
Architect
SACC
2022 中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2022
激发架构性能 点亮业务活力
云上会议 网络直播 | 2022年10月27-29日
ITPUB

荔枝混合云网实践分享

荔枝集团 运维总监 熊振

公司介绍

2020年1月17日

荔枝集团登陆纳斯达克交易所，成为

中国在线音频第一股

个人介绍

熊振

荔枝运维负责人

曾就职于网易游戏、腾讯云

聚焦 IaaS 建设、SDN、全球化混合云网络架构设计

目录

- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

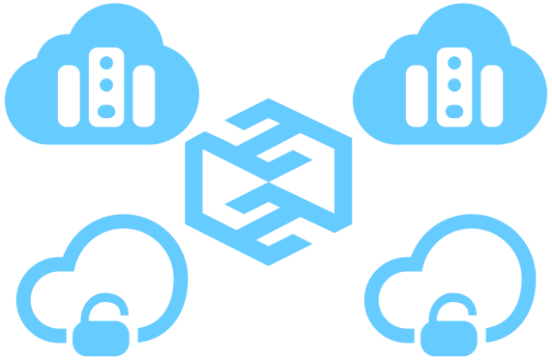
目录

- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

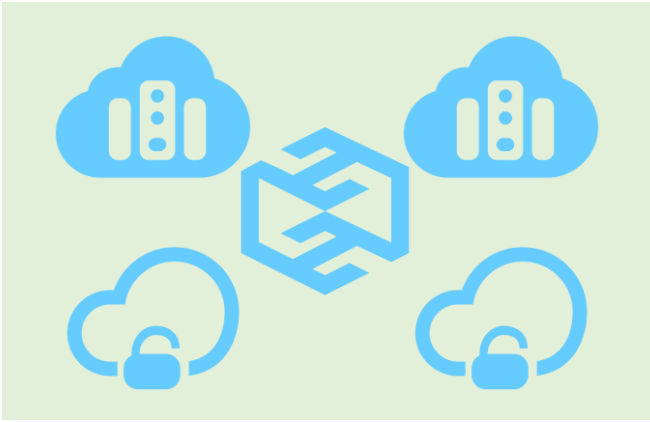
混合云发展历程

单一公有云
单一异构私有云

多个公有云
多个私有云



多个公有云
多个私有云
基础混合云管理



多个公有云
多个私有云
全栈混合云管理

单一混合云
Single Hybrid Cloud

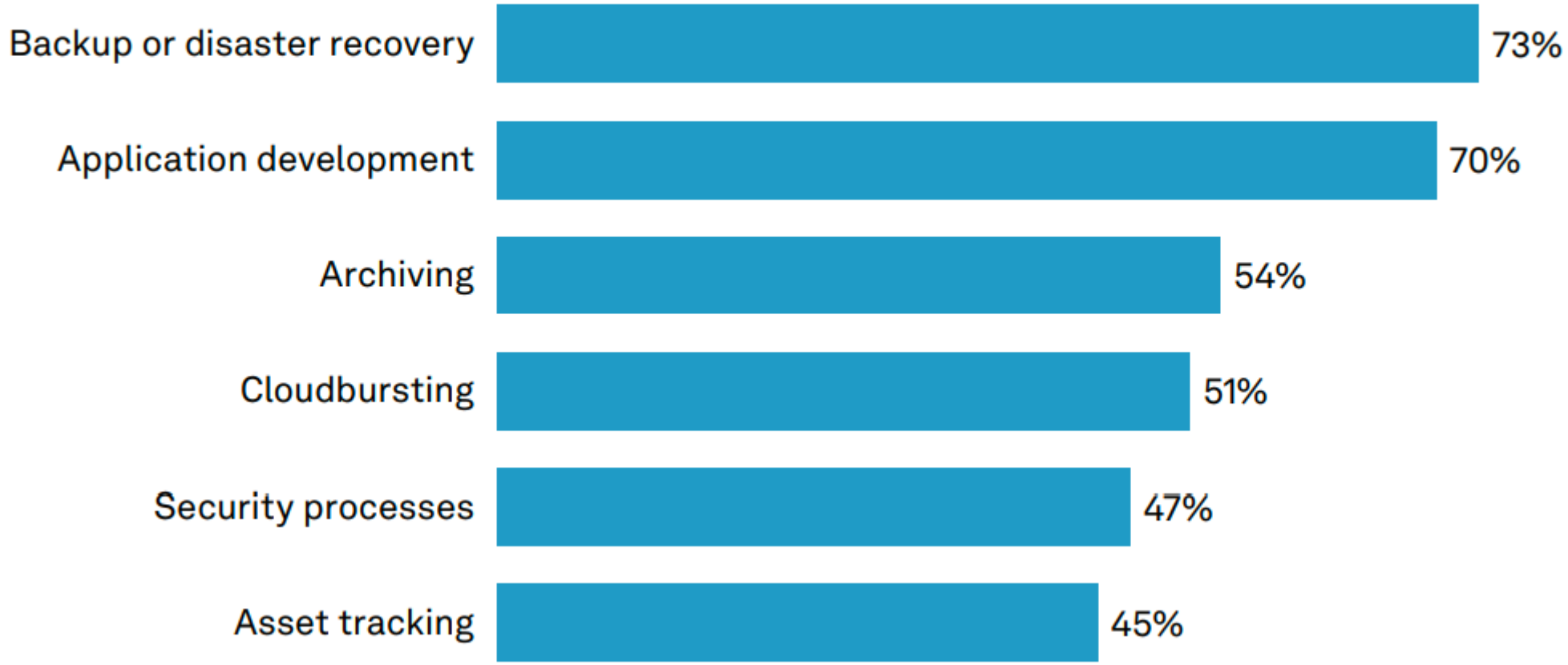
孤立混合云
Isolated Hybrid Cloud

集成混合云
Integrated Hybrid Cloud

协同混合云
Collaborative Hybrid Cloud

出海浪潮中的混合云趋势

Figure 1: Organizations Use Hybrid IT Approach Across Myriad Workloads



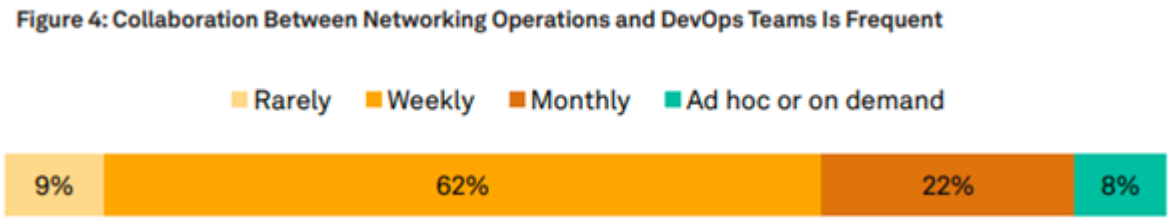
图出自《2022 Global Hybrid Cloud Trends Report》

