H3C
数字化解决方案领导者

ADCampus 7.1一专多能培训

技术服务部·智能管理产品支持部

2024/09/24

特性列表

模块	特性
国产化适配及安装部署	国产化适配
	7.1 底盘、控制器、分析器安装部署介绍
控制器特性	全景运维地图
	控制器数据一致性检查
	支持展示离线ONU
Vxlan场景	逃生权限保持
	防火墙支持SGT和IP-SGT订阅
	VXLAN组网的AAA解耦方案
	VXLAN组播增强
	企业微信认证
Vlan场景	VLAN组网 seed方案
	传统网QoS
	VLAN场景适配
Bras场景	BRAS代拨
	BRAS哑终端认证拆分

目录

国产化适配目的

H3C
数字化解决方案领导者

■ **目的:**

- 将操作系统、数据库、中间件都切换成我司自研的产品，提高自主创新能力和竞争力。
- 国产化可以降低对外国技术的依赖，降低外部风险，保障国家信息安全。
- 新的打包部署方式可以提高部署效率，提升用户体验。

■ **使用侧感知:**

- 服务器降配
- 统一数字底盘和组件部署方式的变化

国产化适配

H3C 数字化解决方案领导者

适配项	国产化适配方案	后台查看方式
操作系统	H3Linux切换Ningos	[root@ningos01 ~]# cat /etc/*release NingOS release V3 (1.0.2403) NAME="NingOS" VERSION="V3 (1.0.2403)" ID="ningos" VERSION_ID="V3" PRETTY_NAME="NingOS V3 (1.0.2403)" ANSI_COLOR="0;31" VERSION_CODENAME=1.0.2403
数据库	pg切换seasql	[root@campus1-6656cb6489-6zvzg /]# ps -ef UID PID PPID C STIME TTY TIME CMD …… ssadmin 2510 2509 0 Aug21 ? 00:00:00 seasql: logger ssadmin 2512 2509 0 Aug21 ? 00:00:09 seasql: checkpointer ssadmin 2513 2509 0 Aug21 ? 00:00:06 seasql: background writer
中间件	底盘由Kafka切换seamq，campus控制器进行适配	[root@ningos01 ~]# kubectl get pod -A | grep seamq service-software init-basers-seamq-job-dx9cj 0/1 Completed 0 32d service-software seamq-base-controller-0 1/1 Running 0 17d
Pod合并及瘦身	集群环境16个合并为4个 单机环境8个合并为2个 占用资源减少	[root@ningos01 ~]# kubectl get pod -n campus NAME READY STATUS RESTARTS AGE campus1-6656cb6489-6zvzg 1/1 Running 1 31d oam-pod-6cd7c99bc8-wcq8k 1/1 Running 1 31d

国产化适配

H3C 数字化解决方案领导者

适配项	国产化适配方案	后台查看方式
Helm打包	组件支持并行部署，缩短部署时间	[root@ningos01 ~]# helm list -n campus NAME NAMESPACE REVISION UPDATED STATUS CHART APP VERSION campus campus 1 2024-08-09 13:04:45.494946439 +0800 CST deployed campus-7101 init campus 1 2024-08-09 13:03:57.696065254 +0800 CST deployed init-7101 oam campus 1 2024-08-09 13:04:45.394116684 +0800 CST deployed oam-7101
Oam pod	Openjdk切openj9，降低内存占用	[root@oam-pod-6cd7c99bc8-wcq8k /]# java -version openjdk version "1.8.0_372" IBM Semeru Runtime Open Edition (build 1.8.0_372-b07) Eclipse OpenJ9 VM (build openj9-0.38.0, JRE 1.8.0 Linux amd64-64-Bit Compressed References 20230518_663 (JIT enabled, AOT enabled) OpenJ9 - d57d05932 OMR - 855813495 JCL - dd0ccb1fb5 based on jdk8u372-b07)
开发语言	Python2切python 3	[root@campus1-6656cb6489-6zvzg /]# rpm -qa | grep python python3-gpgme-1.16.0-2.nos1.x86_64 python3-libcomps-0.1.18-2.nos1.x86_64 python3-libdnf-0.69.0-2.nos1.x86_64 ……

7.1方案推荐策略

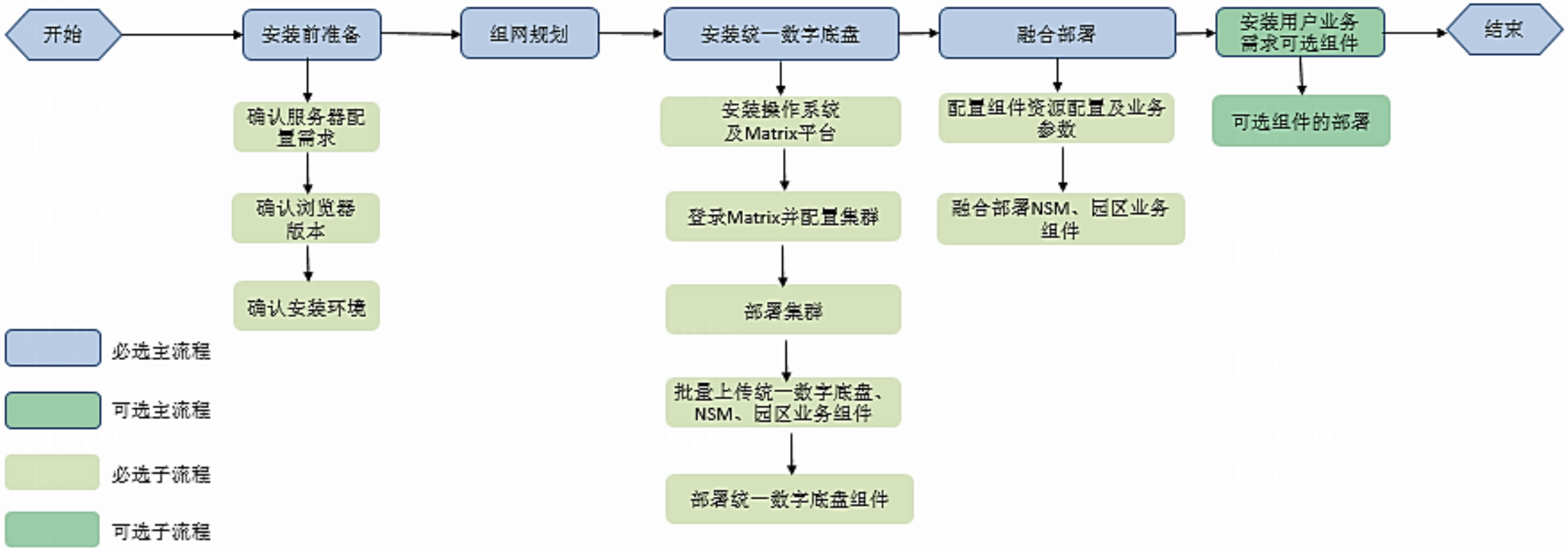
1. 金融、运营商、海外局点不使用7.1方案；
2. 公司立项的重大项目中不使用7.1方案；
3. 如果项目有操作系统、数据库、中间件、XC设备款型等**整体的**国产化要求，仅7.1方案支持；
4. 对功能特性、新需求的强制要求，仅7.1方案合入的，需要使用7.1方案；
5. 短期内不支持6.x方案升级至7.1，预计明年Q2支持，但不会让在网局点随意升级至7.1方案。

如果托付电子流评估使用7.1方案开局，二线会拉通研发、一线、市场等多方开会，谨慎评估使用7.1方案的必要性；如达成共识必须要用7.1方案，则至少今年会对该项目的实施过程重点关注。

H3C
数字化解决方案领导者

ADCampus7.1安装部署简介

7.1方案安装部署过程概述



ADCampus7.1方案各组件版本及资料下载路径

H3C 数字化解决方案领导者

分类	安装包名称	功能说明	FTP路径	部署指导	说明		
统一数字底盘应用包	NingOS-version.iso	H3C 磐宁 NingOS 操作系统的安装包	/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_**U-Center 5.0** & 统一数字底盘&各类V9组件（信创版本）/01-H3C_PLAT_2.0（统一数字底盘）	https://www.h3c.com/cn/Service/Document_Software/Document_Center/SDN/Catalog/TYSZDP/TYSZDP/Installation/Installation_Manual/H3C_E7101-1914-Long/?CHID=1058593	SE、SA均必选		
	UDTP_Base_version_platform.zip	基础服务组件：提供融合部署、用户管理、权限管理、资源管理、租户管理、菜单管理、日志中心、备份恢复和健康检查等基础功能					
	BMP_Common_version_platform.zip	通用服务组件：提供大屏管理、告警、告警聚合和告警订阅等功能					
	BMP_Connect_version_platform.zip	连接服务组件：提供上下级站点管理、WebSocket通道管理和NETCONF通道管理功能					
基础网络管理应用包	U-Center_UCP_BasePlat_version_platform.zip	基础网络管理的依赖包	/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_**U-Center 5.0** & 统一数字底盘&各类V9组件（信创版本）/15-H3C_U-Center_UCP_5.0（UCenter基础平台）	可参考对应版本的版本说明书**“版本安装操作指导”**章节	SE必选	SA均可选	
	U-Center_UCP_CollectPlat_version_platform.zip	基础网络管理的依赖包					
	NSM_FCAPS-Res_version_platform.zip	网络设备的发现、纳管和基本信息管理	/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_**U-Center 5.0** & 统一数字底盘&各类V9组件（信创版本）/10-H3C_U-Center_NSM_5.0（网络设备管理）				
	NSM_FCAPS-Perf_version_platform.zip	网络设备性能监控和展示					
	NSM_FCAPS-ICC_version_platform.zip	网络设备配置和软件部署、配置备份、配置审计					
	NSM_FCAPS-Topo_version_platform.zip	使用网络全景运维地图功能时需要部署（全景运维地图功能使用）			SE可选		
	U-Center_CMDB_version_platform.zip		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_**U-Center 5.0** & 统一数字底盘&各类V9组件（信创版本）/07-H3C_U-Center_CMDB_5.0（配置管理数据库）				

ADCampus7.1方案各组件版本及资料下载路径

H3C 数字化解决方案领导者

安装包名称		功能说明		FTP路径	部署指导	说明
SeerEngine-Campus		园区控制组件		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/50-新网络产品/01.SDN（包括SeerEngine-Campus、SeerEngine-DC、SeerEngine-WAN、SeerEngine-SDWAN、SeerAnalyzer、License Server、WVAS）/12.H3C SeerEngine-Campus（包含SeerEngine_CAMPUS、VCFC-CAMPUS、UNIS_SDNC_CAMPUS）/01.正式版本	https://www.h3c.com/cn/Service/Document_Software/Document_Center/SDN/Catalog/Campus/SeerEngine-Campus/Installation/Installation_Manual/H3C_SeerEngine_Campus_E71XX-20330/#_Toc171080181 EIA和iWM可结合版本说明书查看	必选
vDHCP		用于设备自动化上线及终端地址分配		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/50-新网络产品/01.SDN（包括SeerEngine-Campus、SeerEngine-DC、SeerEngine-WAN、SeerEngine-SDWAN、SeerAnalyzer、License Server、WVAS）/16.H3C vDHCP		必选
EIA	EIA	提供终端用户认证功能		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_U-Center 5.0 & 统一数字底盘&各类V9组件（信创版本）/20- H3C_iMC_V9组件信创版本/-iMC EIA（终端用户智能接入）		必选
	BRANCH	EIA分级功能				可选
	TAM	设备用户认证功能				
iWM	Campus_Wlan_Base	无线基础服务功能	在不安装分析器时，可以仅安装iwm相关组件，做独立的无线运维。	/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_U-Center 5.0 & 统一数字底盘&各类V9组件（信创版本）/20- H3C_iMC_V9组件信创版本/-iMC iWM（智能无线管理）		无线场景必选（SE/SA）
	Campus_Wlan_Management	智能无线管理功能				无线场景必选（SE） 无线场景可选（SA）
	Campus_Wlan_OP	智能无线运维功能				无线场景可选（SE） 无线场景必选（SA）
EAD		终端安全管理，用于终端用户安全状态的准入控制		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_U-Center 5.0 & 统一数字底盘&各类V9组件（信创版本）/20- H3C_iMC_V9组件信创版本/-iMC EAD（终端准入控制）		可选
EPS		端点探测管理，用于对网络中的各种端点进行管理。		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/30-业务软件/03-U-Center（一体化运维）/03-H3C_U-Center 5.0 & 统一数字底盘&各类V9组件（信创版本）/20- H3C_iMC_V9组件信创版本/-iMC EPS （端点探测系统）		
SeerAnalyzer		分析组件，用于对设备性能、用户接入、业务流量的实时数据采集和状态感知。		/New_Internal_Versions(新内部版本归档)/01-IP网络产品/50-新网络产品/01.SDN（包括SeerEngine-Campus、SeerEngine-DC、SeerEngine-WAN、SeerEngine-SDWAN、SeerAnalyzer、License Server、WVAS）/15.H3C SeerAnalyzer/01.正式版本（海外版本请在海外FTP目录或OneDrive取用）	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Public/00-Public/Installation/Installation_Manual/H3C_SeerAnalyzer_E71xx-20570/?CHID=1048232	可选 （如安装，Campus场景必选Analyzer-Collector , Platform, Telemetry, Diagnosis, AI, User ）

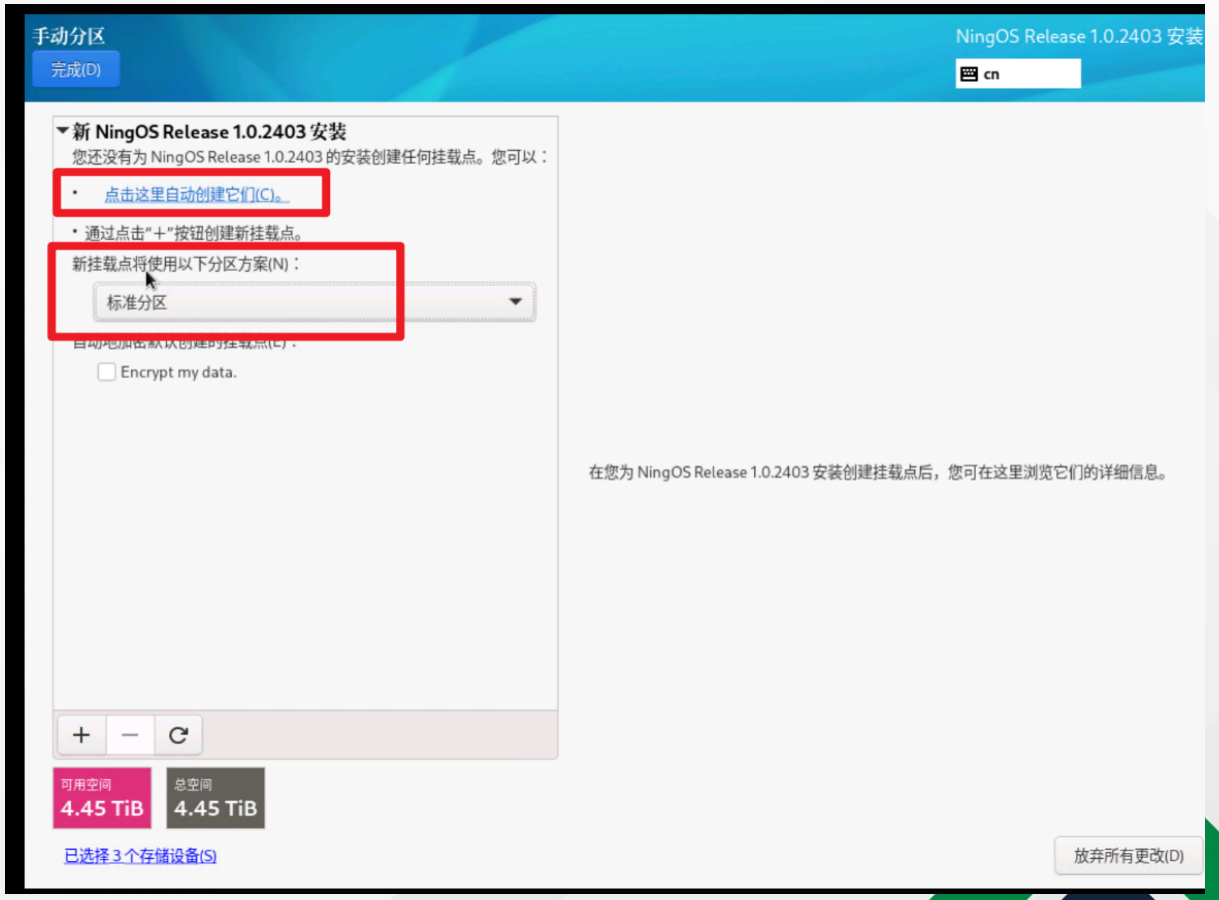
H3C
数字化解决方案领导者

操作系统安装注意事项强调

(以控制器+分析器融合部署为例)

配置磁盘分区

- 当根分区所在磁盘可用空间不低于1.7T 时，系统将会自动分区，如对分区没有要求，可采用自动分区方式；当根分区所在磁盘可用空间低于1T 时，需用户手动分区。
- ADCampus方案中请勿使用自动分区，需要手动分区



磁盘分区规划

- 综合控制器+分析器的部署指导

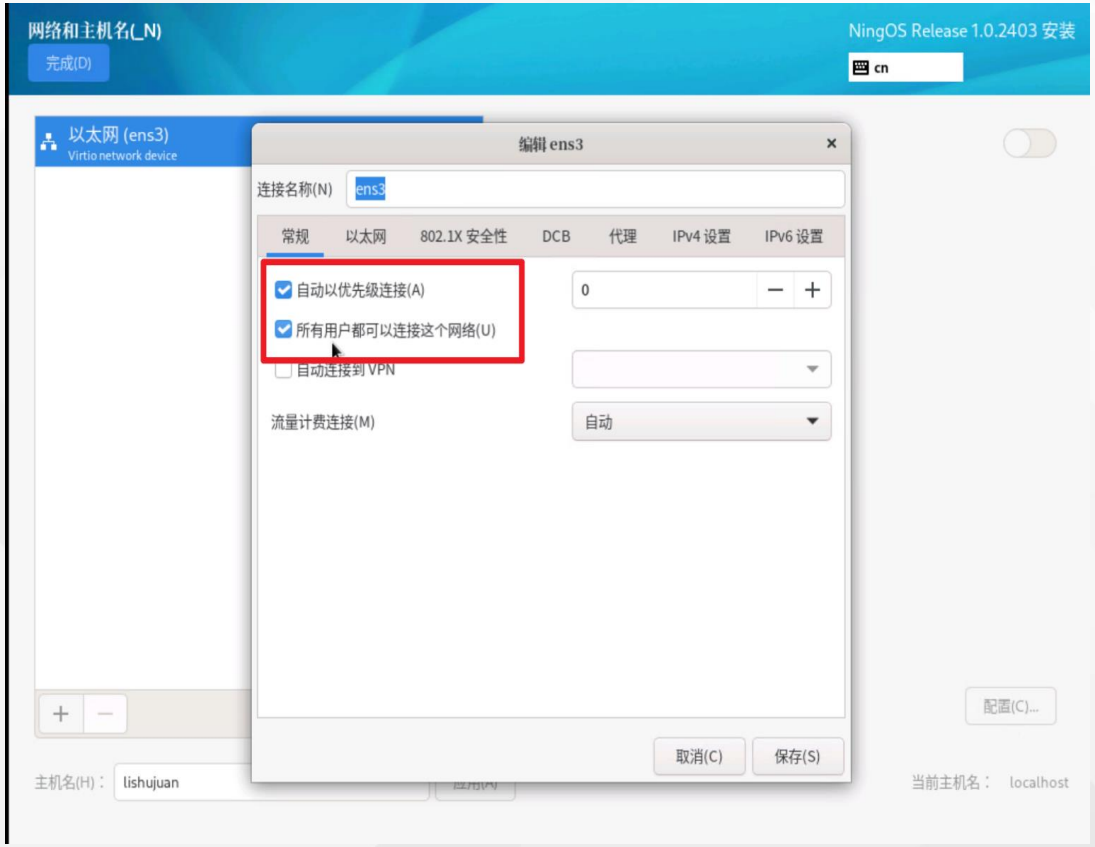
序号	磁盘	挂载点	分区说明	控制器推荐容量 (参考方案安装部署指导)	分析器推荐容量 (参考E7102)	适用模式	文件系统	备注
1	系统盘	/var/lib/docker	与Docker的运行有关	400 GiB	200 GiB	BIOS模式/UEFI模式	ext4	根据产品需求设置容量大小
		/boot		1024 MiB	1024 MiB	BIOS模式/UEFI模式	ext4	不少于1024 MiB
		swap		1024 MiB	4 GiB	BIOS模式/UEFI模式	swap	不少于1024 MiB
		/var/lib/ssdata	供数据库和中间件使用	450 GiB	640 GiB	BIOS模式/UEFI模式	ext4	• 磁盘空间充足时，可适当扩容。 • 对于SA：园区无线运维组件业务数据存储在/var/lib/ssdata路径下，有无线业务时在线用户1w及以下，/var/lib/ssdata需要增加500G容量，在线用户1w以上，/var/lib/ssdata需要增加1T容量。
		/var/lib/ssdata/logcenter	用于存放日志数据	400 GiB	290 GiB	BIOS模式/UEFI模式	ext4	磁盘空间充足时，可适当扩容
		/	Matrix使用，包括K8s，Harbor和各组件上传的安装包	400 GiB	200 GiB	BIOS模式/UEFI模式	ext4	--
		/opt/matrix/app/data/base-service/backupRecovery	业务备份数据存放使用	90 GiB	110 GiB	BIOS模式/UEFI模式	ext4	（可选） • 不创建此分区时，业务备份数据存放于根分区下 • 创建此分区时，业务备份数据存放于此分区下 • 如创建此分区，此分区使用的磁盘空间需要从根分区划出，由于各业务场景需求不同，需要根据实际情况划分大小
		/var/lib/ssdata/middleware/seaio	对应6期版本的GlusterFS功能	350GiB	70 GiB	BIOS模式/UEFI模式	ext4	--
		/boot/efi	系统为UEFI模式时才需配置	200 MiB	200 MiB	UEFI模式	EFI System Partition	不少于200 MiB
2	数据盘	/var/lib/ssdata/middleware/seasqlplus-uc	部署控制器时需要，网管使用	100 GiB	/	BIOS模式/UEFI模式	ext4	• 要求挂载一个单独的磁盘。 • 部署seasqlplus-uc实例的节点需要此分区，推荐每个节点都部署
3	ETCD	/var/lib/etcd		50 GiB	50 GiB	BIOS模式/UEFI模式	ext4	•建议挂载一个单独的磁盘。建议磁盘容量不低于51GB，否则手动分区可能会失败 •Master节点需要此分区，Worker节点不需要此分区
4	数据盘	/sa_data/mpp_data	存储分析组件的业务数据和Kafka数据	/	1300GB		ext4	
		/sa_data/kafka_data		/	700GB		ext4	

