，实现内网东西向安全隔离；
- ✓ **全流量可视：**TR和VPC均可通过Flowlog将业务流量以流日志形式进行记录输出，结合云防火墙实现定期流量审计、回溯

太古可口可乐

基于TR多路由表建立Trust和Untrust等路由表，隔离企业内网东西向访问流量，并通过云防火墙进行异常检测、阻断、观察及放行，来实现企业东西向流量的安全防护

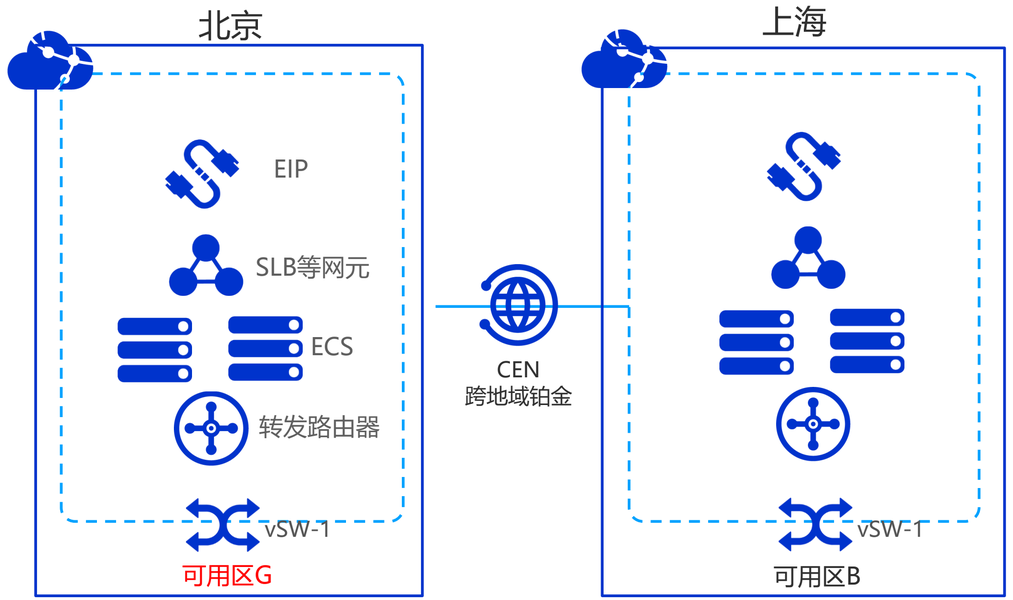
性能 - 最短路径低时延设计

将云上资源按可用区对齐，设计端到端最短时延方案

业务场景

- **游戏行业：**时延敏感类游戏，需要低延迟的公网网络和跨地域网络，保证玩家最好的体验
- **金融交易类行业：**时延敏感类金融交易行业，需要极低时延、稳定的公网与跨地域网络，保障交易顺畅
- 其他**对延迟要求极致**的业务场景

方案设计



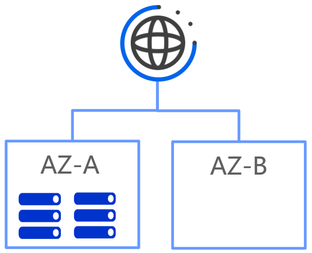
- ✓ **低时延公网：**将EIP、共享带宽、网元SLB和ECS同一可用区部署，避免可用区之间绕行，保证公网接入的最低时延
- ✓ **低时延跨地域网络：**SRTE能力保障铂金带宽跨地域走最短路径，时延稳定可控

区域化部署，同可用区内EIP、ECS等资源对齐，CEN铂金带宽实现跨地域互通，打造极致的游戏玩家体验

可观测 - 网络巡检

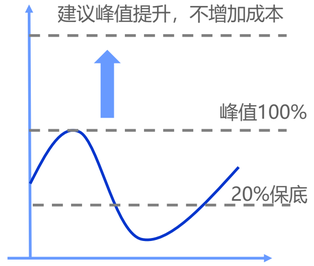
从稳定、安全、性能、成本维度，发现网络潜在的风险，并提供优化建议，帮助客户提升架构健壮性