目录

- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

混合云管理的痛点与挑战

- 第一大挑战：多云异构带来安全的新挑战。
- 第二大挑战：混合多云环境下运营复杂度直线升高，需要CloudOps、DevOps、NetworkOps之间通力协作
- 第三大挑战：混合云环境下，从单一降低成本转向成本管理。



图出自《2022 Global Hybrid Cloud Trends Report》

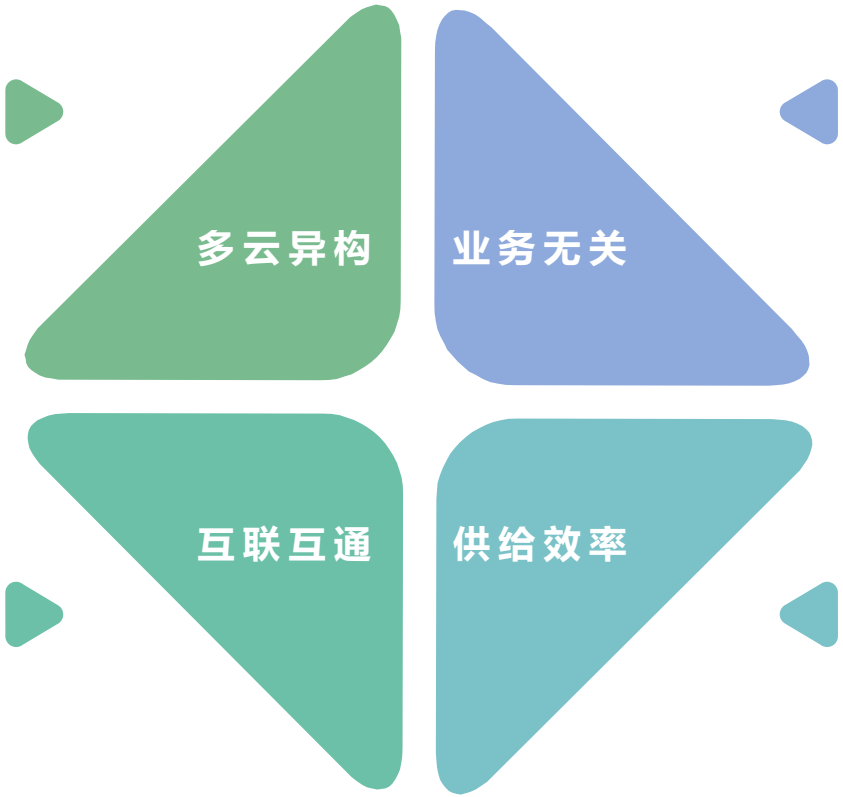
混合云管理的痛点

多云异构