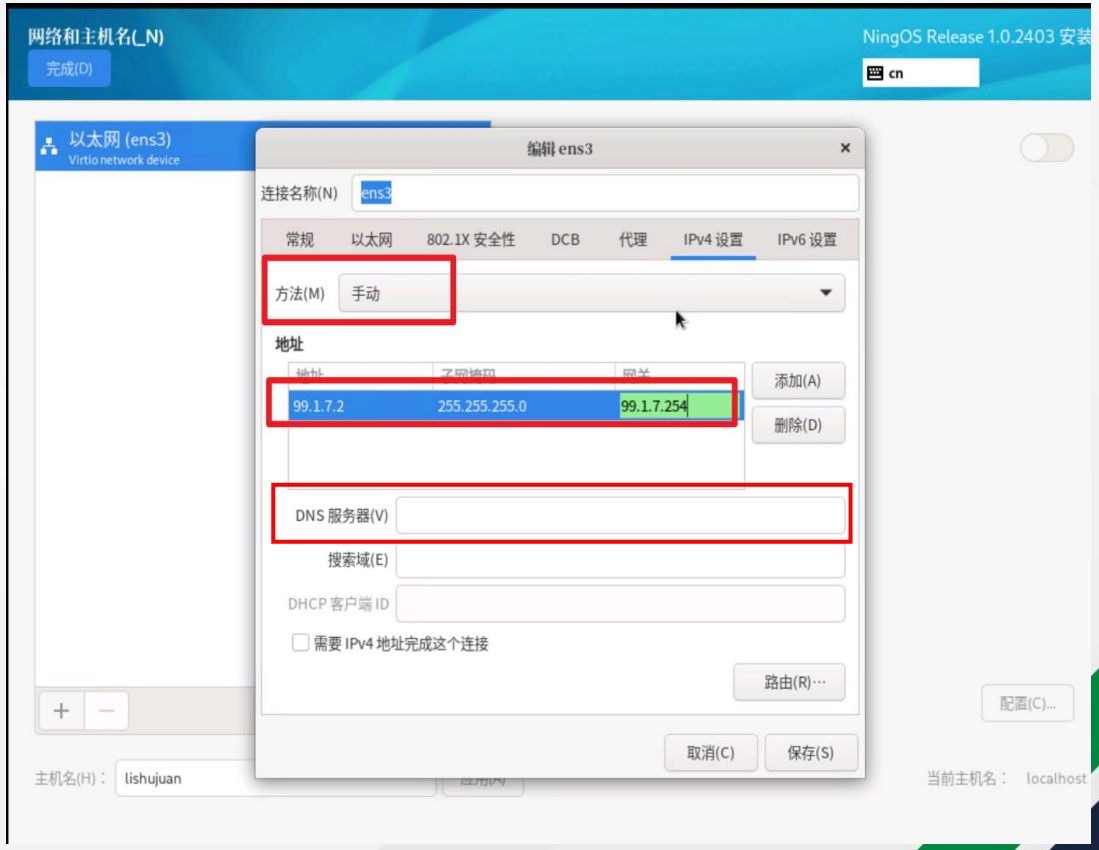
网络和主机名配置—单网卡

H3C 数字化解决方案领导者

- 单张网卡配置

- 配置IPv4、IPv6地址时必须指定网关，否则在创建集群时可能出现问题。
- 配置IPv6单栈环境时，必须禁用IPv4地址，否则IPv6地址配置不生效。若部署双栈集群，必须同时配置IPv4 和IPv6地址。
- 不允许在操作系统中配置DNS 服务器。



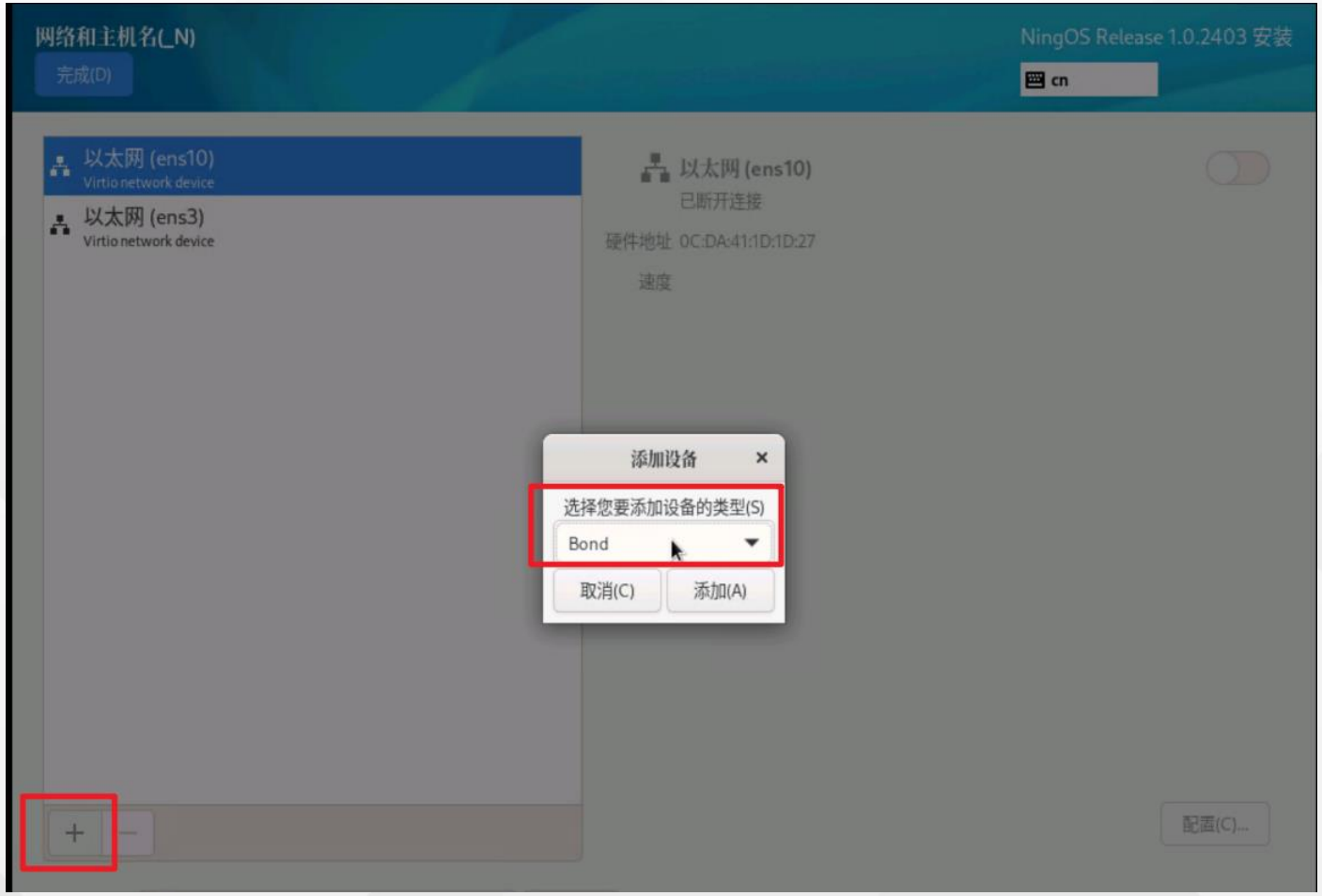


网络和主机名配置---Bond

- NingOS 操作系统安装过程中，配置网卡绑定

推荐使用Mode2 或Mode4：

- Mode2（XOR）表示XOR Hash 负载分担，需与交换机的静态聚合模式配合。
- Mode4（802.3ad）表示支持802.3ad 协议，需与交换机的动态聚合模式配合。

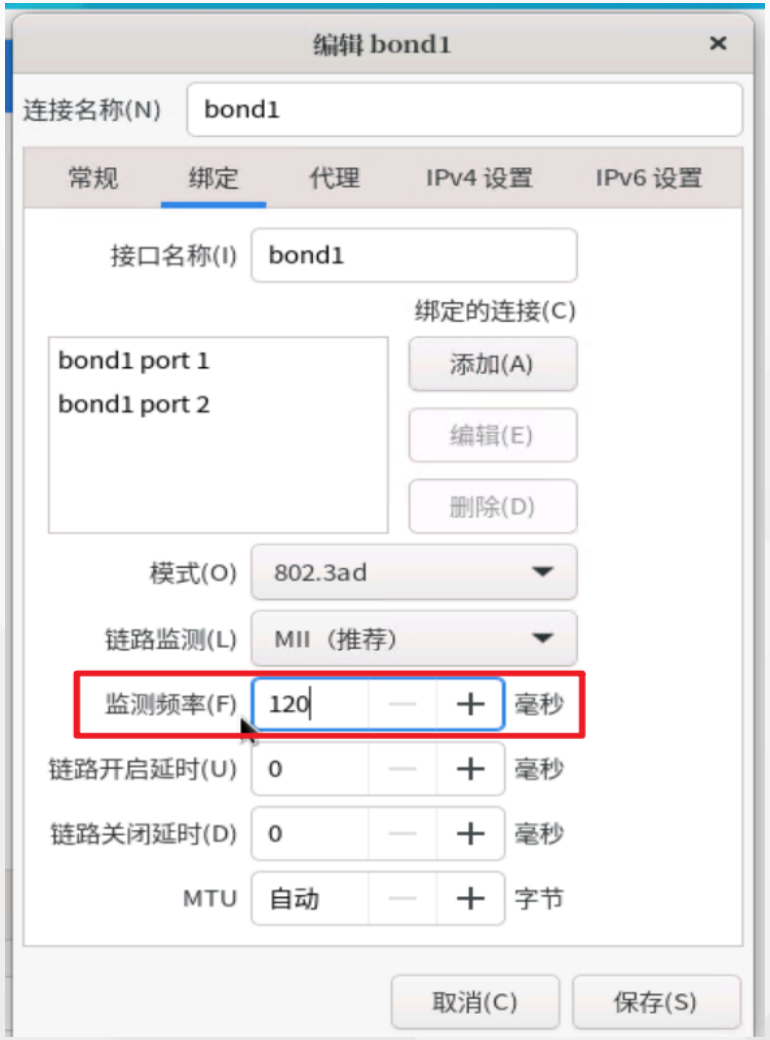


连接名称（bond 网卡名称）和接口名称保持一致，
仅支持字母、数字和下划线的组合，不支持“-”。

网络和主机名配置---Bond

- 配置bond口参数

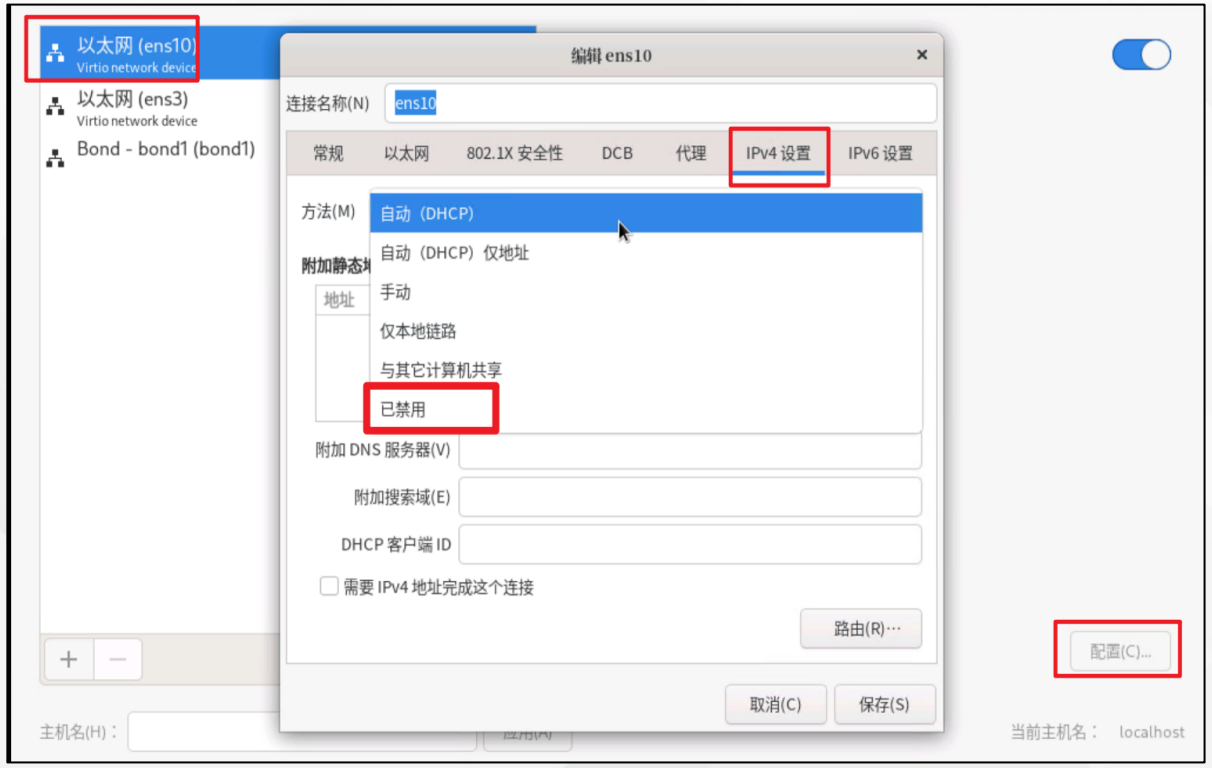
模式为异或/802.3ad；监测频率调整为120；配置IPv4/IPv6地址，仅配置IPv6地址时需禁用IPv4

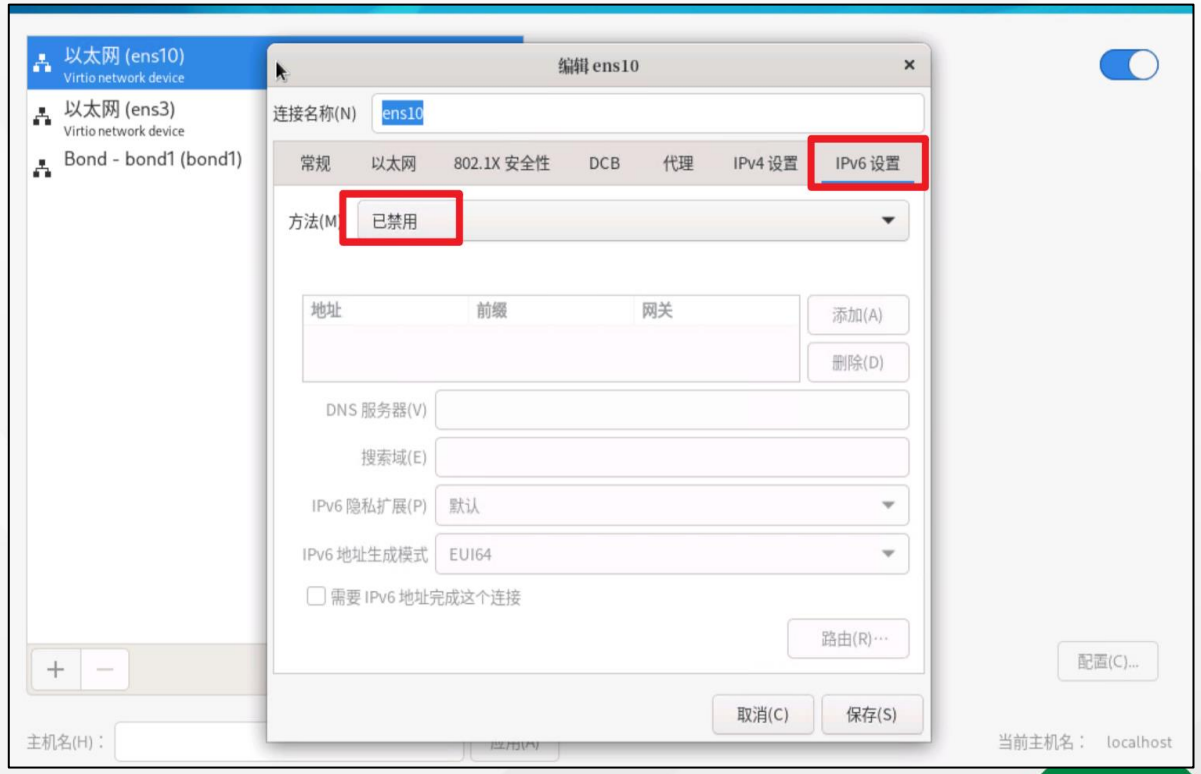


网络和主机名配置---Bond

- 禁用成员口的IPv4和IPv6

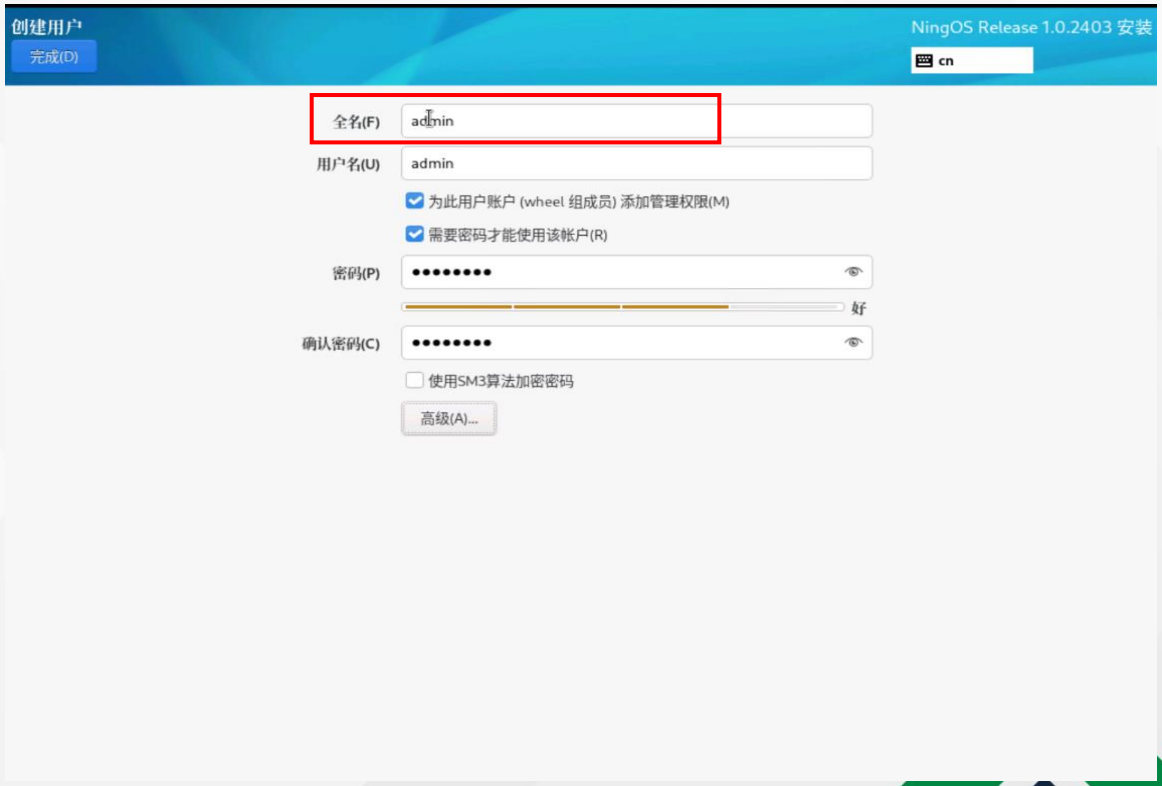
成员网卡配置默认是DHCP，若服务器重启，成员网卡会因为DHCP 获取不到地址而导致网卡无法启动。所以需要修改成员网卡的地址配置方式。





选择管理员帐户设置

- 部署Matrix 集群，需为集群中的所有节点选择相同的用户名。
- 使用root用户作为管理员帐户，该用户拥有所有功能的操作权限，admin用户将不被创建。
- 使用admin用户作为管理员帐户，需同时设置root密码。需先设置root密码，再创建admin用户。 创建admin用户后将会禁用root用户的SSH权限。勾选“为此用户账户（wheel 组成员）添加管理权限(M)”将admin 帐户作为管理员。