单可用区



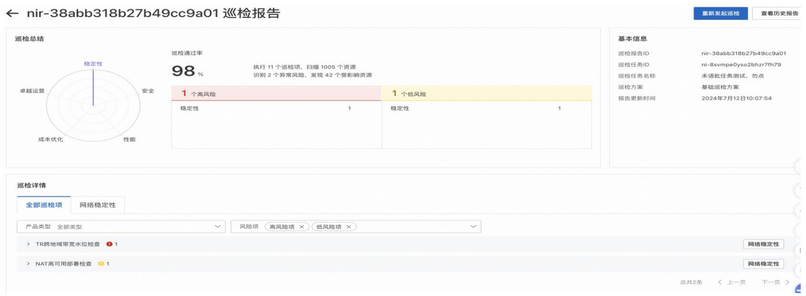
主备不生效

水位隐患

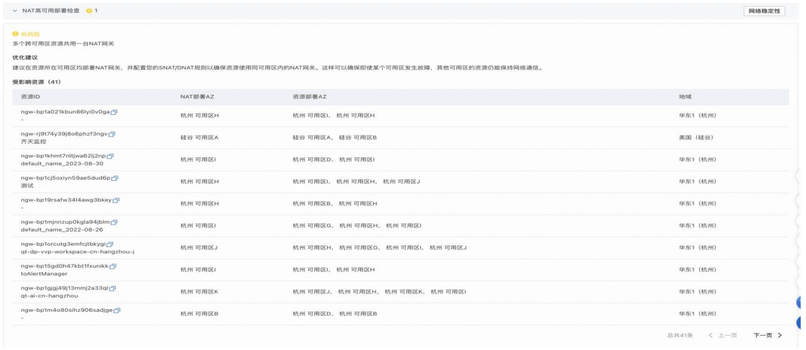


优化建议

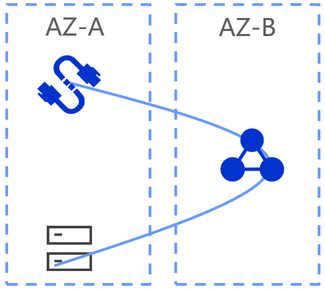
提供汇总报告和评分，支持自定义巡检项和巡检实例



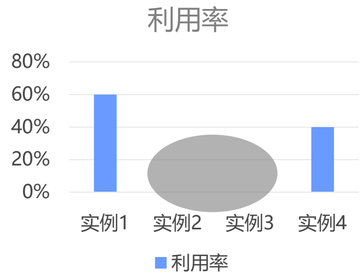
针对风险事件，提供影响面分析和优化建议



流量绕行



成本浪费



其他问题

网络ACL配置漏洞

安全组权限过大

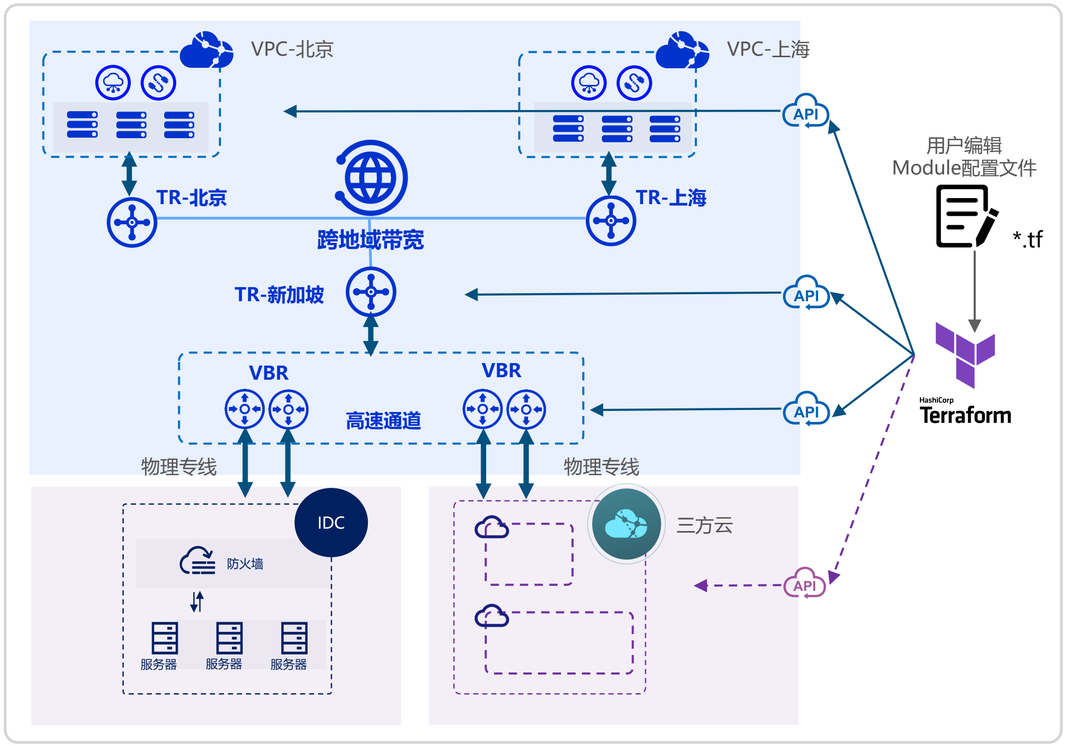
……

自服务 - 通过IaC自动化部署

将符合云网络卓越架构的方案IaC化，通过Terraform实现快速交付

IaC(Infrastructure as Code) for 卓越架构设计示例

卓越架构IaC Module：专线构建混合云/多云网络（"hybrid-cloud-network"）



方案优势

1. 效率提升

- 部署效率：8h->0.5h, 16x ⬆
- 变配效率：1h->10min, 6x ⬆

2. 标准化交付

- 架构标准化
- 代码标准化

3. 扩展性强

- 模块化部署
- 变量按需调整

IaC能力更新

100%