多个公有云 + 一个私有云，架构各异，也意味着体验各异，如何统一所有云的使用体验？

互联互通

多云如何高效、稳定、安全的互联互通？



业务无关

公有云是业务和组织架构无关的，也就没有相应的审批流程，如何进行资源使用的管控？

供给效率

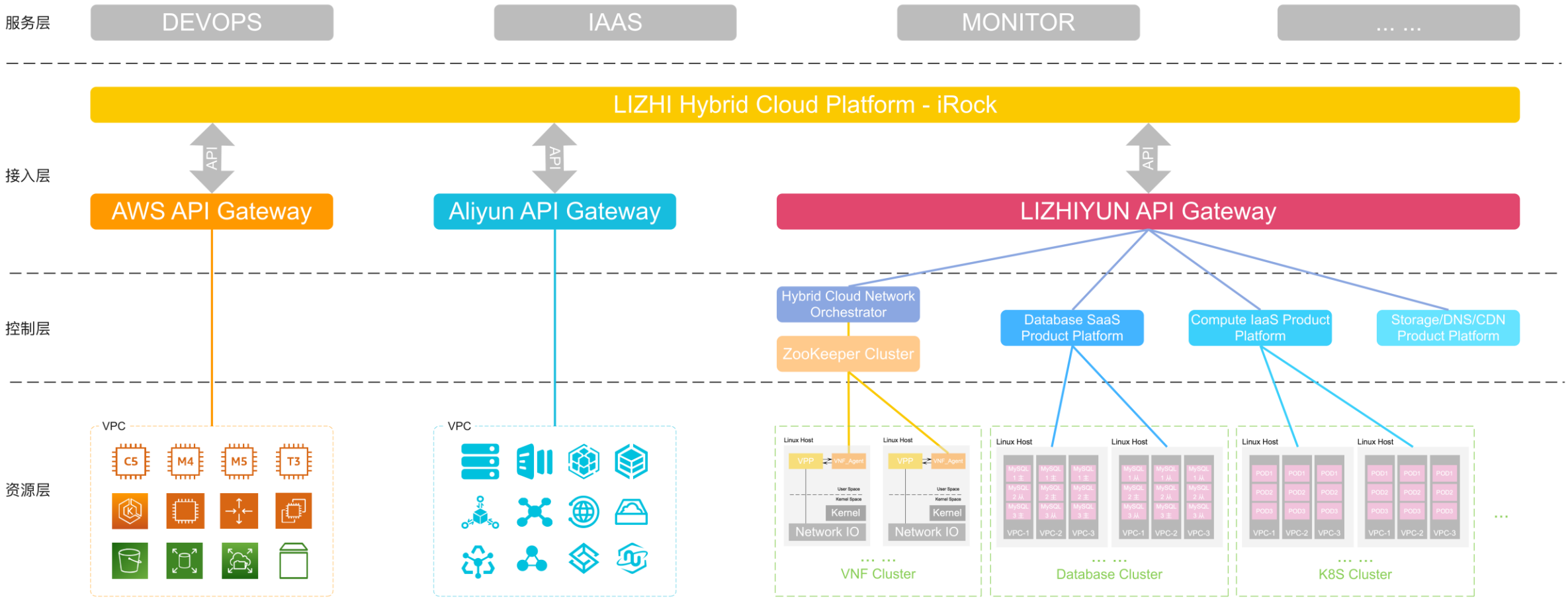
如何让真正的使用者以自助化服务的方式高效获取到所需要的云资源

目录

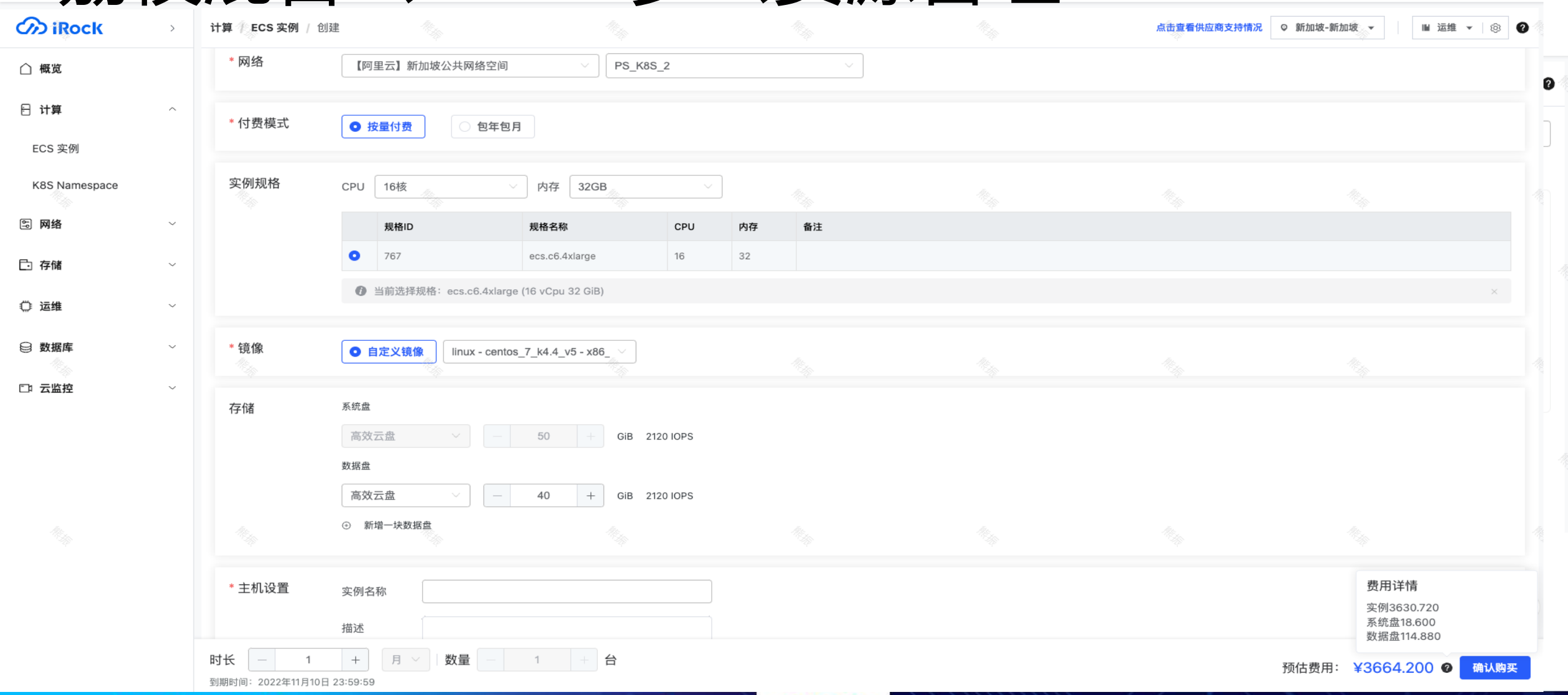
- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