可通过修改/etc/ssh/sshd_config文件中的PermitRootLogin为yes启用root用户SSH权限

安装软件依赖包及工具包

- NingOS V3.1.0 ISO 集成了操作系统和依赖包。在完成操作系统的安装后，将自动安装需要的依赖包。RHEL8.8、麒麟V10 SP2、统信UOS V20操作系统需手动安装依赖包
- 均需要手动安装Matrix 等应用软件包。
- NingOS V3.1.0 ISO 集成了部分工具包（如tcpdump），存放于**/product_config/rpms** 目录中，可以使用**rpm -ivh** 安装。

```
[root@lishujuan ~]# cd /product_config/rpms/
[root@lishujuan rpms]# ll
总用量 5168
drwxr-xr-x. 2 admin wheel    4096  8月 28 20:14 bcc-tools
-r--r--r--. 1 admin wheel  138581  8月 28 20:14 blktrace-1.3.0-2.nos1.x86_64.rpm
-r--r--r--. 1 admin wheel   47257  8月 28 20:14 ftp-0.17-80.nos1.x86_64.rpm
-r--r--r--. 1 admin wheel 4552656  8月 28 20:14 h3diag-1.4.1-hl2.noarch.rpm
-r--r--r--. 1 admin wheel  474945  8月 28 20:14 tcpdump-4.99.1-6.nos1.x86_64.rpm
-r--r--r--. 1 admin wheel   66653  8月 28 20:14 telnet-0.17-78.nos1.x86_64.rpm
[root@lishujuan rpms]#
[root@lishujuan rpms]# rpm -ivh tcpdump-4.99.1-6.nos1.x86_64.rpm
警告：tcpdump-4.99.1-6.nos1.x86_64.rpm: 头V3 RSA/SHA1 Signature, 密钥 ID 418613a2: NOKEY
Verifying...                          ################################# [100%]
准备中...                             ################################# [100%]
正在升级/安装...
   1:tcpdump-14:4.99.1-6.nos1         ################################# [100%]
[root@lishujuan rpms]#
```

H3C
数字化解决方案领导者

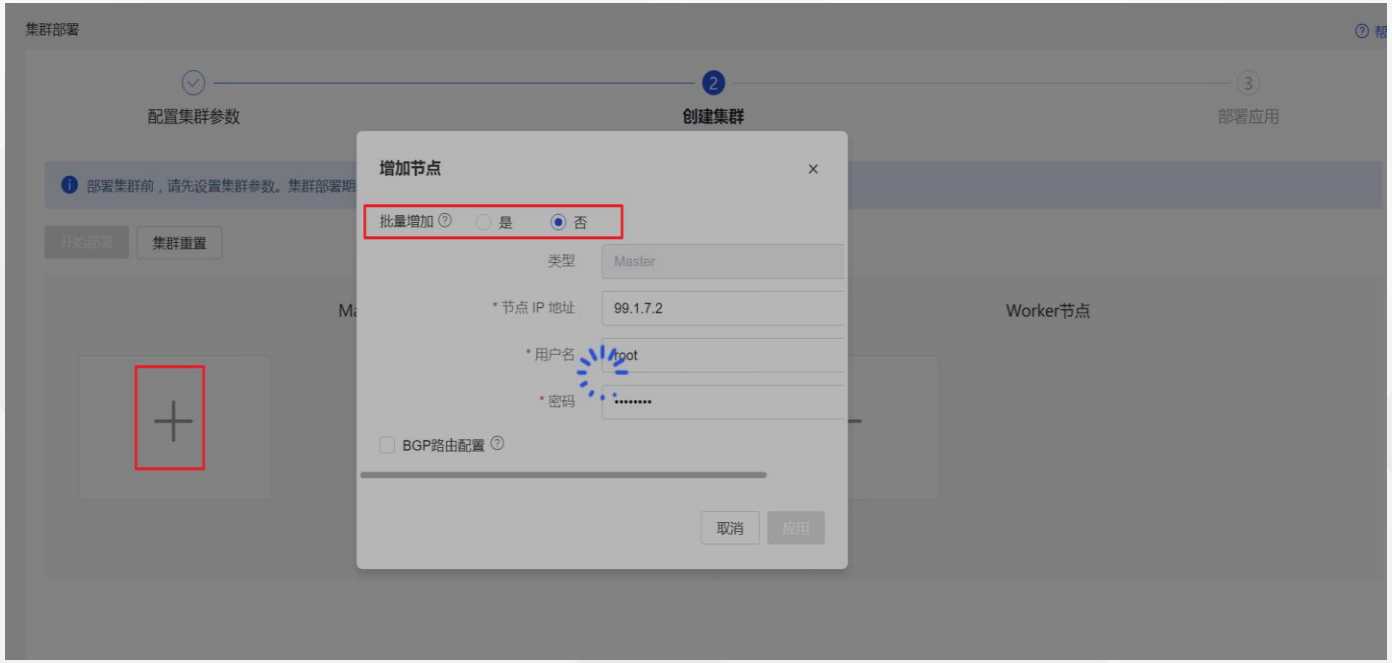
统一数字底盘安装注意事项

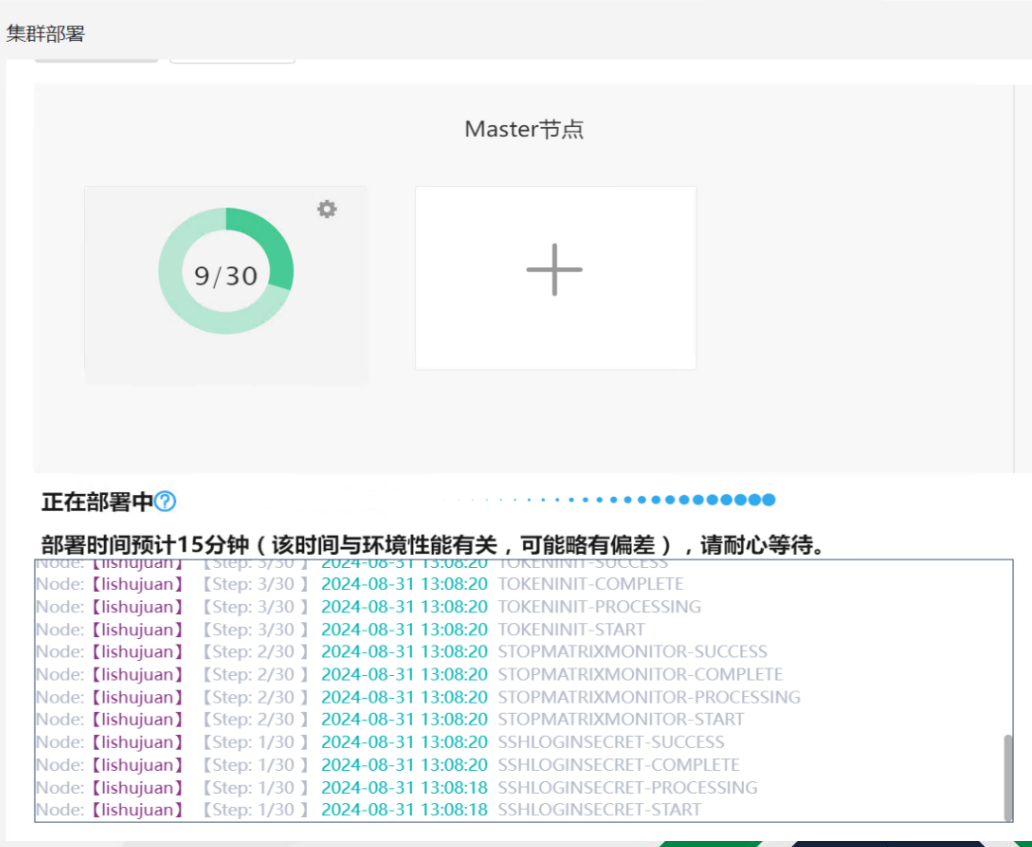
创建Matrix集群

H3C 数字化解决方案领导者

创建集群

- 增加节点，填写对应的IP、用户名、密码，支持批量增加
- Matrix 部署完成后，如需执行kubectl 命令，请断开重连当前SSH 会话后再执行对应命令，否则kubectl 命令无法执行，提示The connection to the server localhost:8080 was refused - did you specify the right host or port?





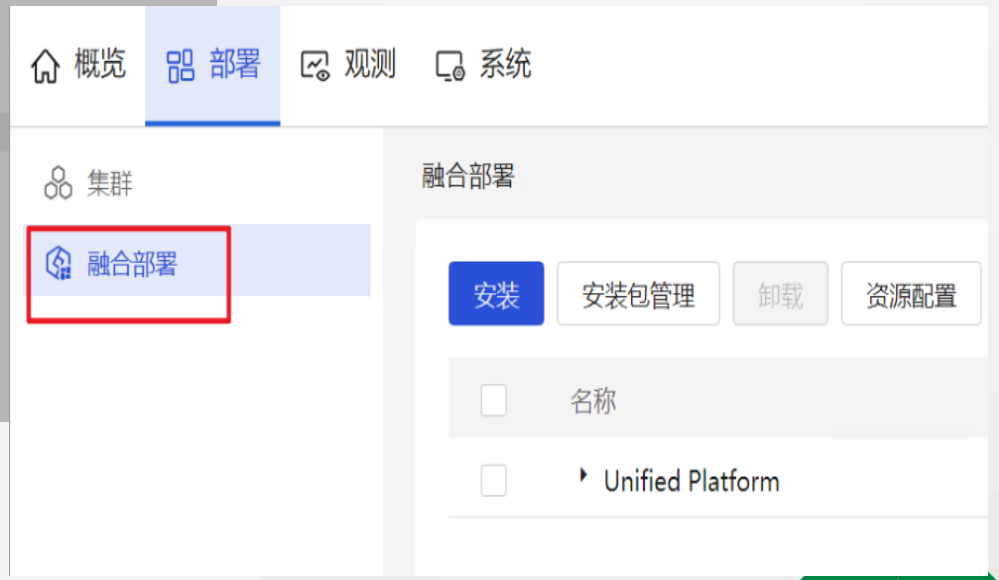
实验室环境单机部署：5.5min

部署统一数字底盘及应用

应用包仅支持在Matrix 页面进行部署，支持批量上传应用包，但必须先部署Base，再部署其他应用。

部署UDTP_BASE：部署-应用-上传组件包

Base 部署完成后，原[部署>应用]页面自动更新为[部署>融合部署]页面，可在该页面下部署其他可选包。



部署统一数字底盘及应用

- 上传其他所需组件包：部署-融合部署-安装包管理-上传
- 使用批量上传功能同时上传应用包时，浏览器部署页面不能关闭，PC 不可以进入睡眠状态、不可以断开PC 到集群的网络（可以切换浏览器页签、最小化浏览器、锁定PC 屏幕），否则会导致部分组件不能正常部署。

名称	版本	大小	创建时间	操作
Analyzer-User-E7101_x86_64.zip	E7101	388.47M	2024-08-31 15:03:44	
Analyzer-Telemetry-E7101_x86_64.zip	E7101	1956.52M	2024-08-31 15:02:27	
Analyzer-Platform-E7101_x86_64.zip	E7101	830.77M	2024-08-31 14:59:58	
Analyzer-Diagnosis-E7101_x86_64.zip	E7101	412.78M	2024-08-31 14:58:35	
Analyzer-AI-E7101_x86_64.zip	E7101	597.03M	2024-08-31 14:57:53	
Campus_Wlan_Management_E7101_x86.zip	E7101	776.71M	2024-08-31 14:46:44	
Campus_Wlan_Base_E7101_x86.zip	E7101	5285.4M	2024-08-31 14:45:18	
EIA-E7101.zip	E7101	1362.25M	2024-08-31 14:21:20	
vDHCPS_H3C-R7101-X64.zip	E7101	188.44M	2024-08-31 14:19:46	
SeerEngine_CAMPUS-E7101-MATRIX.zip	E7101	1542.29M	2024-08-31 14:19:21	
U-Center_UCP_CollectPlat_E7101_x86.zip	E7101	381.69M	2024-08-31 14:09:13	
U-Center_UCP_BasePlat_E7101_x86.zip	E7101	838.86M	2024-08-31 14:08:33	
NSM_FCAPS-Res_E7101_x86.zip	E7101	318.21M	2024-08-31 14:07:01	
NSM_FCAPS-Perf_E7101_x86.zip	E7101	121.46M	2024-08-31 14:06:20	
NSM_FCAPS-ICC_E7101_x86.zip	E7101	453.46M	2024-08-31 14:05:36	
BMP_Connect_E7102_x86.zip	E7102	164.58M	2024-08-31 14:04:57	
BMP_Common_E7102_x86.zip	E7102	1404.43M	2024-08-31 14:04:25	

分析器

iwm

EIA、vdhcp、控制器

UCP

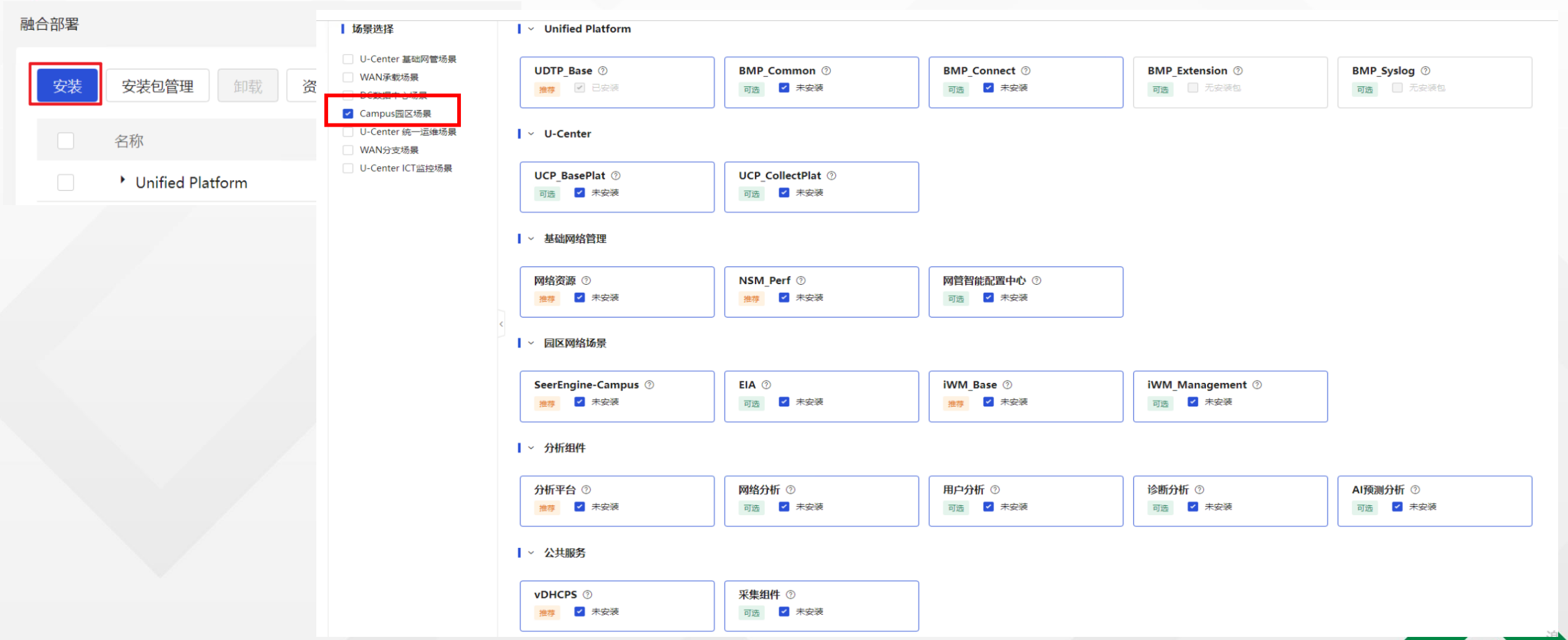
网管

BMP

部署统一数字底盘及应用

H3C 数字化解决方案领导者

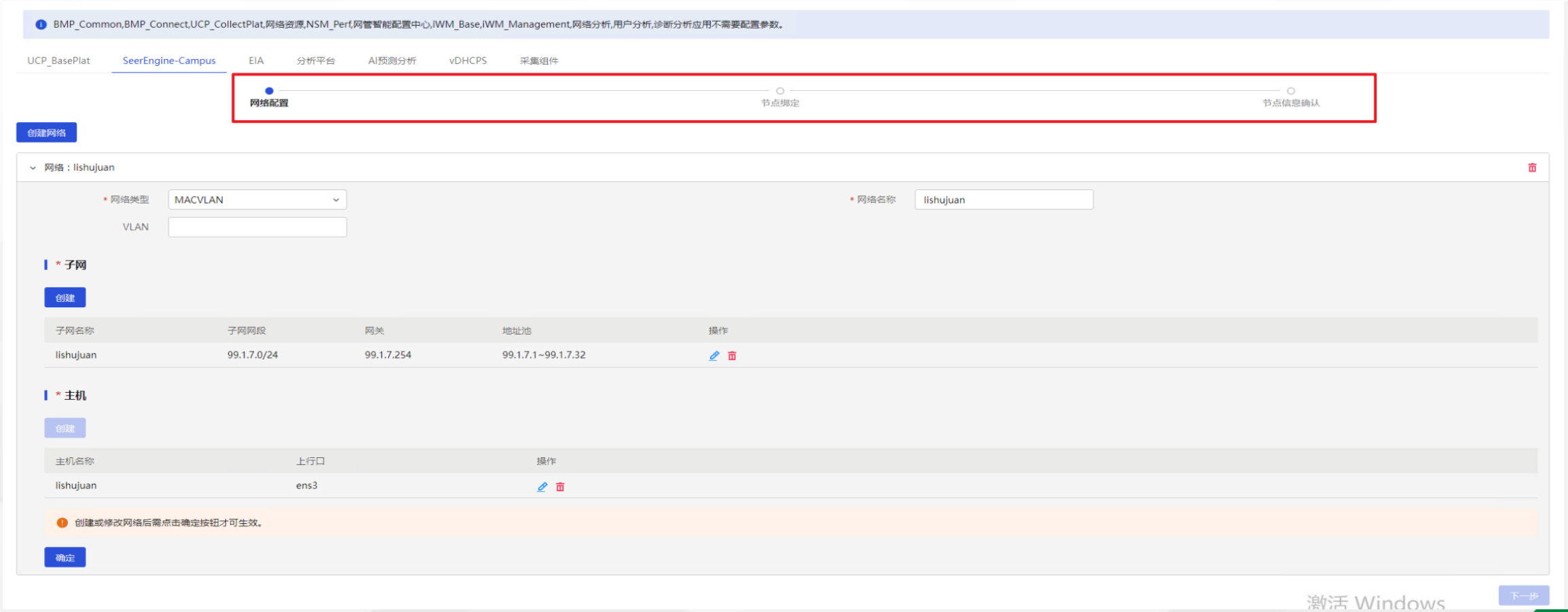
点击“安装”部署组件包，勾选<Campus园区场景>可一键选中所有园区业务组件以及依赖包。