100%适配TerraForm

云网络核心产品 100% 接入Terraform

更易用的IaC能力

从单产品的IaC能力，提升到场景级

云网络卓越架构白皮书和TF Module正式发布

云网络卓越架构白皮书

Well-Architected Framework

云网络卓越架构五大支柱

稳定 Reliability		安全 Security		性能 Elasticity Performance		可观测 Deep Observability		自服务 Efficient Automation	
多机房容灾	同地域多可用区部署设计	安全隔离	安全组	弹性设计	ALB/NLB替换CLB提升弹性能力	流量观测	公网流量分析与监测	自动化	通过IaC自动化部署
	跨地域容灾网络设计		网络ACL	QoS设计	跨地域QoS设计		VPC间流量分析与监测		结合FC自动化运维
	NAT网关多可用区容灾设计		TR路由策略		专线接入QoS设计		混合云流量分析与监测		
	TR多可用区部署设计		TR多路由表	时延设计	公网最短时延设计		跨地域流量分析与监测		
多线路容灾	多专线多点接入高可用	流量安全	东西向流量安全		跨地域最短时延设计	运维监测	网络巡检		
	专线与VPN容灾设计		南北向流量安全		专线上云最短时延设计		告警感知		
	冗灾快速倒换		混合云流量安全	带宽管理	公网带宽选型				