荔枝混合云iRock介绍

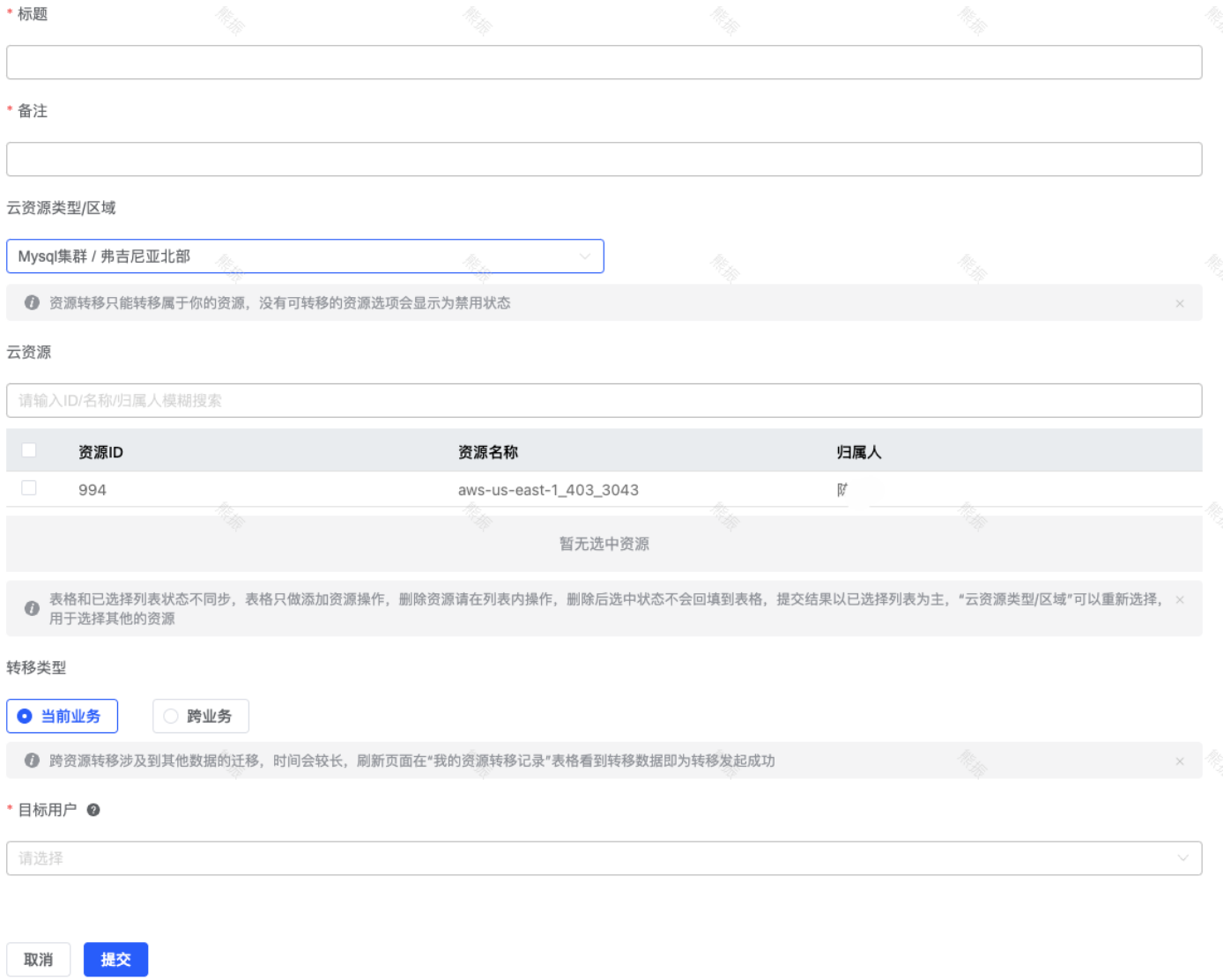
ALL CLOUD IN ONE, ONE CLOUD FOR ALL



荔枝混合云iRock-多云资源管理



荔枝混合云iRock-资源生命周期管理



荔枝混合云iRock-devops

目录

- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

网络流量分类和网络需求

01

互联互通

- VPC内互通
- 与Internet互通
- 与IDC互通
- 与其他VPC互通

02

安全

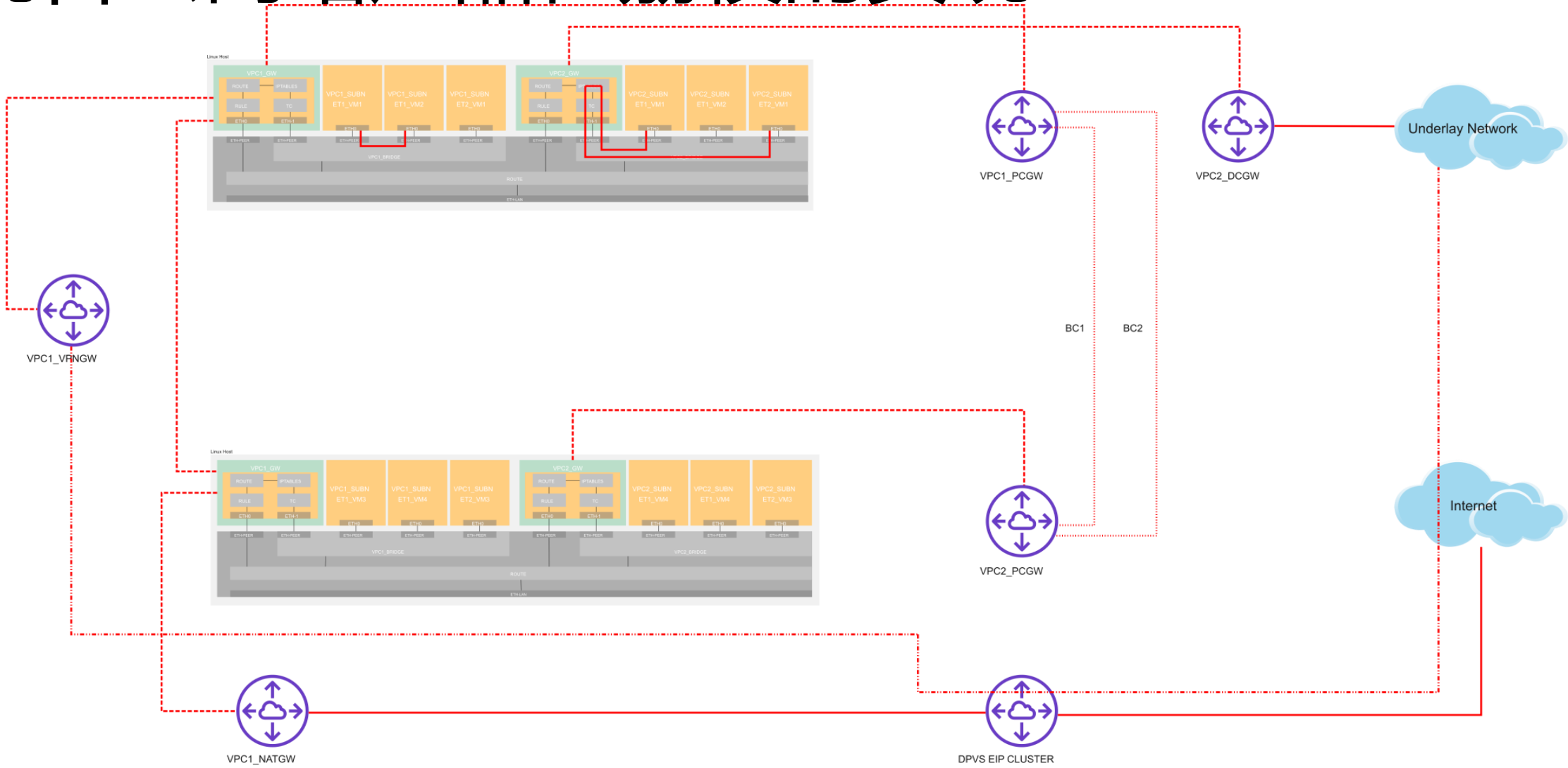
- 租户隔离
- 安全组配置
- 访问控制
- 可插入安全产品

03

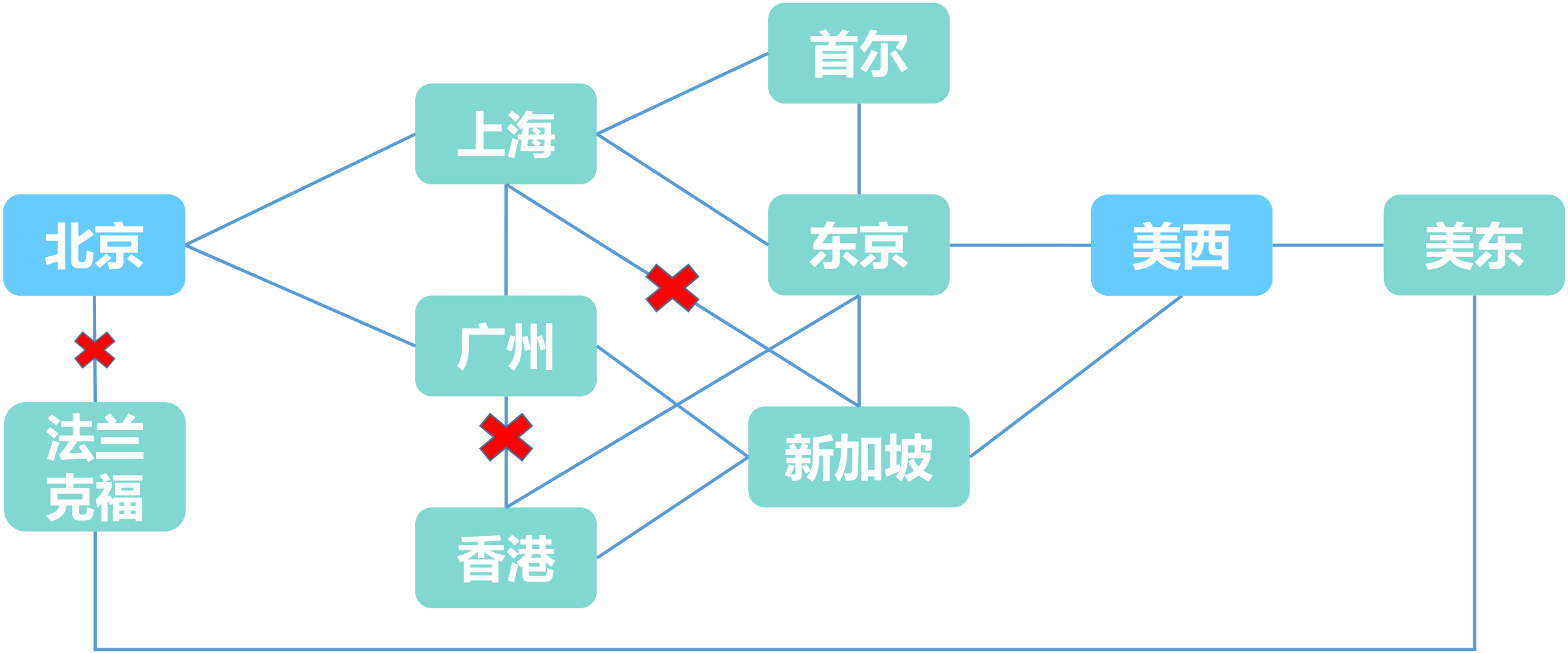
可用性

- 自助操作
- 高可用
- 可计量计费
- 可观测

混合云网络产品在荔枝的实现



跨云跨VPC互联互通需求

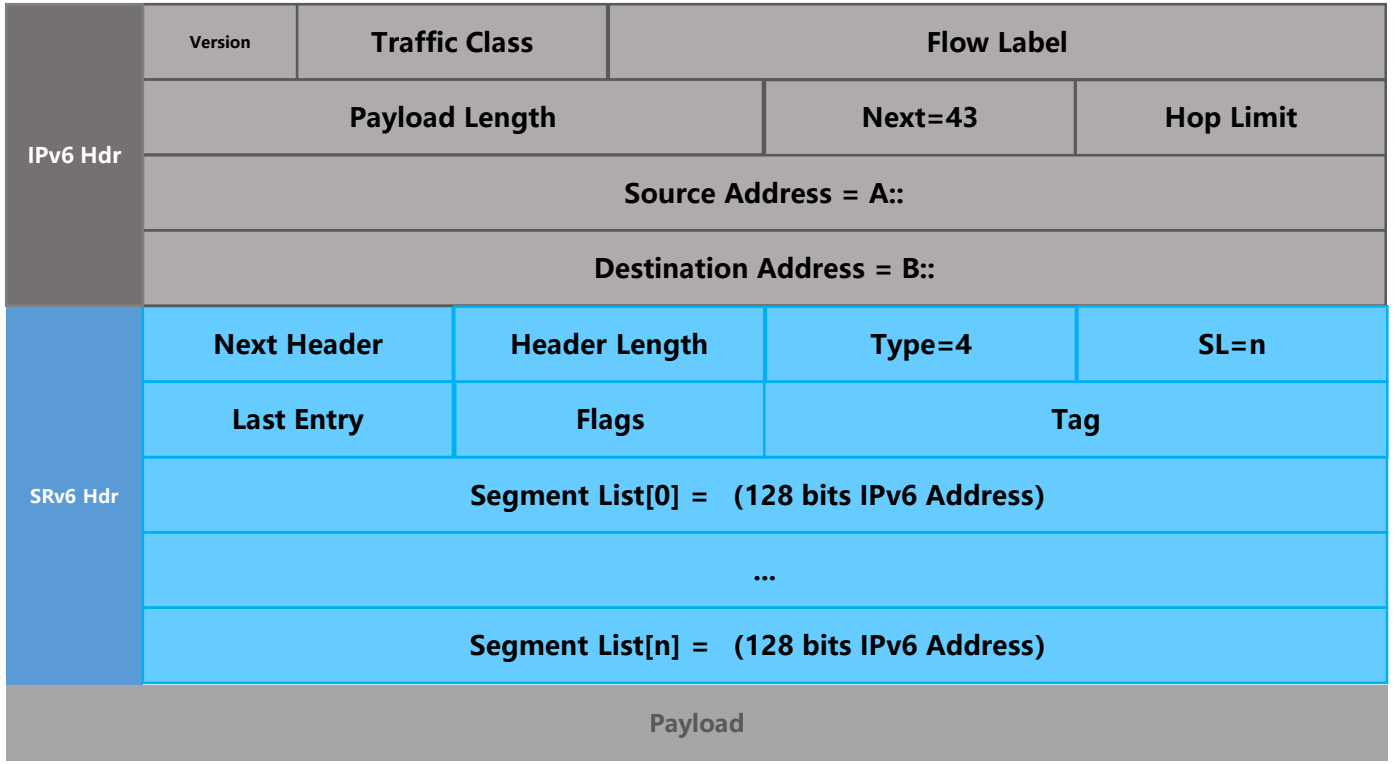


网络产品-BC产品功能需求

- 可用户自助创建，跨云跨VPC互通（必须是SDN的实现而不是人手工操作）
- 可针对不同业务采用不同的调度策略，提高链路利用率（路径可编程）
- 可以自动发现和规避故障（高可用、路径编程）
- 不hack公有云本身网络架构（利用已有的公有云网络产品）
- 结合业务做多云调度（租户隔离，互不影响）

混合云网络产品在荔枝的实现

- VPNGW（IPSec VPN Over Internet）
- DirectConnect
- SRv6 = Segment Routing IPV6



混合云网络产品在荔枝的实现

SRv6 Endpoint Behaviors