部署参数配置

H3C
数字化解决方案领导者

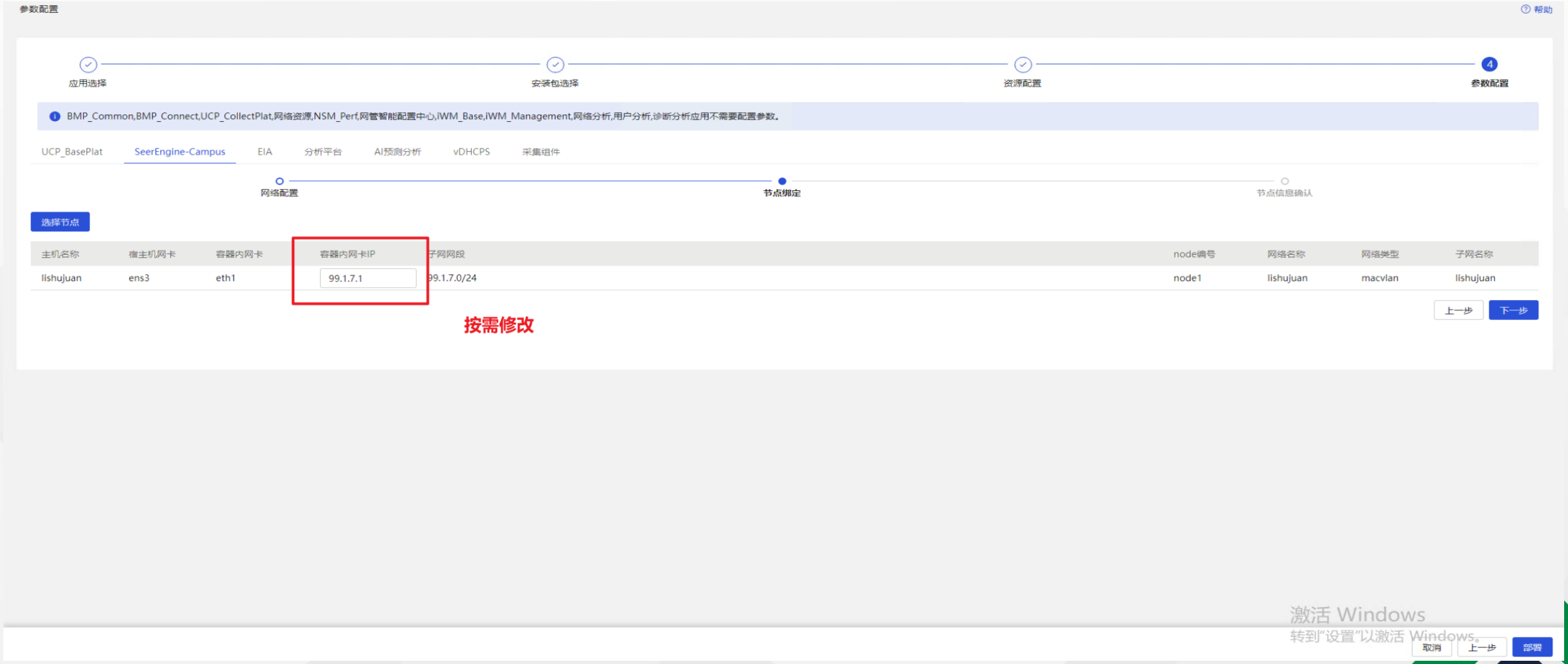
控制器：创建网络、绑定节点、确认信息



部署参数配置

H3C
数字化解决方案领导者

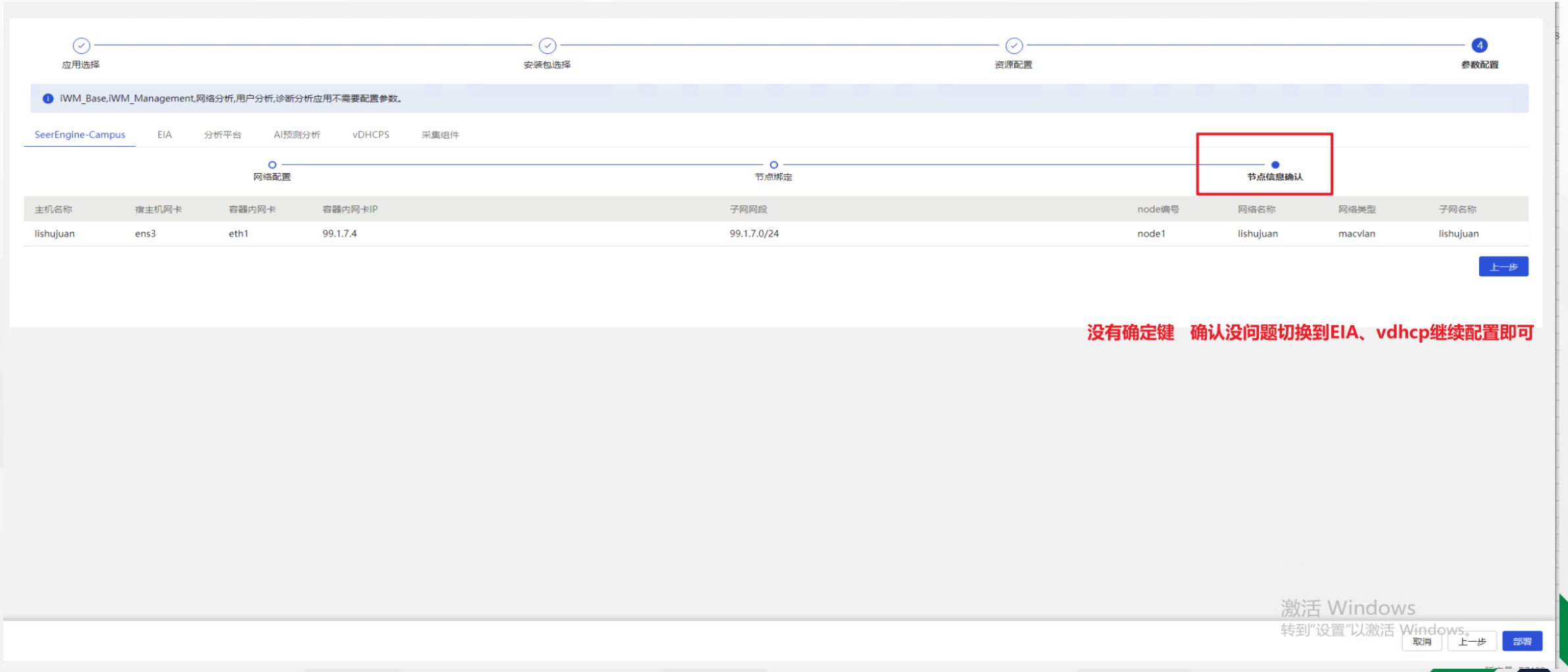
控制器：创建网络、绑定节点、确认信息



部署参数配置

数字化解决方案领导者

控制器：创建网络、绑定节点、确认信息

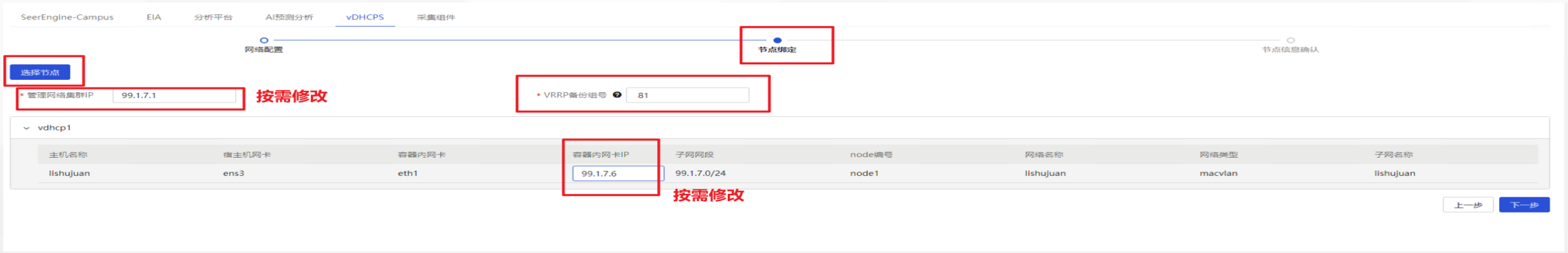


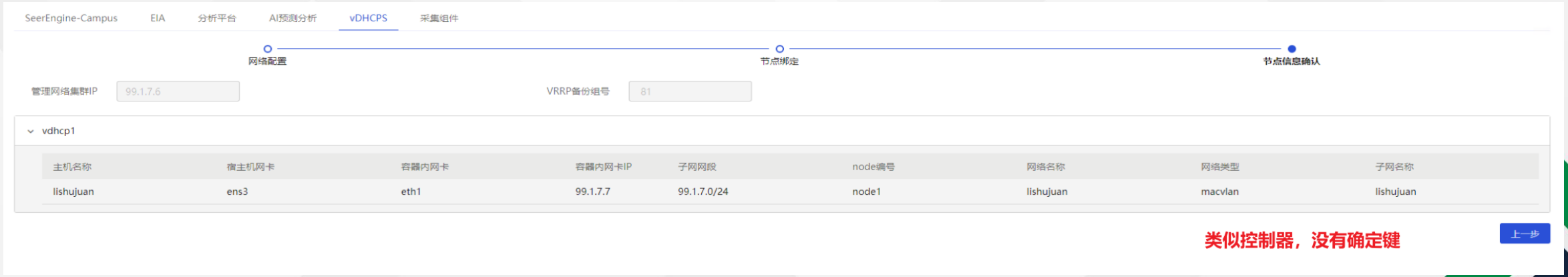
部署参数配置

H3C
数字化解决方案领导者

vdhcp：创建网络（支持选择南向单栈或双栈）、绑定节点、确认信息

IP、备份组号按需修改，不要和已有IP冲突





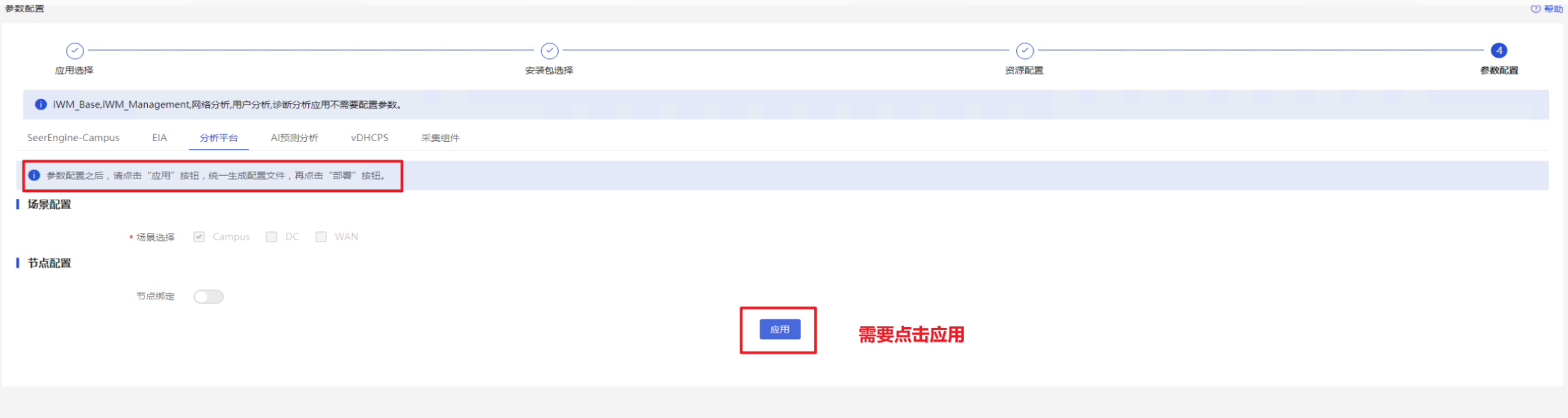
部署参数配置

EIA：节点数大于3时可选绑定节点
需要在本页点击“应用”才能部署

部署参数配置

H3C
数字化解决方案领导者

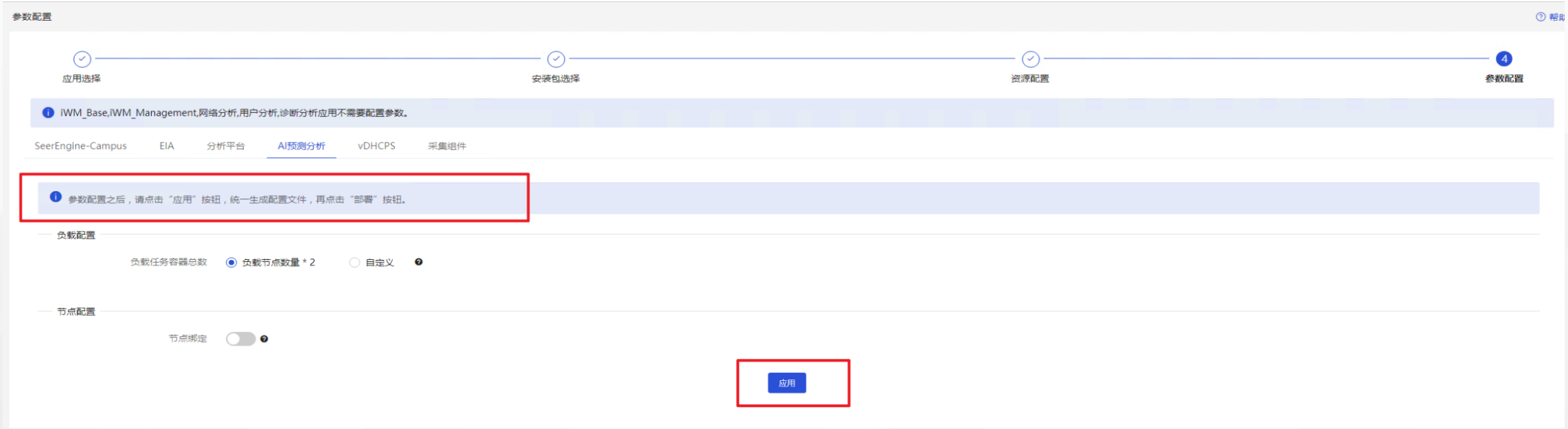
分析平台：需要点应用生效



部署统一数字底盘及应用

H3C
数字化解决方案领导者

分析器AI预测分析：需要点应用生效



部署统一数字底盘及应用

H3C 数字化解决方案领导者

采集组件：

- 节点配置

– 单机模式：采集组件不支持节点绑定，默认部署在Master节点。

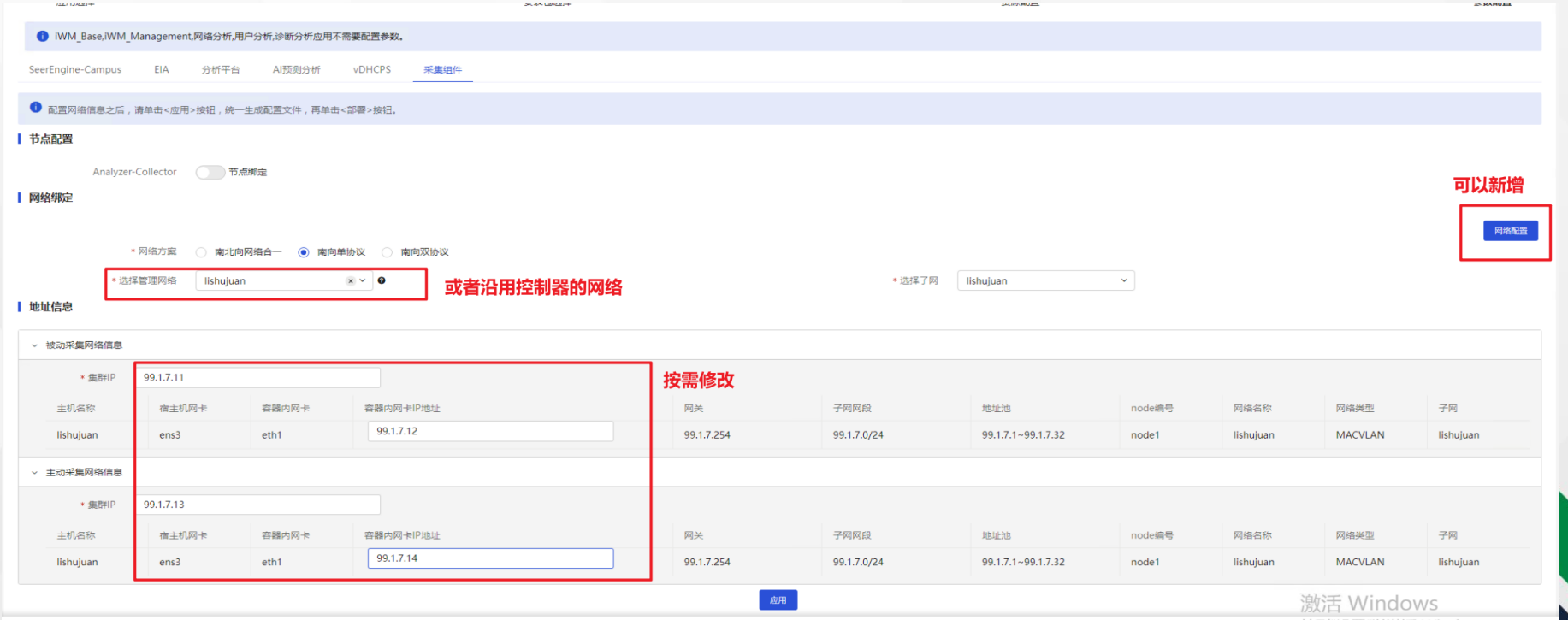
– 集群模式：采集组件支持任选Master或者Worker中的一个或三个节点部署，不启用节点绑定默认部署在Master节点。

- 网络配置

– 南北向网络合一：无需配置网络，直接进行下一步，不推荐使用

– 南向单协议：创建一个IPv4或IPv6网络。

– 南向双协议：创建一个IPv4和一个IPv6网络。



部署统一数字底盘及应用

H3C 数字化解决方案领导者

在各组件的参数配置页面配置完参数并点击<应用>按钮以后，单击<部署>按钮，部署组件。

注意事项

园区场景单机融合部署控制器和分析器时:

单机部署园区管控析产品：统一数字底盘+NSM+vDHCP+SeerEngine+EIA+iWM+SeerAnalyzer，微服务数量会超过规格限制(300个)，需要对Kubernetes启动参数进行调整至400个。具体操作：

(1) 首先确认当前单机环境已部署Matrix，且系统运行正常。

(2) 进入后台命令行，编辑Kubernetes的配置文件：

vi /etc/systemd/system/kubelet.service.d/10-kubeadm.conf

将--max-pods=300改为--max-pods=400

```
[Service]
Environment="KUBELET_KUBECONFIG_ARGS=--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf --kubeconfig=/etc/kubernetes/kubelet.conf"
Environment="KUBELET_SYSTEM_PODS_ARGS=--pod-manifest-path=/etc/kubernetes/manifests --pod_infra_container_image=matrix-registry.h3c.com:8088/matrix/pause:3.4.1"
Environment="KUBELET_NETWORK_ARGS=--network-plugin=cni --cni-conf-dir=/etc/cni/net.d --cni-bin-dir=/opt/cni/bin"
Environment="KUBELET_DNS_ARGS=--cluster-dns=10.96.0.10 --cluster-domain=cluster.local --resolv-conf=/opt/matrix/k8s/conf/dns/resolv.conf"
Environment="KUBELET_AUTHZ_ARGS=--authorization-mode=Webhook --authentication-token-webhook=true --client-ca-file=/etc/kubernetes/pki/ca.crt"
Environment="KUBELET_CGROUP_ARGS=--cgroup-driver=systemd --system-reserved=cpu=1,memory=6Gi"
Environment="KUBELET_CERTIFICATE_ARGS=--rotate-certificates=true --cert-dir=/var/lib/kubelet/pki"
Environment="KUBELET_EXTRA_ARGS=--feature-gates=EphemeralContainers=true --fail-swap-on=false --node-labels=kubernetes.io/hostname=lishujuan,node=node1,master=m
aster1,role=master --node-ip=99.1.7.2 --max-pods=400 --tls-cipher-suites=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECD
HE_ECDSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305"
Environment="KUBELET_LOG_ARGS=--v=2 --logtostderr=true"
ExecStart=
ExecStart=/bin/sh -c "/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS $KUBELET_SYSTEM_PODS_ARGS $KUBELET_NETWORK_ARGS $KUBELET_DNS_ARGS $KUBELET_AUTHZ_ARGS $KUBELET_C
ADVISOR_ARGS $KUBELET_CGROUP_ARGS $KUBELET_CERTIFICATE_ARGS $KUBELET_EXTRA_ARGS $KUBELET_LOG_ARGS 1>>/var/log/matrix-diag/Matrix/kubelet/kubelet.log 2>&1"
~
~
```

(3) 保存配置文件之后，重启kubelet服务即可生效

systemctl daemon-reload && systemctl restart kubelet

H3C
数字化解决方案领导者

目录

H3C
数字化解决方案领导者

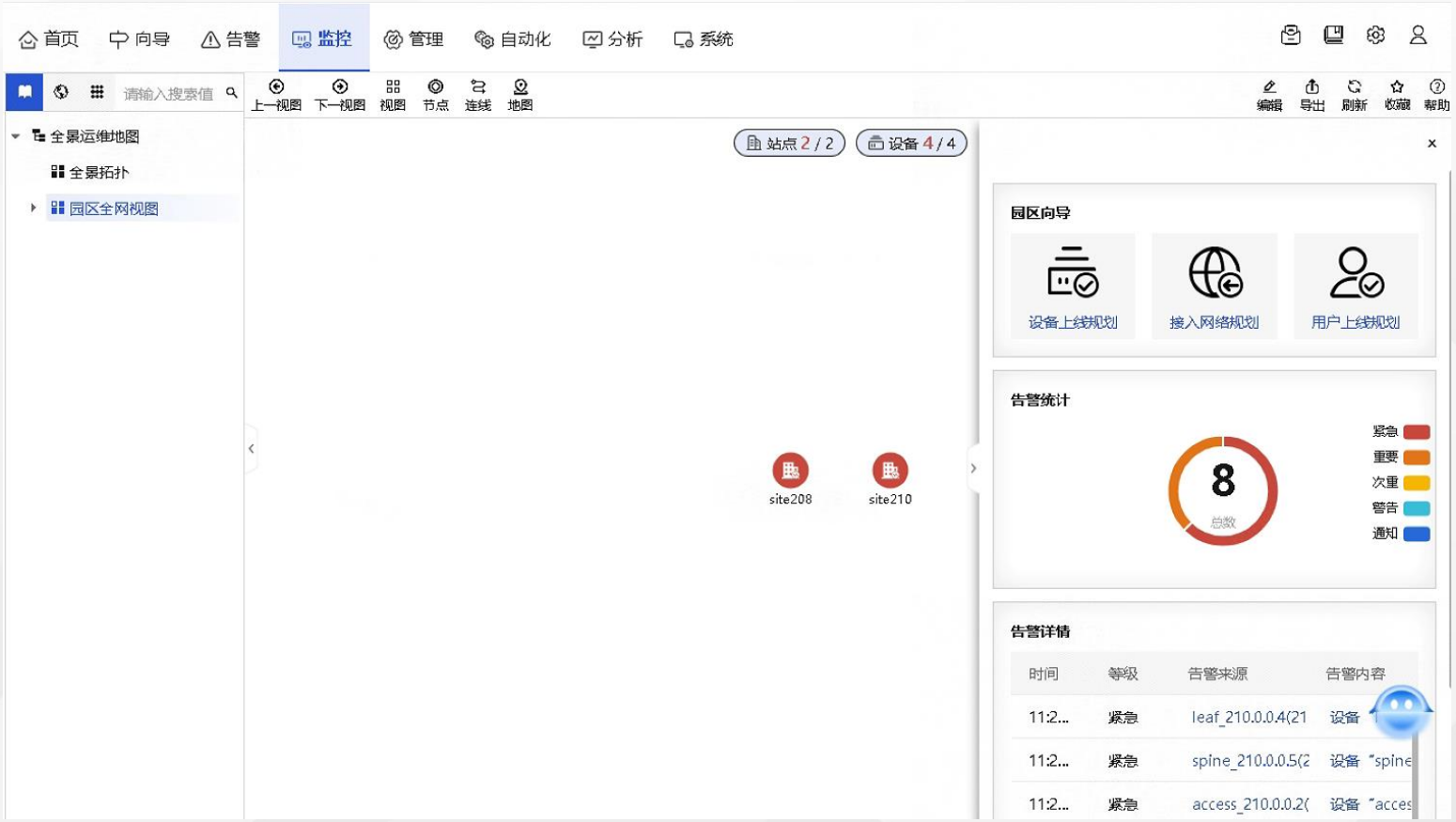
全景运维地图

全景运维地图简介

- 全景运维地图：全景运维地图支持对全网资源进行拓扑展示和编排，提供右键快捷菜单，并展示资源告警情况，设备上下线状态，链路Tip等信息。运维人员可以通过全景运维地图入口直观的了解整个网络环境的运行状态并进行排障处理。
- 需要安装CMDB和NSM_TOPO组件
- 点击【监控】默认展示全景运维地图的全景拓扑，包括控制组件上创建的所有站点，融合部署场景会展示通过不同控制组件创建的站点

园区全网视图

- ADCampus控制组件上创建的fabric绑定站点后，会创建园区全网视图。侧拉栏页签支持隐藏。
  - 园区向导：提供设备上线规划、接入网络规划、用户上线规划的一键跳转配置功能。
  - 告警统计：展示园区所有站点的资源告警信息级别和总数。
  - 告警详情列表：展示资源告警详情，支持选中跳转。