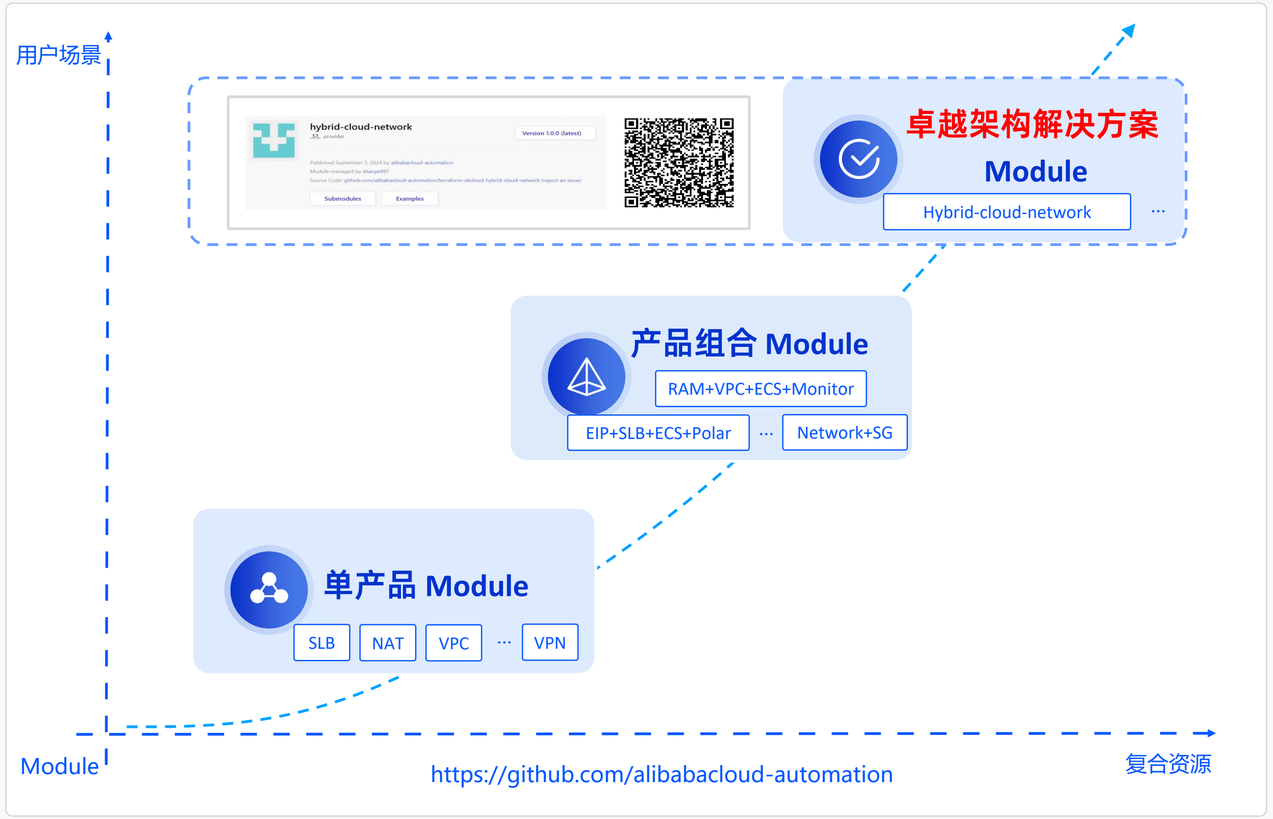
云网络卓越架构覆盖四大核心业务场景

VPC组网	全球互联	应用交付	智能运维
同地域网络设计	专线构建混合云	应用加速网络	性能观测
统一公网出入口	云上跨地域网络	跨地域调度网络	事件告警
东西向安全设计	IPsec VPN构建分支接入	七层应用交付网络	网络流量可视化
企业服务共享网络	3Rd SD-WAN构建分支接入	四层应用交付网络	网络实例和路径诊断

将于11月上线阿里云官网

卓越架构 TerraForm Module

WAF TF Module



更多卓越架构Module，敬请期待

APSARA 云栖大会

谢谢

Thank You