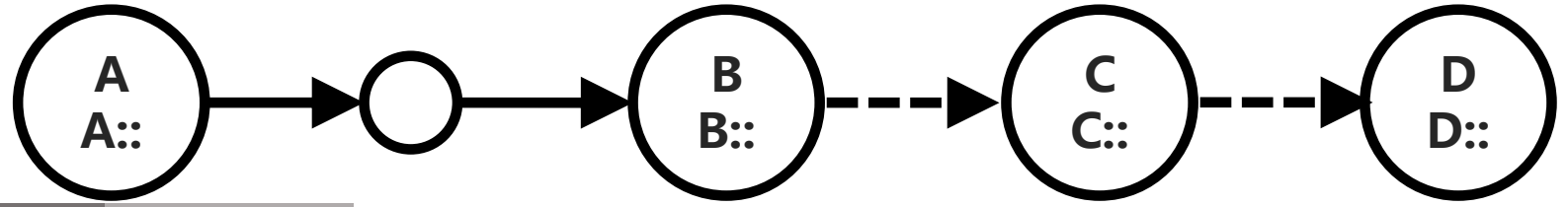
- H.Encaps—SR Headend Behavior with Encapsulation in an SRv6 Policy

SRv6 Endpoint Behaviors

- The following is a subset of defined SRv6 endpoint behaviors that can be associated with a SID.
- End—Endpoint function. The SRv6 instantiation of a Prefix SID [RFC8402].
- End.DX6—Endpoint with decapsulation and IPv6 cross-connect (IPv6-L3VPN - equivalent to per-CE VPN label).
- End.DX4—Endpoint with decapsulation and IPv4 cross-connect (IPv4-L3VPN - equivalent to per-CE VPN label).
- End.DT6—Endpoint with decapsulation and IPv6 table lookup (IPv6-L3VPN - equivalent to per-VRF VPN label).
- End.DT4—Endpoint with decapsulation and IPv4 table lookup (IPv4-L3VPN - equivalent to per-VRF VPN label).
- End.DX2—Endpoint with decapsulation and L2 cross-connect (L2VPN use-case).