站点TIP

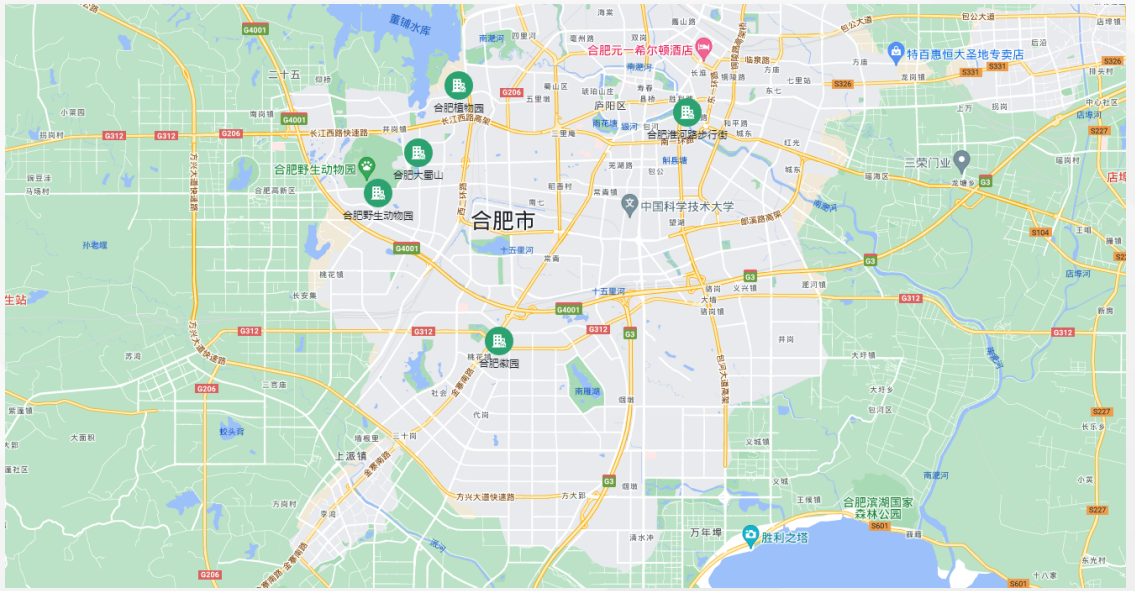
■ 左键单击站点，展示该站点下的关键信息，包含告警、Fabric、设备、告警信息等。

节点颜色以告警级别进行标示，若最高告警为紧急告警则置为红色，若最高告警为重要告警则置为橙色。

- 关注告警：展示当前站点的最高等级的告警信息，如果最高等级的告警信息有多条，则展示最新的告警信息。
- Fabric：展示园区当前站点下的Fabric信息，支持跳转至Fabric配置页面。
- 设备：展示当前站点下的设备类型以及设备数量。
- 告警信息：展示当前站点下的告警类型以及告警数量，支持跳转至告警页面进行处理。

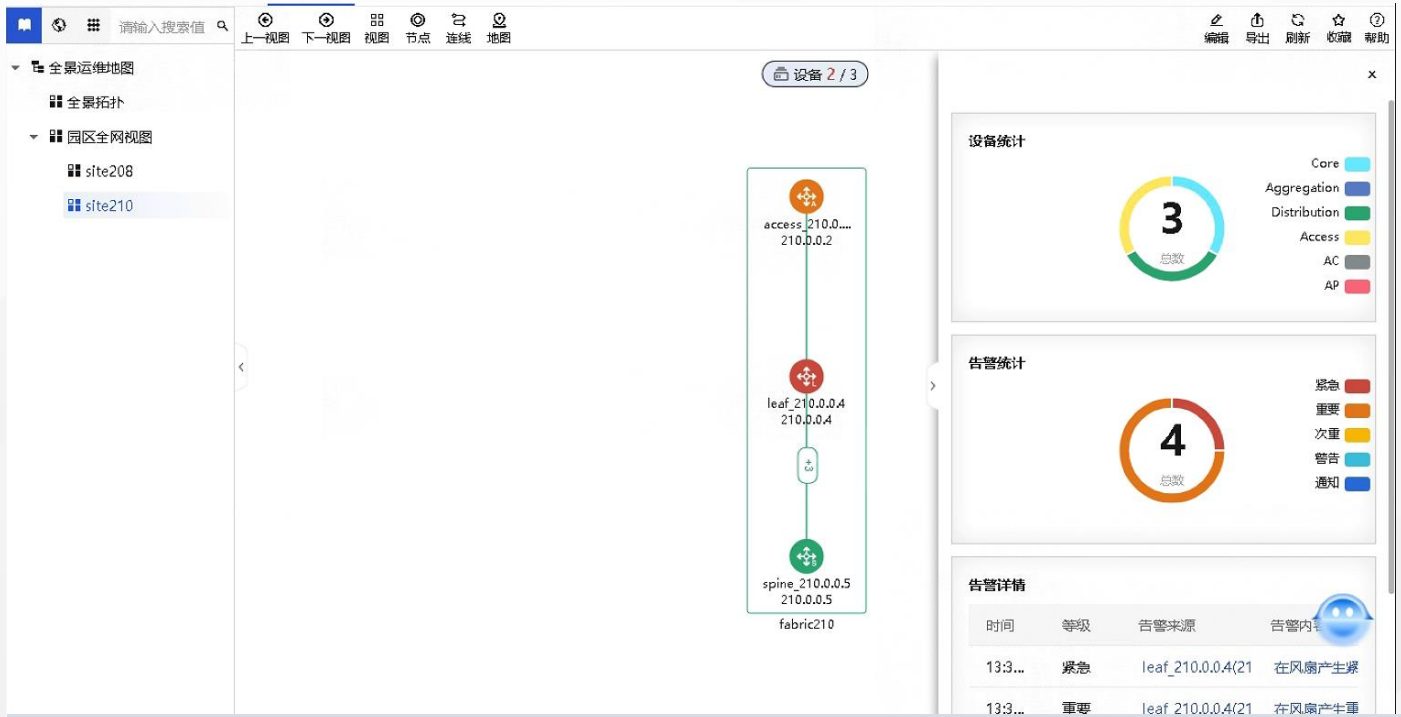
GIS地图设置

- GIS地图设置坐标可以精确到经纬度。 需要客户申请键值才能使用。



站点视图

- 若该站点被多个Fabric绑定，会展示该站点下绑定的所有fabric及对应设备



- 站点视图的fabric tip

Tip

■ 站点视图的设备tip

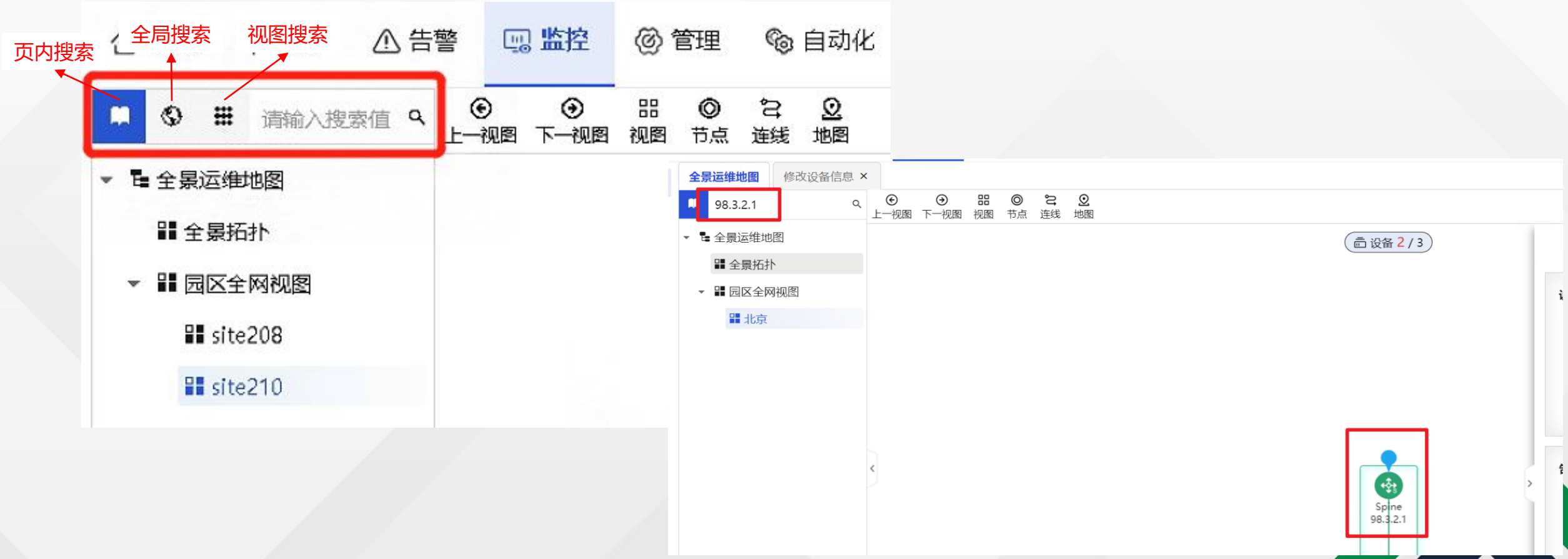
■ 在线用户tip

■ 操作步骤

- 下载putty.zip，并解压到C盘。即C:\putty\路径下有putty.bat，putty.exe，putty.reg三个文件。
- 双击运行C:\putty\putty.reg文件。
- 单击设备对应操作列的Telnet设备图标或者SSH设备图标，弹出确认对话框。
- 单击<打开putty.bat>按钮，弹出窗口。

搜索逻辑

- 页内搜索：搜索当前页的数据，如下图搜索site210页内的设备、IP等，搜不到site208的信息
- 全局搜索：在全景拓扑和园区全网视图下进行内容搜索
- 视图搜索：只能搜索站点视图名称，不能搜索视图下的设备。如果想搜索视图、fabric、设备或者用户等，切到全局搜索下进行搜索。



控制器数据一致性检查

数据一致性检查介绍

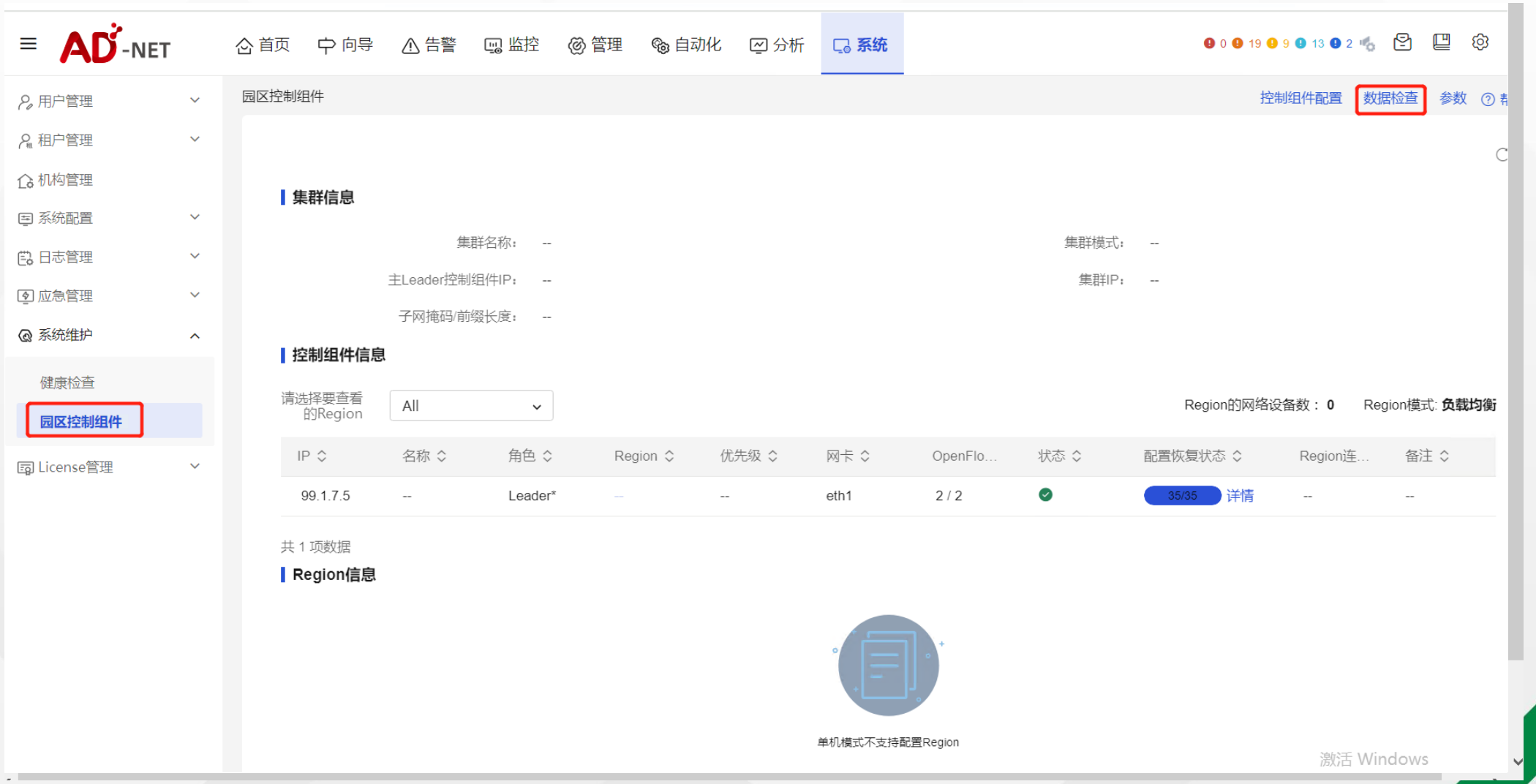
- 当前园区控制组件支持数据一致性比较，会对主备节点数据库数据进行比较。针对的场景主要是升级或者主备倒换等，切主之后可以通过这个功能去对各节点的数据进行检查。
- 实际业务中有的表字段可能因为升级场景或者使用方式发送改变，差异结果对控制器业务无影响，但是数据一致性检查会检查出差异。
- 针对上述情况，支持用户对没有业务影响的表或者字段添加到白名单中。增加到白名单中的表和属性列不再参与数据一致性比较

- 局限性：当前只支持控制器的数据一致性检查（如安全组、私有网络等），但EIA/vDHCP还未合入

数据一致性检查界面

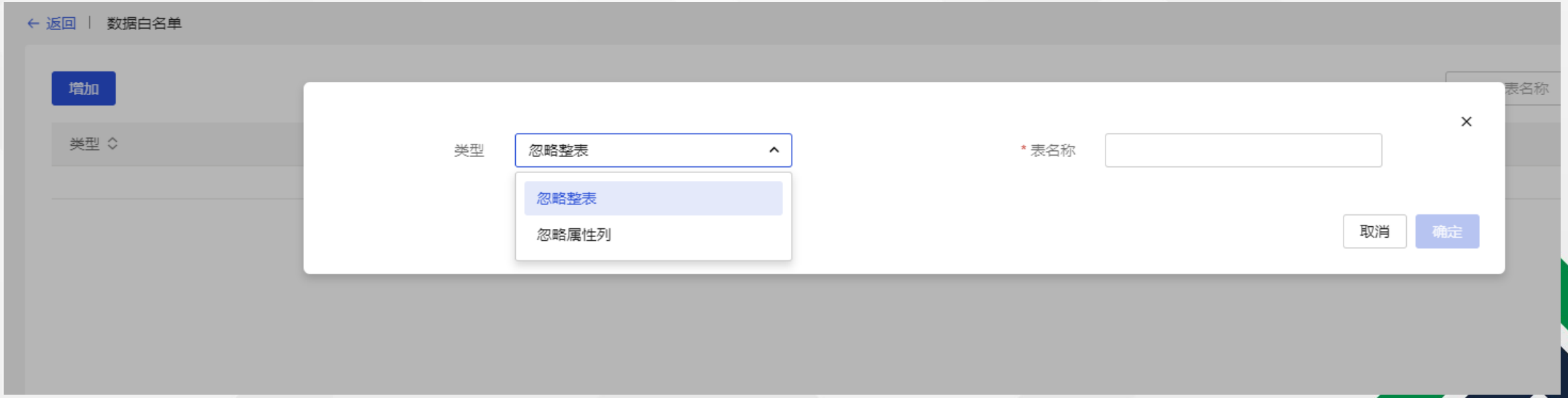
H3C
数字化解决方案领导者

- 功能入口



数据一致性检查界面

- 检查效果：一致会绿灯，不一致会红灯



支持展示离线ONU

支持展示离线ONU

- 背景：原有场景下控制器界面只展示最近的ONU。部分局点通过Campus控制器从网管同步过来ONU之后，客户验收需要在平台上看到纳管了多少的ONU，多少在线多少不在线，因为环境限制没法把所有ONU都上线，所以控制器上始终只能看到不全数量的ONU。

- 新版本合入了可以同步离线ONU的特性，并且将保留原有的离线ONU的上线位置，只要上线过都可以看到。如果存在一个ONU迁徙端口，也可以同时保留两条记录。即：ONU换位置上线不删除原位置ONU，支持不同ONU绑定同一MAC

效果展示

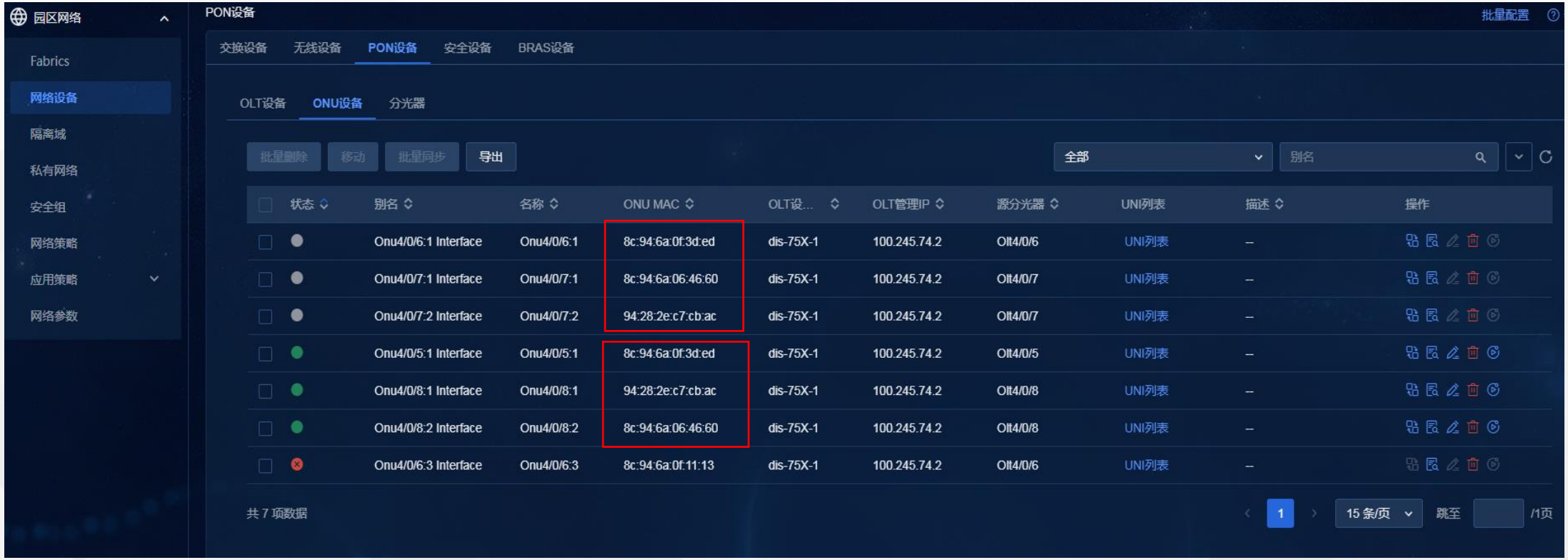
支持同步离线ONU到控制器

点击同步，OLT设备会把绑定了MAC的ONU（包括在线和离线）从网管侧同步到控制组件

效果展示

H3C
数字化解决方案领导者

ONU换位置上线不删除原位置ONU，支持不同ONU绑定同一mac



目录

H3C
数字化解决方案领导者

逃生权限保持

逃生权限保持

- 背景：

部分金融局点对用户的权限有强管控，不允许逃生的时候，所有的终端都用同一个网段的地址，希望仍能保持原有业务IP。

- 实现效果

802.1x/mac认证用户上线后，设备本地缓存记录服务器授权关键信息，进入逃生时使用缓存的信息授权给用户，使用户仍用原先业务网段IP上线。全新上线终端查不到缓存表项按正常逃生流程进入critical vxlan，获取逃生网段IP。

- 手工配置（仅支持在XC设备上手配，控制器暂不支持下发，预计Q4合入）
  - Radius配置
- 认证表项查看
  - 802.1X认证
  - MAC认证
  - 逃生权限保持
- 注意事项

手工配置

- Radius配置

开启AAA用户授权信息缓存功能。
<Sysname> system-view
[Sysname] aaa authorization-cache enable
#

#开启 lan-access用户的RADIUS授权信息缓存功能。
<Sysname> system-view
[Sysname] domain xx（在认证域下配置）
[Sysname-isp-test] authorization lan-access radius-cache enable
#

#配置授权信息缓存的过期时间为10小时。缺省授权信息缓存的过期时间为336小时
<Sysname> system-view
[Sysname] aaa authorization-cache expiry 10
#

修改AAA用户授权信息缓存功能的最大记录条数为8K条。
<Sysname> system-view
[Sysname] aaa authorization-cache number 8000
#

aaa authorization-cache expiry x取值范围为0~2147483647，单位为小时。过期时间取值为0时，表示用户的授权信息缓存不会老化。即上过线的用户无论在离线多久，在eia故障时都可以继承原来的权限继续业务访问。

表项查看

- 802.1X认证

正常802.1X用户认证表项

```
[fabric1-fs55-1]dis dot1x connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-d8d6
Access interface: Bridge-Aggregation2
M-LAG NAS-IP type: Peer
M-LAG user state: Inactive
Username: hz-cw1
User access state: Successful
Authentication domain: campus
IPv4 address: 12.1.0.6
IPv4 address source: IP Source Guard
EAP packet identifier: 2
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 141
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: vsi5
Authorization microsegment ID: N/A
```