混合云网络产品在荔枝的实现

Source Node



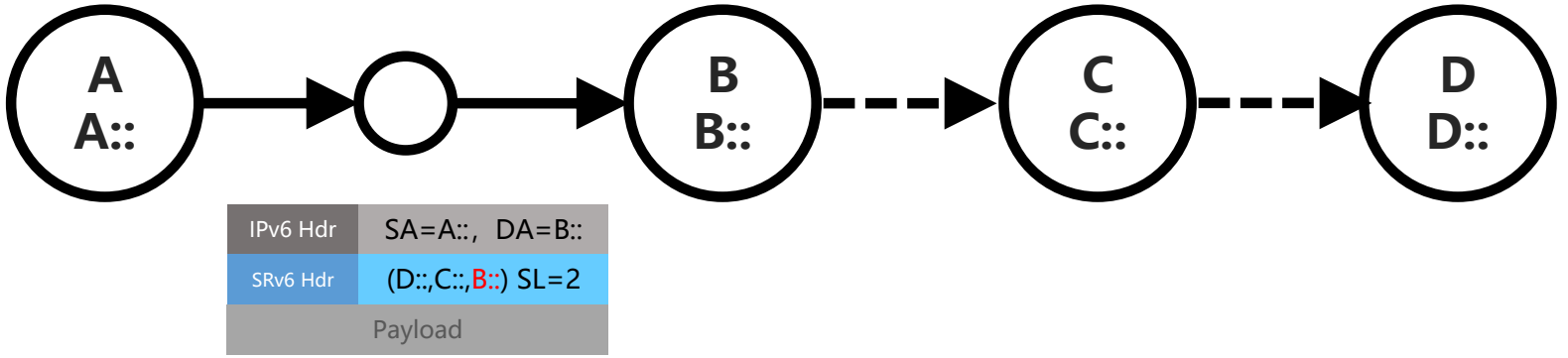
IPv6 Hdr	SA=A::, DA=B::
SRv6 Hdr	(D::,C::,B::) SL=2
Payload	

- Source node is SR-capable
- SR Header (SRH) is created with
  - Segment list in reversed order of the path
    - Segment List [0] is the LAST segment
    - Segment List [n − 1] is the FIRST segment
  - Segments Left is set to n − 1
  - Last Entry is set to n − 1
- IP DA is set to the first segment
- Packet is send according to the IP DA
  - Normal IPv6 forwarding

IPv6 Hdr	Version	Traffic Class	Flow Label	
	Payload Length		Next=43	Hop Limit
	Source Address = A::			
	Destination Address = B::			
SRv6 Hdr	Next Header	Length=6	Type=4	SL=2
	Last Entry=2	Flags	Tag	
	Segment List[0] = D::			
	Segment List[1] = C::			
	Segment List[2] = B::			
Payload				