802.1X认证之后认证点设备自动生成一个cache缓存表项
通过display aaa authorization-cache [dot1x | mac-auth | static | web-auth] [mac mac-address]查看

```
User MAC address: 0cda-411d-d8d6
Username: hz-cw1
Access type: 802.1x authentication
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
[fabric1-fs55-1]
```

表项查看

- MAC认证

正常MAC用户认证表项

```
[fabric1-fs55-1]dis mac-au connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-7027
M-LAG NAS-IP type: Local
M-LAG user state: Active
Access interface: Bridge-Aggregation2
Username: 0cda411d7027
User access state: Successful
Authentication domain: campus
IPv4 address: 12.1.0.9
IPv4 address source: IP Source Guard
Initial VLAN: 141
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
```

MAC认证之后认证点设备自动生成一个cache缓存表项
通过display aaa authorization-cache查看

```
[fabric1-fs55-1]dis aaa authorization-cache
Total cache entries: 2

User MAC address: 0cda-411d-7027
Username: 0cda411d7027
Access type: MAC authentication
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
Egress VLAN ID: N/A
Egress VLAN Name: N/A
Authorization ACL number: N/A
Authorization ACL name: N/A
Authorization ACL version: N/A
Authorization user profile: N/A
```

表项查看

- 静态IP用户认证

正常认证表项

```
[fabric1-fs55-1]dis port-security static-user connection
The memory usage has reached or exceeded the early-warning threshold. Please
Memory used/total: 1636836/1946044 KB.
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-b12a
M-LAG NAS-IP type: Peer
M-LAG user state: Inactive
Access interface: Bridge-Aggregation2
Username: 12.1.0.123
User access state: Successful
Authentication domain: static
IPv4 address: 12.1.0.123
IPv4 address source: User packet
Initial VLAN: 141
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
```

认证点设备自动生成一个cache缓存表项
通过display aaa authorization-cache查看

```
[fabric1-fs55-1]dis aaa authorization-cache mac 0cda-411d-b12a
The memory usage has reached or exceeded the early-warning threshold. Pleas
Memory used/total: 1637088/1946044 KB.
Total cache entries: 1

User MAC address: 0cda-411d-b12a
Username: 12.1.0.123
Access type: Static user access
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
Egress VLAN ID: N/A
Egress VLAN Name: N/A
Authorization ACL number: N/A
Authorization ACL name: N/A
Authorization ACL version: N/A
Authorization user profile: N/A

[fabric1-fs55-1]
```

- 使能逃生权限保持后，静态IP认证用户也会生成cache表项，此时逃生是依靠cache表项的。
- 静态IP认证用户的认证域下也需要配置authorization lan-access radius-cache enable

表项查看

- 逃生权限保持

当用户下线后，cache认证表项开始倒计时3小时（倒计时时间可自定义）

```
[fabric1-fs55-1]dis aaa author
[fabric1-fs55-1]dis aaa authorization-cache
Total cache entries: 2

User MAC address: 0cda-411d-d8d6
Username: NW1ZHxpTOy53QU1kLQF0Jzg2++E=  hz-cw1
Access type: 802.1x authentication
Remaining time: 2:57:42 (hh:mm:ss)
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
Egress VLAN ID: N/A
Egress VLAN Name: N/A
Authorization ACL number: N/A
Authorization ACL name: N/A
Authorization ACL version: N/A
Authorization user profile: N/A
```

802.1x

```
<fabric1-fs55-1>dis aaa authorization-cache mac 0cda-411d-b12a
The memory usage has reached or exceeded the early-warning thresho
Memory used/total: 1637332/1946044 KB.
Total cache entries: 1

User MAC address: 0cda-411d-b12a
Username: 12.1.0.123
Access type: Static user access
Remaining time: 2:59:45 (hh:mm:ss)
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi5
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
Egress VLAN ID: N/A
Egress VLAN Name: N/A
Authorization ACL number: N/A
Authorization ACL name: N/A
Authorization ACL version: N/A
Authorization user profile: N/A
```

静态IP用户

表项查看

- 逃生权限保持

radius故障时终端再上线。仍可以获取业务网段IP
接入状态是：critical domain，逃生状态

```
<fabric1-fs55-1>dis dot
<fabric1-fs55-1>dis dot1x  con
<fabric1-fs55-1>dis dot1x  connection
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-d8d6
Access interface: Bridge-Aggregation2
M-LAG NAS-IP type: Peer
M-LAG user state: Inactive
Username: hz-cw1
User access state: Critical domain
Authentication domain: campus
IPv4 address: 12.1.0.8
IPv6 address: 12:1::ACB4:971D:D05B:ED2D
IPv4 address source: IP Source Guard
IPv6 address source: User packet
EAP packet identifier: 3
Authentication method: CHAP
AAA authentication method: RADIUS
Initial VLAN: 141
```

Cache不再倒计时

```
User MAC address: 0cda-411d-d8d6
Username: hz-xz1
Access type: 802.1x authentication
UUID: N/A
AAA authentication method: RADIUS
Authorization VSI: vsi11
Authorization microsegment ID: N/A
Authorization microsegment name: N/A
Authorization VLAN ID: N/A
Authorization VLAN name: N/A
Egress VLAN ID: N/A
Egress VLAN Name: N/A
Authorization ACL number: N/A
Authorization ACL name: N/A
Authorization ACL version: N/A
Authorization user profile: N/A
```

注意事项

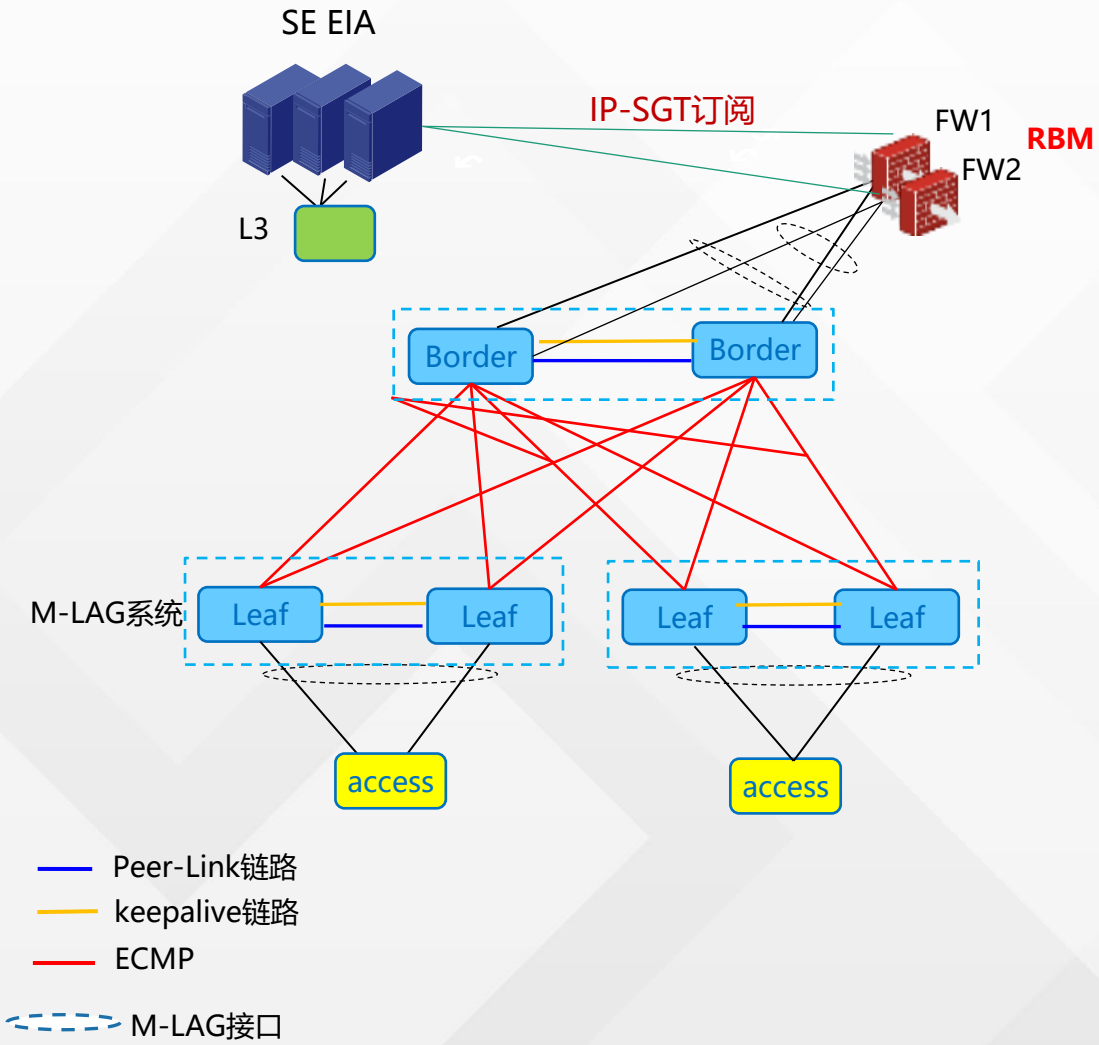
1. 目前此功能只支持在**XC设备上手动配置**，控制器前台预计Q4合入。XGS设备不开发新特性，如果现网有明确需求case by case分析。
2. 逃生权限保持只能在终端**曾经认证过的设备**上进行权限保持。逃生后迁移到其他未认证过的设备上无法进行逃生权限保持。
3. Cache表项仅存在于运行数据库，最大表项限制和设备支持的用户数量一致，**对硬件资源无影响**，可以通过aaa authorization-cache max-number命令进行配置。
4. **如果设备发生重启，则逃生缓存表项会删除。**MLAG场景，两台Leaf中的一台如果重启，则cache表项会丢失，重启完后缓存表项也不会从另一台同步过来，导致重启后只有一半用户可以匹配cache获取原业务网段的IP，另一半会进入普通的逃生。（mlag场景根据奇偶mac分别在两台设备认证）
5. 对MAC PORTAL认证，BYOD用户不会生成缓存表项。
6. 无线认证AC设备暂不支持。
7. 因为逃生权限保持功能在逃生时需要从业务DHCP获取地址，所以该功能在EIA故障时适用，集群故障时（此时vDHCP也故障）不适用。此时需要reset aaa authorization-cache清除缓存的表项，让终端走正常的逃生流程，去逃生DHCP获取逃生网段IP。——理想环境是要求客户使用独立部署的业务DHCP Server
8. **名址绑定场景：**逃生权限保持时无法获取原先的业务IP，因为依赖EIA下发uuid，逃生时EIA异常无法支持 —— 已给设备侧提单，要求认证设备配置逃生权限保持终端上线时能正常记录UUID信息，逃生后地址保持不变，可解决名址绑定场景IP变化问题；短期内需要注意地址池规划，极端情况需要考虑两倍需求。

   非名址绑定场景：逃生后，短时间内终端匹配cache再上线可以获取原先的业务IP，依靠dhcp服务器自己的缓存。

H3C
数字化解决方案领导者

防火墙支持SGT和IP-SGT订阅

防火墙IP-SGT订阅



价值：

在IP-SGT解耦场景下，如果防火墙仍然根据IP地址段做安全策略，防火墙就无法做到安全策略随行。因此引入防火墙IG-SGT订阅方式，实现过防火墙安全策略随行。

早期已支持根墙IP-SGT订阅，本期新增虚墙IP-SGT订阅能力。

适用场景：

单Fabric场景组策略时，跨私网流量过FW时做精细访问控制。（IP-SGT跨园区暂不支持)

连接方式：

FW旁挂：2台FW，FW做RBM（主备模式），跟VRRP联动；Border做M-LAG，通过M-LAG口跟每台FW互连。

防火墙IP-SGT订阅

- 流量引流到FW（SMP组件未适配，需手配）
  - Spine及防火墙上手配，将业务流量引到防火墙，可参考早期“安全融合配置指导”中控制器下发的配置进行类似配置
- FW设备基础配置（SMP组件7.1方案未完成国产化适配，需手配）
  - 业务使用根墙
  - 业务使用虚墙
- EIA配置
  - 订阅配置
- FW上配置基于SGT的安全策略

FW配置

- 业务使用根墙

#配置防火墙的网管口地址

interface GigabitEthernet1/7/0

ip address 50.50.50.1 255.255.255.0

#将管理口加入安全域中

security-zone name Management

import interface GigabitEthernet1/7/0

#配置到统一数字底盘北向IP地址的路由，下一跳是管理交换机的地址。

ip route-static 101.1.0.0 24 50.50.50.200

#配置云连接服务器（即：统一数字底盘）的IP地址

cloud-management server domain 101.1.0.100 //101.1.0.100是统一数字底盘北向IP地址

#使能微分段

microsegment enable //仅需使能微分段功能，不需配微分段ID，微分段和IP对应关系通过EIA推送。

#

#使能IP-SGT订阅功能

ipsgt enable

#

#跨私网流量过防火墙的跨私网路由配置

ip route-static vpn-instance zww 27.0.0.0 22 vpn-instance aaa 100.3.0.2 //私网zwww到私网aaa的静态路由，其中27.0.0.22是Fabric内私网aaa的网段，下一跳是在目的私网，100.3.0.2是Spine设备接口地址

ip route-static vpn-instance aaa 80.20.1.0 24 vpn-instance zww 100.3.0.10 //私网aaa到私网zww的静态路由，其中80.20.1.0是Fabric内私网zww的网段，下一跳是在目的私网，100.3.0.10是Spine设备接口地址

#

FW配置

- 业务使用虚墙

#先创建虚墙，并将虚墙要用的管理口和业务口（业务口的数量请根据实际使用场景选择）加到该虚墙：

```
context test2 id 2 vlan-unshared  //创建context ID为2，名为test2的虚墙
 context start
 allocate interface GigabitEthernet1/7/0 share   //管理口
 allocate interface Route-Aggregation10 share    //业务口
 allocate interface Route-Aggregation20 share    //业务口
```

#创建完虚墙后，要进入虚墙配置管理口，并将管理口加入安全域中：

```
RBM_P[FW5K-1]switchto context test2
RBM_P<H3C>
#
interface GigabitEthernet1/7/0
 ip address 50.50.50.2 255.255.255.0
#
security-zone name Management
 import interface GigabitEthernet1/7/0
#
```

#配置到统一数字底盘北向IP地址的路由，下一跳是管理交换机的地址。

```
ip route-static 101.1.0.0 24 50.50.50.200
#
```

#配置云连接服务器（即：统一数字底盘）的IP地址，后续建立websocket连接，依赖websocket下发配置

```
cloud-management server domain 101.1.0.100  //101.1.0.100是统一数字底盘北向IP地址
#
```

FW配置

- 虚墙配置.续

#使能微分段

microsegment enable //需使能微分段功能，不需配微分段ID，微分段和IP对应关系通过EIA推送。

#

#使能IP-SGT订阅功能

ipsgt enable

#

#跨私网流量过防火墙的跨私网路由配置

ip route-static vpn-instance zww 27.0.0.0 22 vpn-instance aaa 100.3.0.2 //私网zwww到私网aaa的静态路由，其中27.0.0.22是Fabric内私网aaa的网段，下一跳是在目的私网，100.3.0.2是Spine设备接口地址

ip route-static vpn-instance aaa 80.20.1.0 24 vpn-instance zww 100.3.0.10 //私网aaa到私网zww的静态路由，其中80.20.1.0是Fabric内私网zww的网段，下一跳是在目的私网，100.3.0.10是Spine设备接口地址

#

EIA配置

- 订阅配置

- EIA手动启用IP-SGT业务

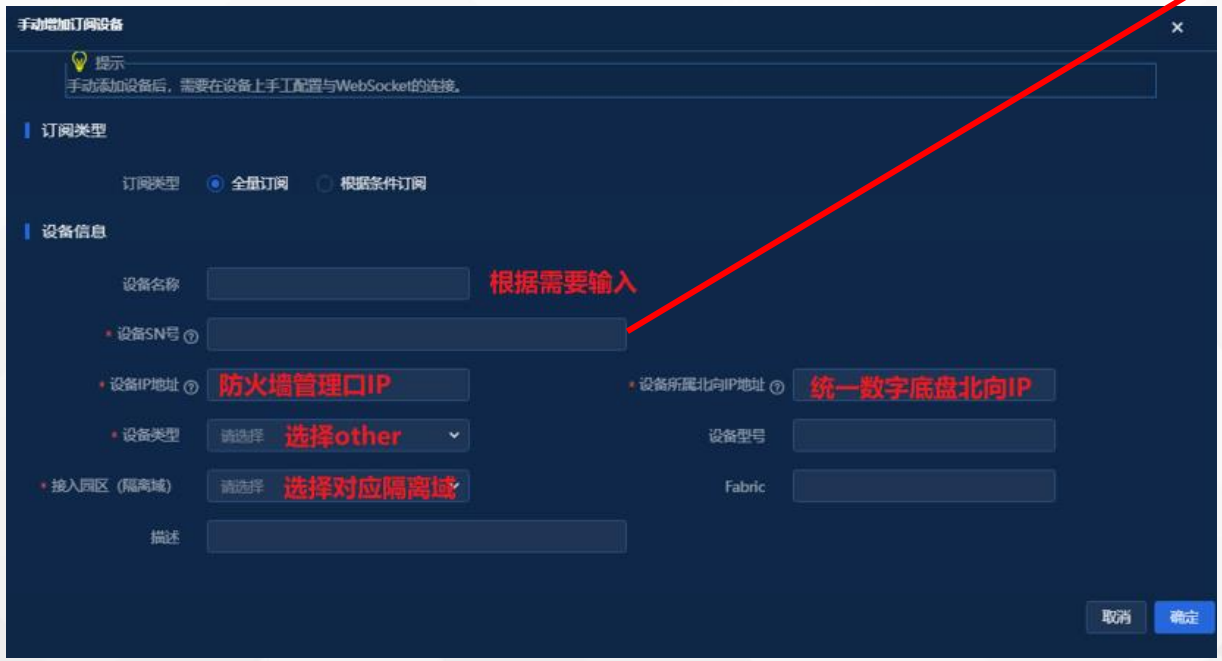
（用户上线后，EIA会向订阅设备发送上线用户的IP-SGT信息。设置为“禁用”，则关闭IP-SGT业务，EIA不再发送上线用户信息给订阅设备。）

- IP-SGT HA用于IP-SGT分级，当前防火墙不支持

EIA配置

- 订阅配置

手工增加FW或vFW订阅设备



- 设备 SN 号：如果是根墙，通过 display device manuinfo 获取防火墙的 SN；对于框式防火墙，用框的 SN。如果是虚墙，通过 display device manuinfo 查看 Serial Number in Contex 1 显示的 SN，虚墙的 SN 等于 Serial Number in Contex 1+context id-1，其中 context id 是创建虚墙时所使用的 context ID，或通过 display context 查看虚墙的 SN。

```
RBM_P[FW5K-1]display device manuinfo
 Slot 1 CPU 0:
 DEVICE_NAME           : SecPath F5060
 DEVICE_SERIAL_NUMBER  : 210235A1XYB20C000003
 MAC_ADDRESS           : 9429-2FFC-7EE8
 MANUFACTURING_DATE    : 2020-12-12
 VENDOR_NAME           : H3C
Serial Number in Contex 1:210235A1XY94292FFC7EF0

RBM_P[FW5K-1]display context
ID      Name            Status      Description
1       Admin           active      DefaultContext
2       test2           active      //虚墙 test2 的 context id 是 2

Total contexts:2
```

IP-SGT通道建立后，防火墙可以通过EIA获取订阅信息。

```
RBM_P[FW5K-1]display ipsgt map
Total IPv4 IP-SGT entries: 10
 Microsegment ID: 3509
 IPv4 address          VPN instance
 92.20.1.2             mnt
 92.20.1.3             mnt
```

FW上基于SGT的安全策略配置

H3C 数字化解决方案领导者

可根据实际需求配置基于SGT的安全策略，支持防火墙上手配，或通过web页面配置，以跨私网和内网到外网的安全策略配置为例：

跨私网的安全策略

```
#
security-policy ip
rule 402 name mnt
  action pass
  logging enable
  counting enable
  vrf mnt       //VRF是报文源IP地址所在的私网
  source-microsegment 3509        //报文源IP地址所属的SGT
  destination-microsegment 3545        //报文目的IP地址所属的SGT
#
```

配置内网到外网的安全策略

```
security-policy ip
 rule 403 name mnt-out
  action pass
  logging enable
  counting enable
  vrf mnt        //VRF是报文源IP地址所在的私网
  source-microsegment 3520       //报文源IP地址所属的SGT，目的SGT不配，表示匹配任意目的
#
```

FW上基于SGT的安全策略配置

- 基于SGT安全策略.续

如果需要匹配某些特定外网地址，可以配置静态微分段，关联对应的网段：

```
microsegment 65535
  member ipv4 192.168.91.0 255.255.255.0 vpn-instance gx //外网从共享私网接入，故外网网段192.168.91.0/24要关联共享私网gx
```

或者配置地址对象组，目的地址使用

```
object-group ip address out
 0 network subnet 192.168.91.0 255.255.255.0
```

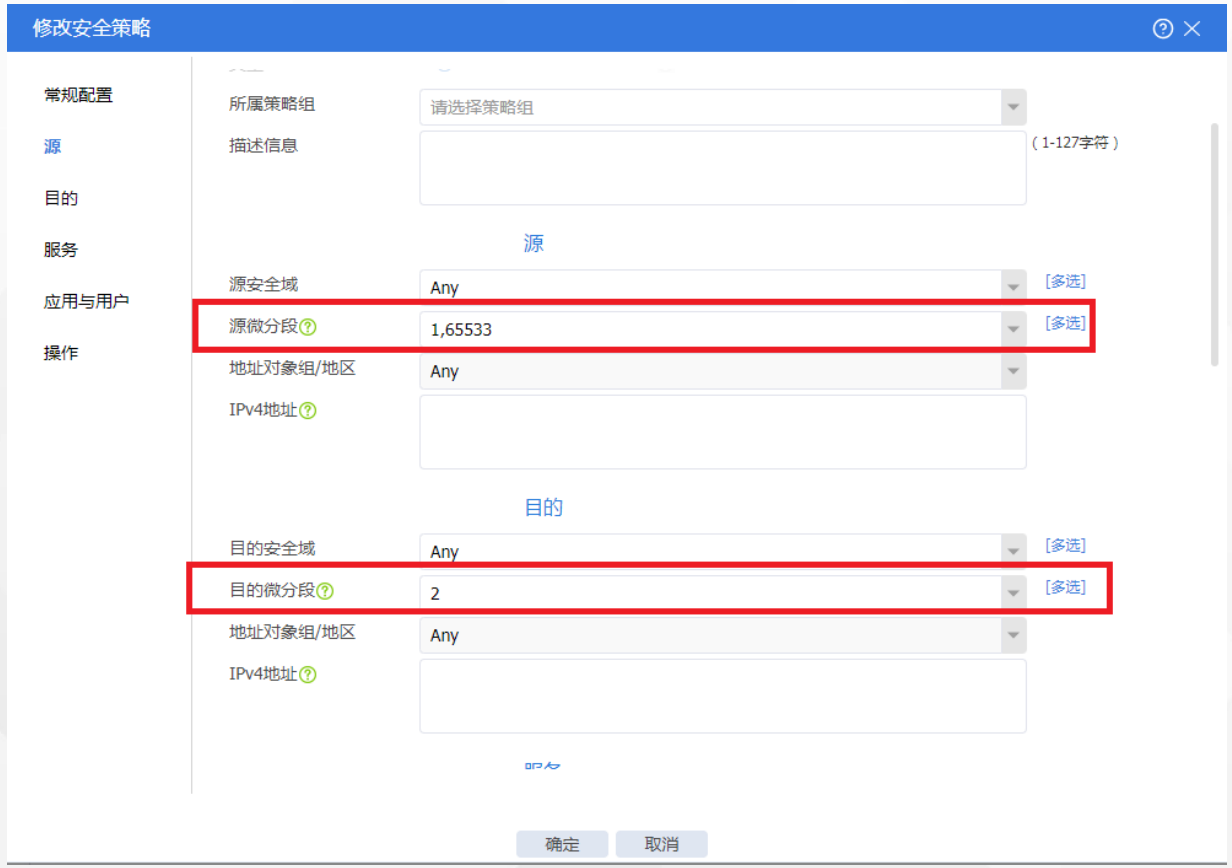
配置内网到某些特性外网的安全策略如下：

```
#
security-policy ip
 rule 403 name mnt-out
  action pass
  logging enable
  counting enable
  vrf mnt
  source-microsegment 3520
  destination-microsegment 65535   //目的SGT是特性外网网段
```

FW上基于SGT的安全策略配置

H3C 数字化解决方案领导者

Web页面上基于微分段做安全策略



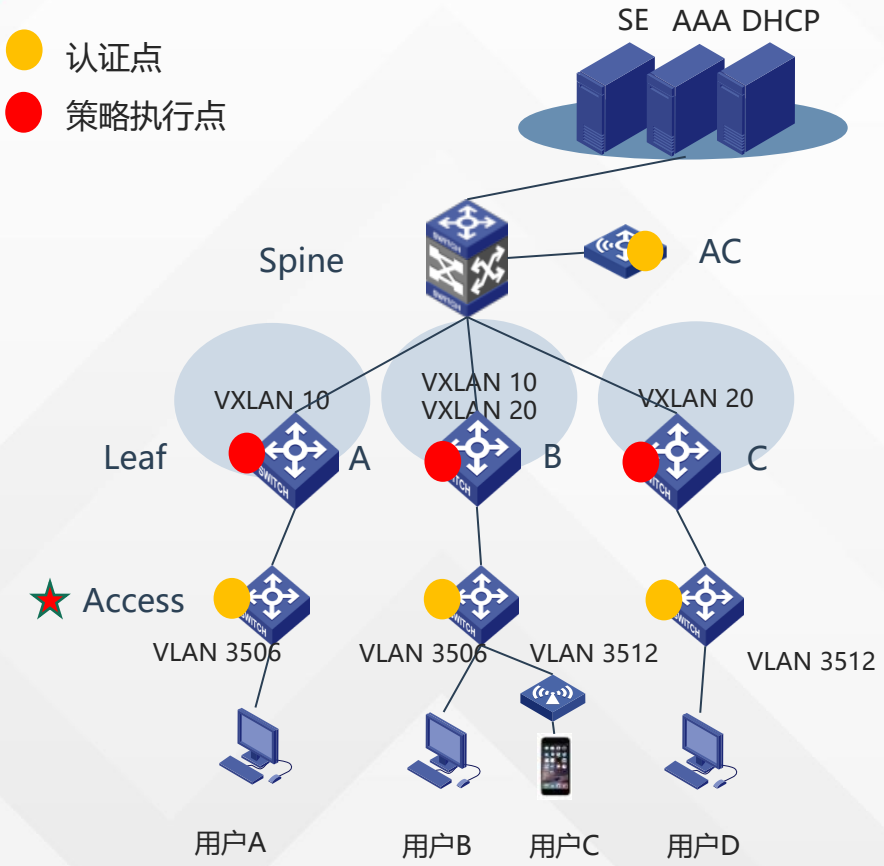
注意事项

- FW不支持EIA故障逃生
- 该特性涉及的FW配置要手配或通过FW的Web界面配
- 仅支持F5000-AI-20/40，F5060和M9006，其中M9006不支持context IPSGT
- 由于FW都是软转，故FW没有IP-SGT按需下发功能
- 当前仅支持单fabric场景，不支持跨园区的过墙策略随行
- FW是旁挂模型，业务引流FW的配置需手配（注意：跨私网流量过FW涉及的跨私网路由不能用下一跳是Loopback的方式，下一跳IP地址要直接指向Spine设备接口地址）

H3C
数字化解决方案领导者

VxLAN组网的AAA解耦方案

VXLAN组网的AAA解耦方案



安全组	二层网络域	网络范围	用户
VLAN 3506	VXLAN 10	leaf A、leaf B	用户A、用户B
VLAN 3512	VXLAN 20	leaf B、leaf C	用户C、用户D

组网特点： VXLAN组网下AAA解耦。

认证点下移到Access设备，用户认证通过后授权安全组vlan，在leaf上映射到VXLAN实现业务随行。

适用场景：

- **互联网/金融/医疗**等行业：客户有自研或已采购第三方认证系统，仅希望通过AD-Campus实现underlay、overlay网络自动化部署，并实现网随人动、业务随行。
- **公安行业**：认证点下沉到接入，但VXLAN网关仍然保留在Leaf，实现认证点与网关分离。
- **网络运维与准入控制**，部门分管的场景。

已开局项目：小米、百度园区

方案价值：

- **解耦AAA，无需适配对接，即可实现VXLAN组网业务随行**
- VXLAN组网覆盖范围更广，**摆脱AAA依赖**

VXLAN组网的AAA解耦方案

H3C
数字化解决方案领导者

配置思路及流程--控制器已有功能下的最佳实践

1、开启“AP本地转发”，并将leaf下行口添加到AP非直连-Leaf接口组中，让leaf下行口下发静态服务实例及免认证vlan
此时终端在leaf上不需要做认证，直接通过网关去进行转发

```
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 3504 to 3511 4090 4093 to 4094
 port-security free-vlan 1 3504 to 3511 4090 4093 to 4094 //VLAN免认证
 #
  service-instance 3506   //无线业务静态服务实例
  encapsulation s-vid 3506 //匹配授权VLAN
  xconnect vsi vsi6 microsegment 3506 //映射业务VSI和组策略微分段
  arp detection trust
  ipv6 nd detection trust
 #
  service-instance 4093 //用于无线管理网
  encapsulation s-vid 4093
  xconnect vsi vsi4093
  arp detection trust
  ipv6 nd detection trust
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
```

VXLAN组网的AAA解耦方案

H3C
数字化解决方案领导者

2、通过【通用策略组-策略模板】给access下发接口及全局认证配置，实现认证点挪移到access上。第三方认证平台上，把access设置为接入设备

全局配置

```
#
 radius session-control enable
 radius session-control client ip 110.0.0.100 key cipher $c$3$/5IOnULUsNaKh6DrK4Wv9H3MkMrfZA==
 radius nas-ip 120.0.1.13     //指定nas-ip，使用4094地址
#
radius scheme radius1
 primary authentication 110.0.0.100
 primary accounting 110.0.0.100
 accounting-on enable send 255 interval 15
 key authentication cipher $c$3$G3nkpzwH+5IbktJwbva/RYZkY1Btdw==
 key accounting cipher $c$3$eGmJWPVilF+d9LfGsJl5s0O0Ss/fRw==
 timer realtime-accounting 15
 user-name-format without-domain
#
domain h3c
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
 domain default enable h3c
#
 dot1x
 dot1x authentication-method eap
#
```

接口配置：

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 300 3501 to 4000 untagged
 port hybrid pvid vlan 300enable //只能用于hybrid
 mac-vlan 口
 port-isolate enable group 1
stp edged-port //手工配置边缘端口
dot1x
 dot1x unicast-trigger
 dot1x guest-vlan 3518          //按需开启guest
 dot1x auth-fail vlan 3519     //按需开启认证失败
 dot1x critical vlan 3505      //按需开启逃生
 dot1x critical eapol
#
```

VXLAN组网的AAA解耦方案

H3C
数字化解决方案领导者

3、认证服务器下发授权vlan，终端正常上线

```
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-1c8b
Access interface: Ten-GigabitEthernet1/0/9
Username: 3506
User access state: Successful
Authentication domain: h3c
IPv4 address: 147.1.0.2
IPv4 address source: User packet
EAP packet identifier: 194
Authentication method: EAP
AAA authentication method: RADIUS
Initial VLAN: 107
Authorization untagged VLAN: 3506
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Authorization temporary redirect: Disabled
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Online from: 2011/03/13 04:25:11
Online duration: 0h 50m 42s
```

VXLAN组网的AAA解耦方案

H3C
数字化解决方案领导者

注意事项：

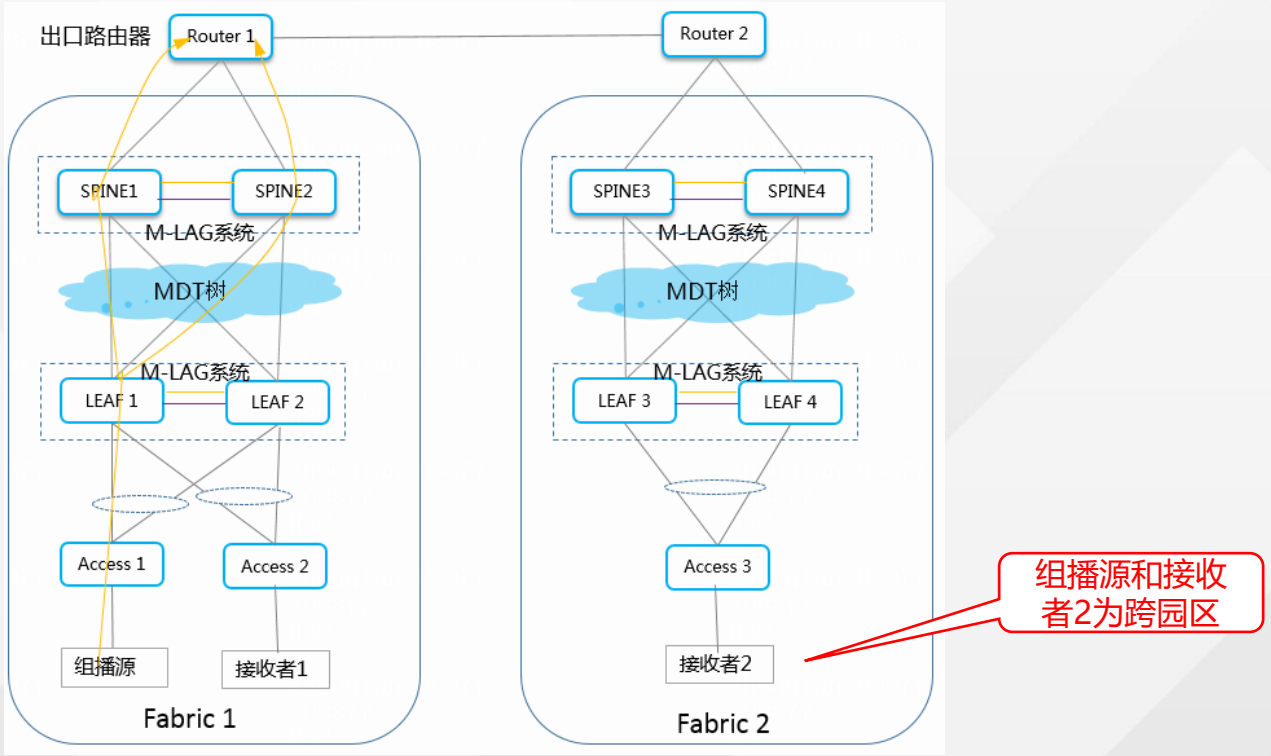
1. 第三方Access作认证需要单独适配，涉及配置均需要手动下发。Access配置审计白名单及认证接口加入保留接口，可避免审计差异。
2. 认证点在接入设备，实质为传统网认证，因此仅支持1x、Mac认证。
3. 要求第三方AAA支持授权VLAN。

H3C
数字化解决方案领导者

VXLAN组播增强

特性增强1 解决多园区双份流问题

- **组网介绍：**多园区组网，组播源和接收者分布在不同园区，Spine（同时是ED角色）做M-LAG
- **存在问题：**Spine1和Spine2都会收到组播流量，并向另一个园区进行发送，导致跨园区组播接收者会收到双份组播流
- **解决方案：**
  - 对于XGS设备，2台Spine间建立IBGP邻居，仅发布10类路由，只让其中1台Spine转发跨Fabric的组播流量（配置需要手配）。
  - 对于XC设备，EVPN组播通过Peer-link链路同步数据（公网和私网组播信息），Spine1和Spine2通过Rlink机制进行ED竞选，竞选成功的ED转发组播流量（XC设备机制实现，不涉及新增命令）。



特性增强1 XGS设备手工增加命令

H3C 数字化解决方案领导者

- 指定本fabric的其他ED设备IP地址

```
#
multicast-vpn vxlan m-lag local 2.1.1.51 remote 2.1.1.52        //remote地址是本fabric的另一台ED设备的IP地址
```

- 2台Spine间需要建立IBGP邻居，通过配置路由策略，仅发布10类路由，对于每个组播流仅有1台Spine转发跨Fabric的组播流量，不同的组播流根据设备的机制自动在不同spine上转发，实现负载分担。

```
#
route-policy policy1 permit node 0
 if-match route-type bgp-evpn-s-pmsi //匹配10类路由
#
route-policy policy1 deny node 1
#
bgp 100
 non-stop-routing
 router-id 2.1.1.51
 peer 2.1.1.52 as-number 100
 peer 2.1.1.52 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  nexthop evpn-m-lag group-address
  peer 2.1.1.52 enable
  peer 2.1.1.52 route-policy policy1 export
```

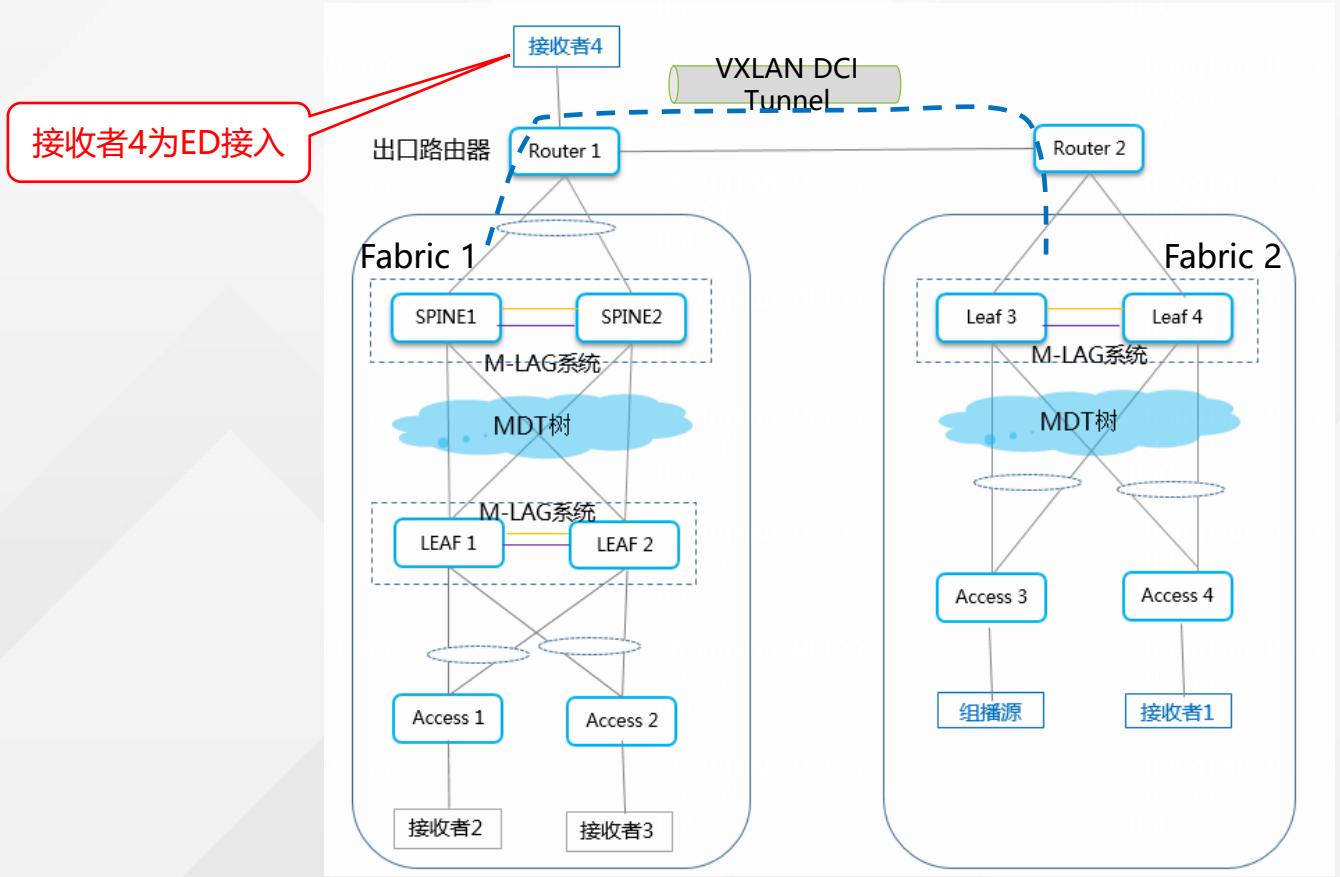
- BGP EVPN中，单播靠2/3/5类路由，组播主要用到6类和10类路由。
- 6类路由：用于接收者侧决定接收哪些流量。
- 10类路由：用于建立MDT树，控制组播流量沿着什么样的路径转发。

特性增强2 组播源和接收者可以从ED接入

H3C 数字化解决方案领导者

■ **组播源/接收者接在ED的场景：**

- 组播源和接收者从ED接入，支持VLAN或VSI接入。
- 组播原理跟多园区组播类似：Leaf3和4的本地私网组播表项，出接口是私网L3VNI口。收到组播报文后，做单播VXLAN封装，通过DCI隧道发给Spine1或2 。
- ED之间实隧道改虚隧道，如果用实隧道还需要用策略路由配合。（仅XGS涉及该问题，需要手动增加命令）

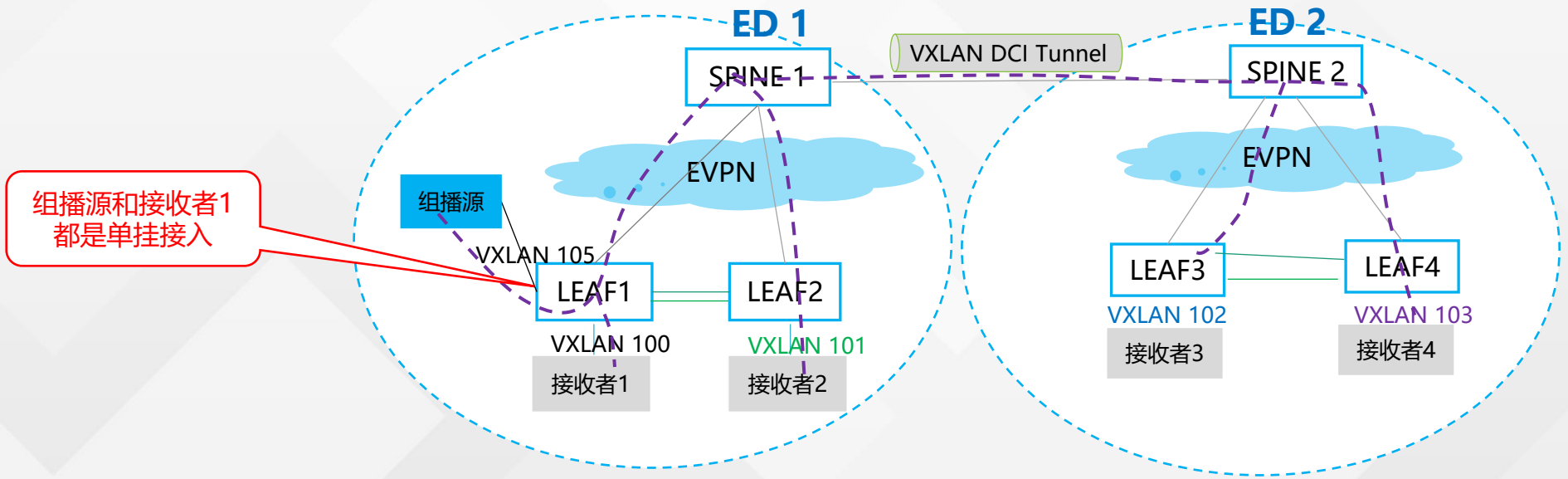


特性增强3 组播源和接收者单挂接入

数字化解决方案领导者

■ **组播源/接收者单挂接入LEAF/ED，当前仅XC款型支持**

- Access设备仅接入M-LAG系统的其中一台M-LAG设备，则该access设备称为单挂设备，组播源和接收者通过access设备接入，则此时组播源和接收者是单挂接入。
- 组播源和接收者直接连接在M-lag系统的一台设备上



组播场景注意事项

- 组播源和接收者可以同fabric或者跨fabric，但需要相同VPN，即单隔离域多Fabric、单vpn拉通场景，不支持跨VPN复制；
- 当组播报文经过组播VXLAN隧道时，有部分类型单板（SG/FD/FE类型）要求经过组播VXLAN隧道的接口和以VLAN方式连接的接口不能在同一块单板上，需要跨板转发。（产品限制）
- 多Fabric组网下，组播源和接收者仅支持从Access接入。M-LAG组网下，每个Fabric的两台ED之间要配置IBGP邻居，只发送10类路由，用于解决接收者会收到双份流问题，这部分配置当前要手配。（仅XGS款型要求）
- M-LAG组网下，仅XC款型支持组播源和接收者单挂接入。
- 不支持Spine-Aggr-Leaf组网下的组播。
- 5560X/6520X不支持M-LAG组网下的组播。
- 要求先配置二层组播，再配置三层组播。
- 目前组播业务不支持IPv6。

H3C
数字化解决方案领导者

企业微信认证

支持企业微信认证

- **单栈场景：MAC-Portal支持企业微信认证**

有线和无线仍然使用ACL 3001并配置域名过滤。
备注：（1）有线已经支持配置域名
（2）AC已支持（集中式转发），**AP已支持**。
（本期新增本地转发场景AP配置acl加域名，不需要认证点上移）

- **双栈场景：MAC-Portal支持企业微信认证**

备注：（1）有线使用ACL 5001，已经支持配置域名。
（2）无线仍然使用ACL 3001并配置域名过滤。
AC已支持（集中式转发），**AP已支持**（本地转发）。