混合云网络产品在荔枝的实现

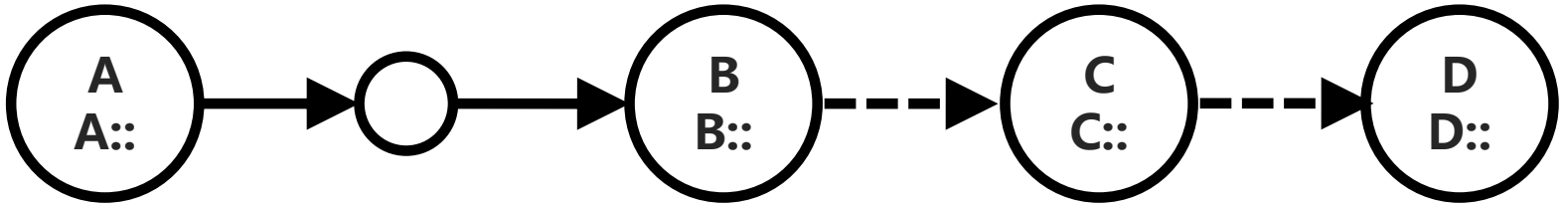
Non-SR Transit Node



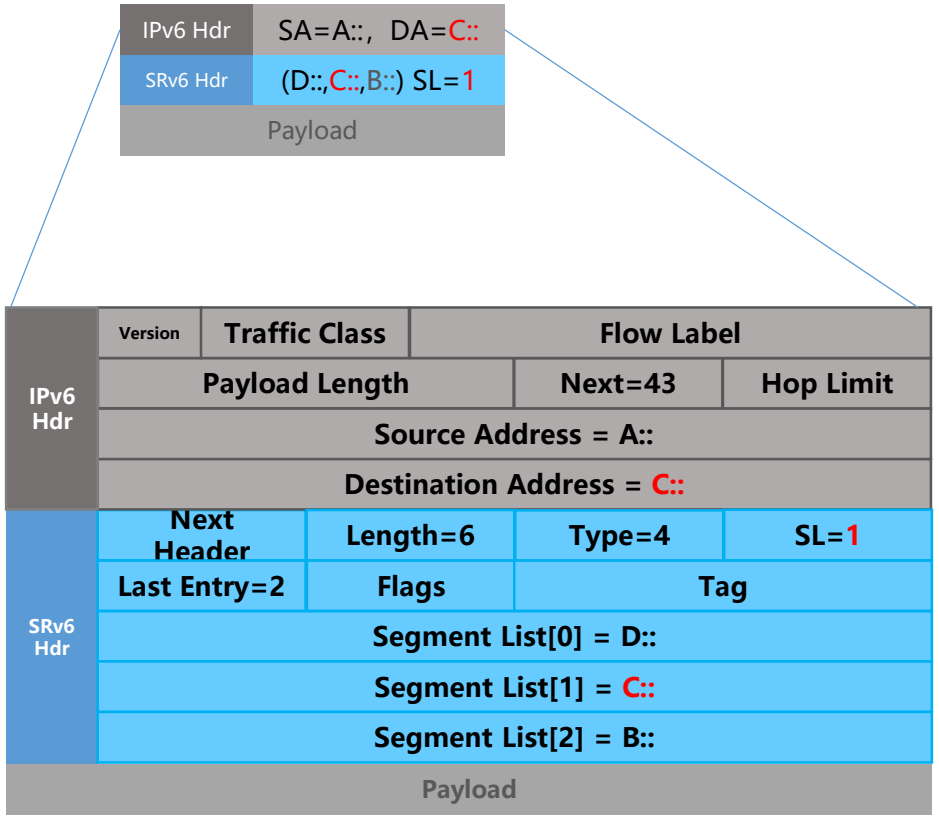
- Plain IPv6 forwarding
- Solely based on IPv6 DA
- No SRH inspection or update

混合云网络产品在荔枝的实现

SR Segment Endpoints

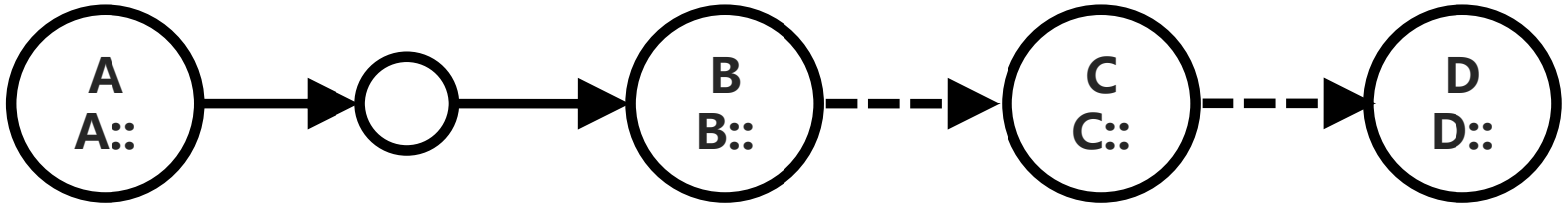


- SR Endpoints: SR-capable nodes whose address is in the IP DA
- SR Endpoints inspect the SRH and do:
  - IF Segments Left > 0, THEN
    - Decrement Segments Left (-1)
    - Update DA with Segment List [Segments Left]
    - Forward according to the new IP DA



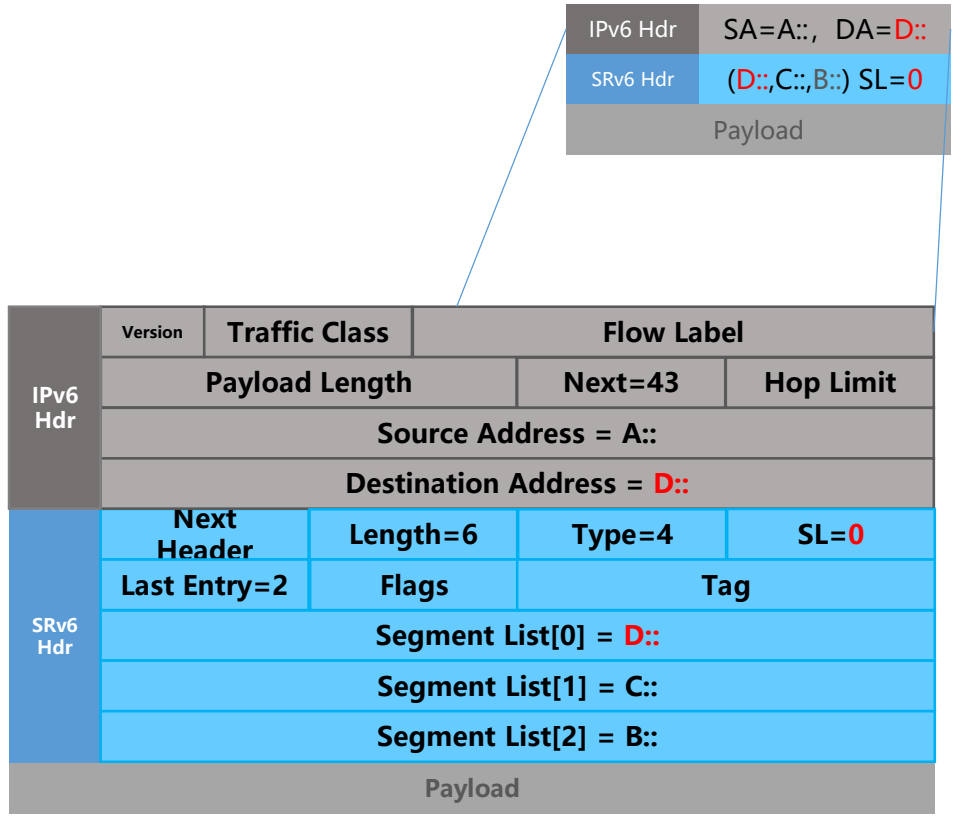
混合云网络产品在荔枝的实现

SR Segment Endpoints

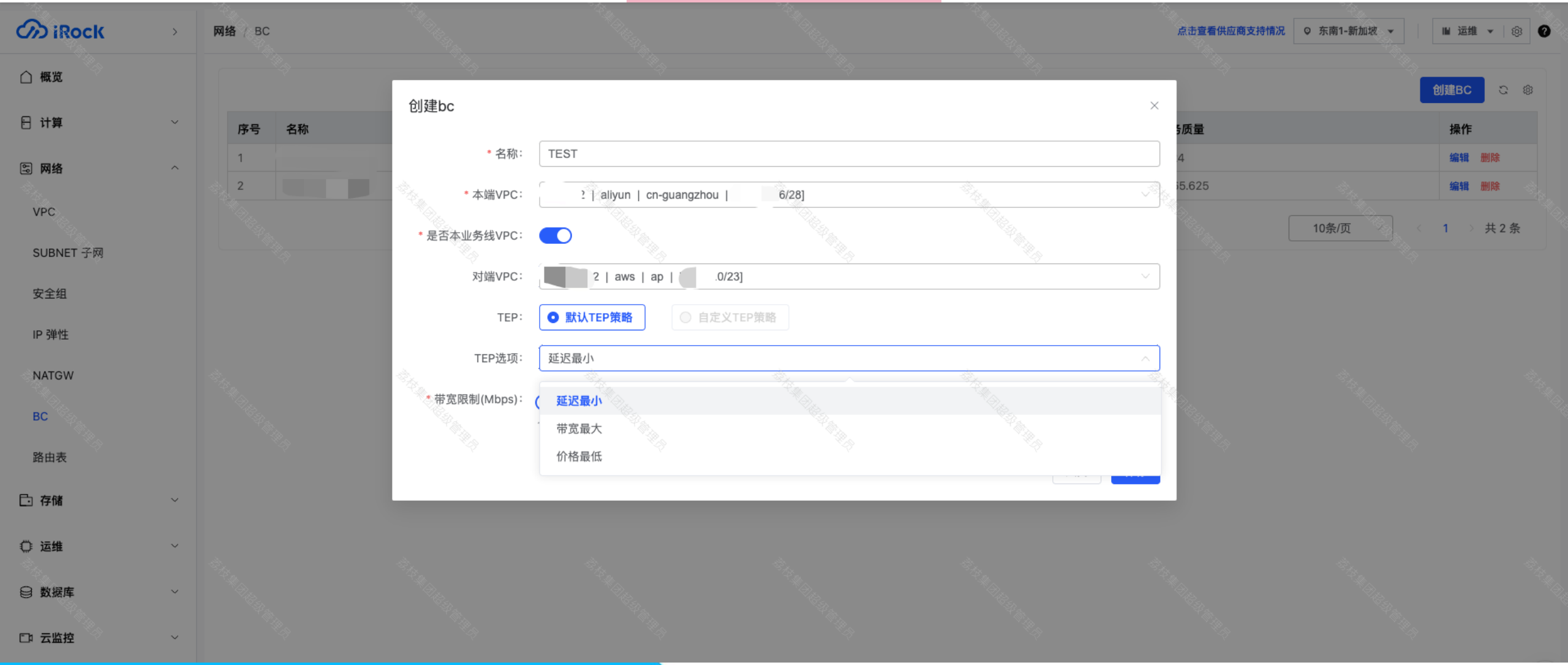


SR Endpoints: SR-capable nodes whose address is in the IP DA

- SR Endpoints inspect the SRH and do:
  - IF Segments Left > 0, THEN
    - Decrement Segments Left (-1)
    - Update DA with Segment List [Segments Left]
    - Forward according to the new IP DA
  - ELSE (Segments Left = 0)
    - Remove the IP and SR header
    - Process the payload:
    - Inner IP: Lookup DA and forward
    - TCP / UDP: Send to socket



混合云网络产品在荔枝的实现



目录

- 出海浪潮中的混合云趋势
- 混合云管理的痛点和挑战
- 荔枝混合云iRock介绍
- 混合云网络产品在荔枝的实现
- 演进规划和未来展望

演进规划与愿景

- 自定义TEP
- End to End Path Visualization
- 网络流量分析，如ntopng
- 性能提升
- 结合业务做多云调度

Cover TOC Chapter1 Chapter2 Chapter3 Chapter4 Chapter5 Ending

THANKS