```
#
 object-group ip address weixinyuming
  30 network host name open.work.weixin.qq.com vpn-instance vpn-default
  略...
  220 network host name gap.work.weixin.qq.com vpn-instance vpn-default
#
#
 acl number 5001
   rule 0 permit udp destination-port eq dns
   rule 1 permit ip destination 172.29.223.5 0  //IPv4 EIA地址
   rule 2 permit ipv6-protocol ipv6 destination 2400:DD0D:1001:104::9/128 //IPv6 EIA地址
   略...
   rule 16 permit ip destination object-group weixinyuming
   rule 17 permit udp destination-port eq bootps
   rule 18 permit udp destination-port eq bootpc
   rule 20 permit udp source-port eq dns
#
```

- **页面编排：控制器创建ACL 3001/5001时，支持配置域名过滤（当前需要手配，控制器开发中）**

主要涉及以下场景：

（1）有线单栈场景：IPv4或IPv6的ACL3001里需要支持配置域名过滤rule。

（2）有线双栈场景：ACL5001里需要支持同时配置双栈的域名过滤rule。

（3）无线单栈、双栈场景：IPv4、IPv6 的ACL 3001均需要支持配置域名过滤rule。

支持企业微信认证

- Matrix DNS配置
  - MATRIX DNS
- 企业微信配置（管理员身份）
  - 创建企业微信应用
  - 配置应用主页及域名
- EIA企业微信认证配置
  - NAT配置--实现内网环境和端口映射到公网IP和端口
  - 配置mac-portal认证及认证前ACL
  - EIA企业微信页面配置
  - 认证点设备配置全局DNS、IPv4及IPv6对象组、ACL 3001或5001中关联对象组

目录

H3C
数字化解决方案领导者

VLAN组网 Seed方案

Vlan seed组网的目标

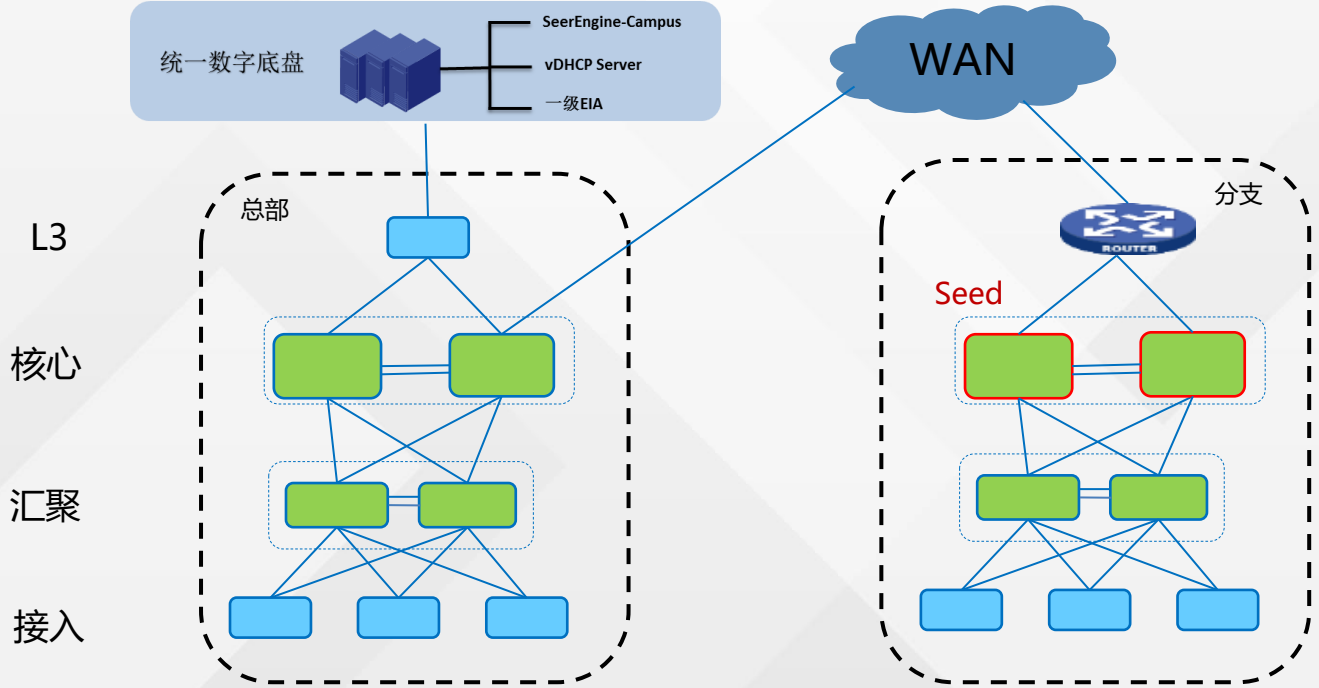
H3C
数字化解决方案领导者

- **减少对上联设备需求：**
  - Vlan1、Vlan4094等管理网关均在内部设备上
  - 与上连设备通过三层转发到控制器
- **上线场景统一化：**
  - 适配单机/IRF/MLAG等各种场景
- **管理Vlan优化：**
  - 三层组网支持有线多管理Vlan，管理vlan以汇聚组为粒度，网关在汇聚上，减小有线管理网的二层广播域
  - 单汇聚网络定位为小型网络，不涉及多管理vlan，但可由用户指定管理Vlan
- **管理地址统一：**
  - 汇聚以上采用loopback口管理，接入使用管理vlan

应用场景

- **对于总部园区**：部署集群服务器时需要汇聚交换机，此时建议借用该交换机充当L3交换机，实现园区设备的自动化上线。
- **对于分支园区 / 控制器拉远的场景**：可使用Seed方案代替半自动化，更加便捷的实现设备上线。
- **支持的组网**
  - **堆叠模式**
    - 三层组网
    - 单汇聚组网
  - **M-LAG模式**
    - 三层组网
    - 单汇聚组网

（注：核心和汇聚组成M-LAG系统时，需手动配置M-LAG认证虚拟IP，不支持自动分配）



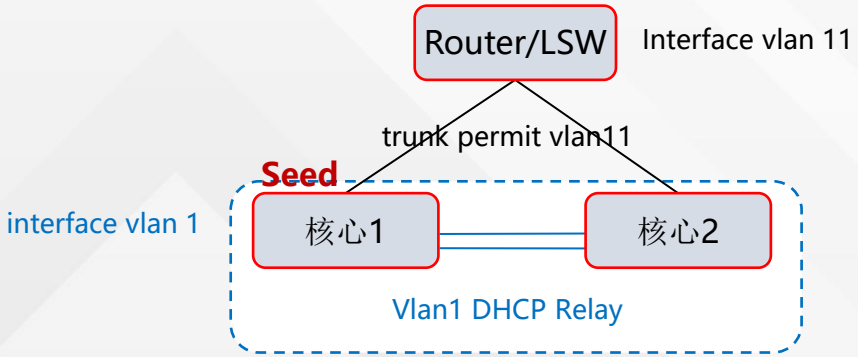
Vlan1 DHCP Server的位置

- **在Seed设备上配置Vlan1 DHCP relay：**

  在核心上配置Vlan1网关和 DHCP relay；（配置简单，Vlan1地址池继续放到vDHCP上）

- **选择为seed节点的设备上下发的相关配置：**

```
#
ip address 90.0.0.1 255.255.255.0  //vlan1网关
mac-address 0001-0001-0002
dhcp select relay  //dhcp relay配置
dhcp relay server-address 214.10.1.7
dhcp relay server-address 214.10.1.8
#
```

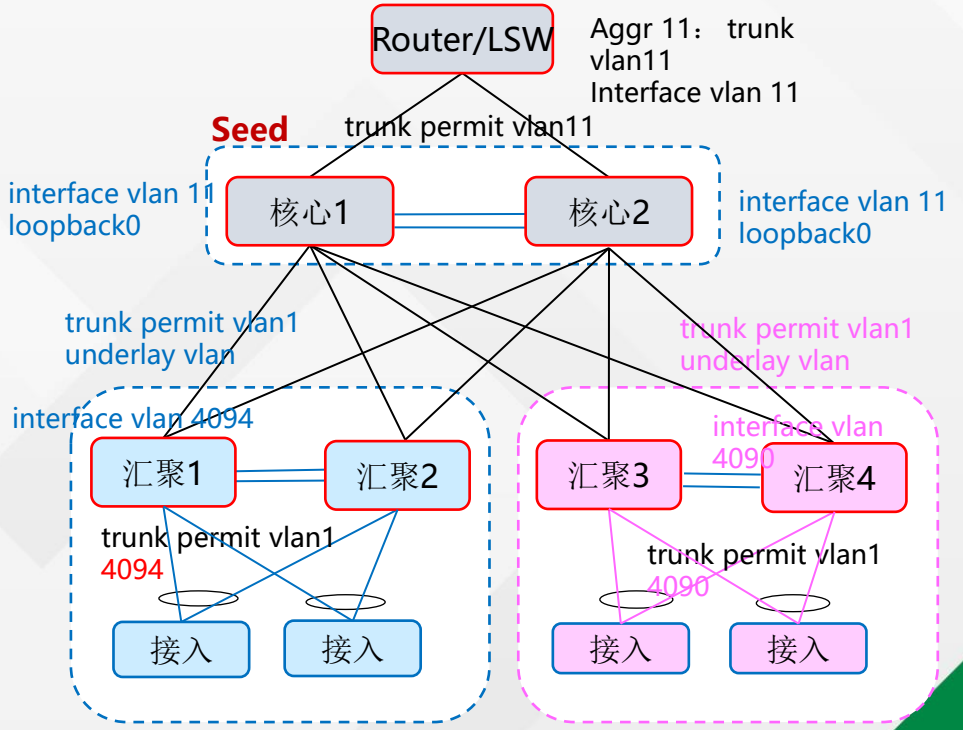


三层组网—单机/堆叠场景

- **连接方式：**核心/汇聚设备和上连设备之间，单机采用单链路或聚合，IRF场景采用聚合链路

- **1. 核心上线：（手工配置）**
  1. 需要IRF的设备，先手工堆叠；
  2. Router/LSW 配置Interface Vlan 11互联接口，配置到核心/汇聚的回程路由（到loopback0的32位主机路由）用于控制器与待纳管设备连通；
  3. 核心/汇聚上配置相应interface Vlan接口，并配置loopback0地址作为管理地址，路由可达控制器
  4. 增加cloud management的配置，用于和控制器建立websocket连接。
  5. 增加Router/LSW上到Loopback网段的路由（保证汇聚纳管）
- **3. 汇聚/接入上线：**
  1. Router/LSW 配置到Vlan1网关的路由，用于控制器与待纳管设备连通；
  2. 汇聚/接入上线，获取到Vlan1 IP，并连接控制器；
  3. 自动化拓扑调整并完成IRF；
- **4. 汇聚/接入纳管：**
  1. 选择汇聚，指定有线管理Vlan（单汇聚缺省使用Vlan 4094，支持修改；多汇聚每个汇聚下一个有线管理vlan ）；Router/LSW配置到管理Vlan的网段路由
  2. 核心汇聚间下发underlay vlan，并使能ospf；
  3. 汇聚上下发管理Vlan网关，并将Vlan网关发布到ospf中；
  4. 接入下发对应管理vlan的地址，接入到控制器路由的下一跳为管理网Vlan网关；
  5. 设备完成纳管停止自动化时，汇聚和接入删除vlan1地址，汇聚通过loopback0纳管，接入通过管理vlan纳管；
  6. 认证业务的网关地址需要修改为loopback地址（管理地址使用lo口）

- **2. 核心纳管：**
  1. 选择核心设备自动化上线纳管；
  2. 选择核心为Seed设备，下发Vlan1 interface 作为网关,下发Vlan1 DHCP relay。



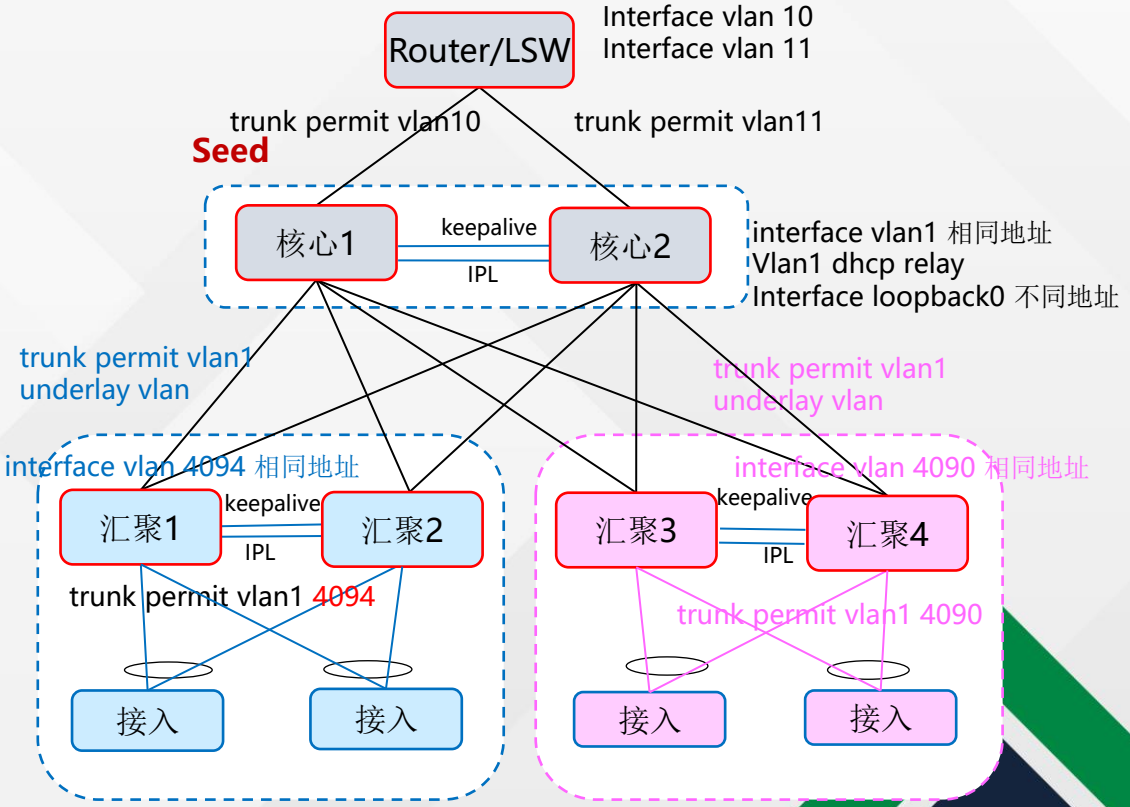
三层组网—MLAG场景

H3C 数字化解决方案领导者

- **连接方式：**核心/汇聚设备和上连设备之间，采用ECMP方式连接

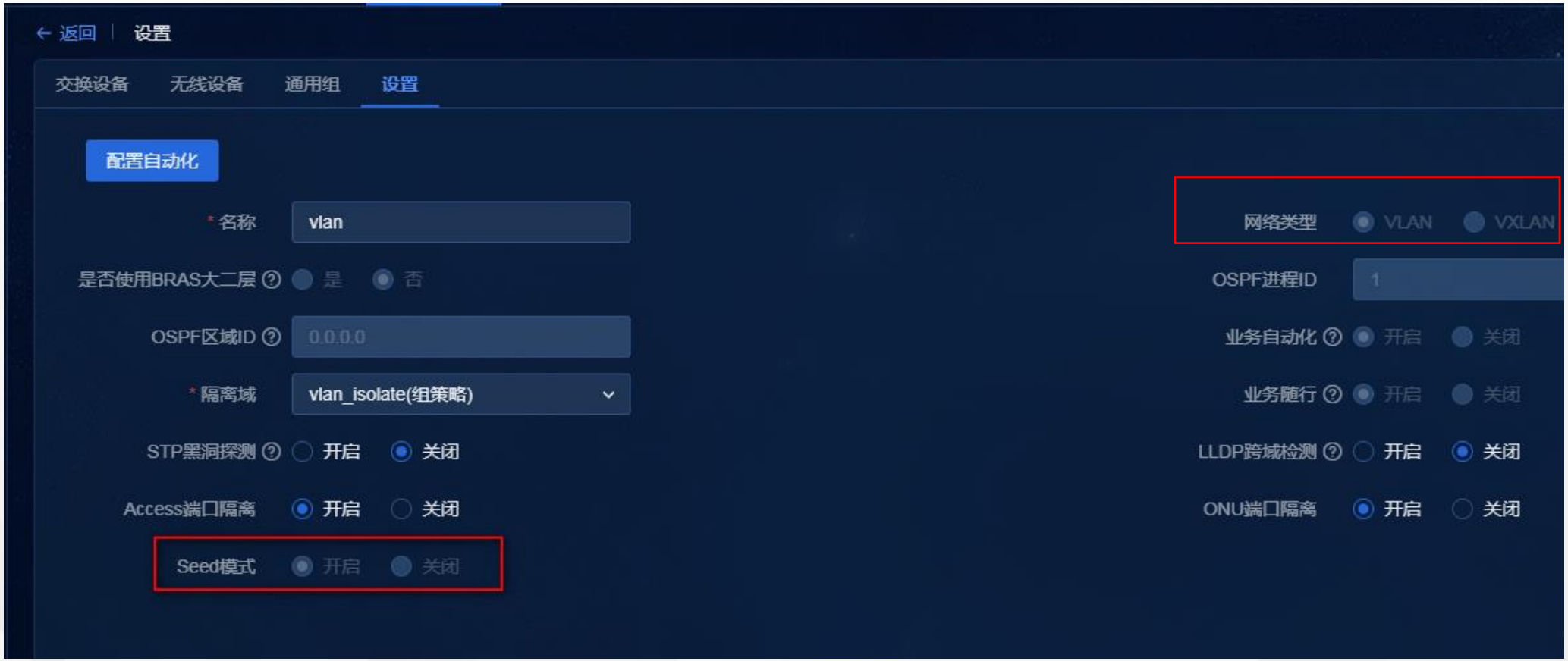
- **1. 核心上线：**（手工配置）
  1. Router/LSW 配置inter Vlan10和11接口，配置到核心/汇聚的回程路由（到loopback0的32位主机路由），用于控制器与待纳管设备连通。
  2. 核心/汇聚上配置相应interface Vlan接口，并配置loopback0地址，路由可达控制器；
  3. 增加cloud management的配置，用于和控制器建立websocket连接
  4. 增加Router/LSW上到Loopback网段的路由，此时为等价路由。（保证汇聚纳管）
- **3. 汇聚/接入上线：**
  1. Router/LSW 配置到Vlan1网关的路由，用于控制器到待纳管设备连通；
  2. 汇聚/接入上线，获取到Vlan1 IP，并连接控制器；
- **4. 汇聚/接入纳管：**
  1. 选择汇聚，指定有线管理Vlan（例如Vlan 4090）；Router/LSW配置到管理Vlan的网段路由，下一跳为互联的ECMP或者其他interface Vlan(DR 聚合上放通该Vlan)。
  2. 核心汇聚间配置underlay vlan，并使能ospf；
  3. 汇聚上配置管理Vlan网关，并将Vlan网关发布到ospf中；
  4. 接入分配对应管理vlan的地址，接入到控制器路由的下一跳为管理网Vlan网关；
  5. 设备完成纳管停止自动化时，汇聚和接入删除vlan1地址，汇聚通过loopback0纳管，接入通过管理vlan纳管。
  6. 控制器通过loopback口管理汇聚，并配置汇聚的MLAG。

- **2. 核心纳管：**（注：三层组网只支持AC集中转发，目前只支持Mlag场景，暂不考虑双border场景）
  1. 选择核心设备自动化上线纳管。
  2. 通过Loopback0口管理Border配置为MLAG。
  3. 选择核心为Seed设备，配置Vlan1 interface 网关,下发Vlan1 DHCP relay。



Fabirc创建及Seed配置

1. 创建vlan类型fabric，新增“Seed模式”配置项（一旦创建不可修改）



Vlan Seed组网地址池配置

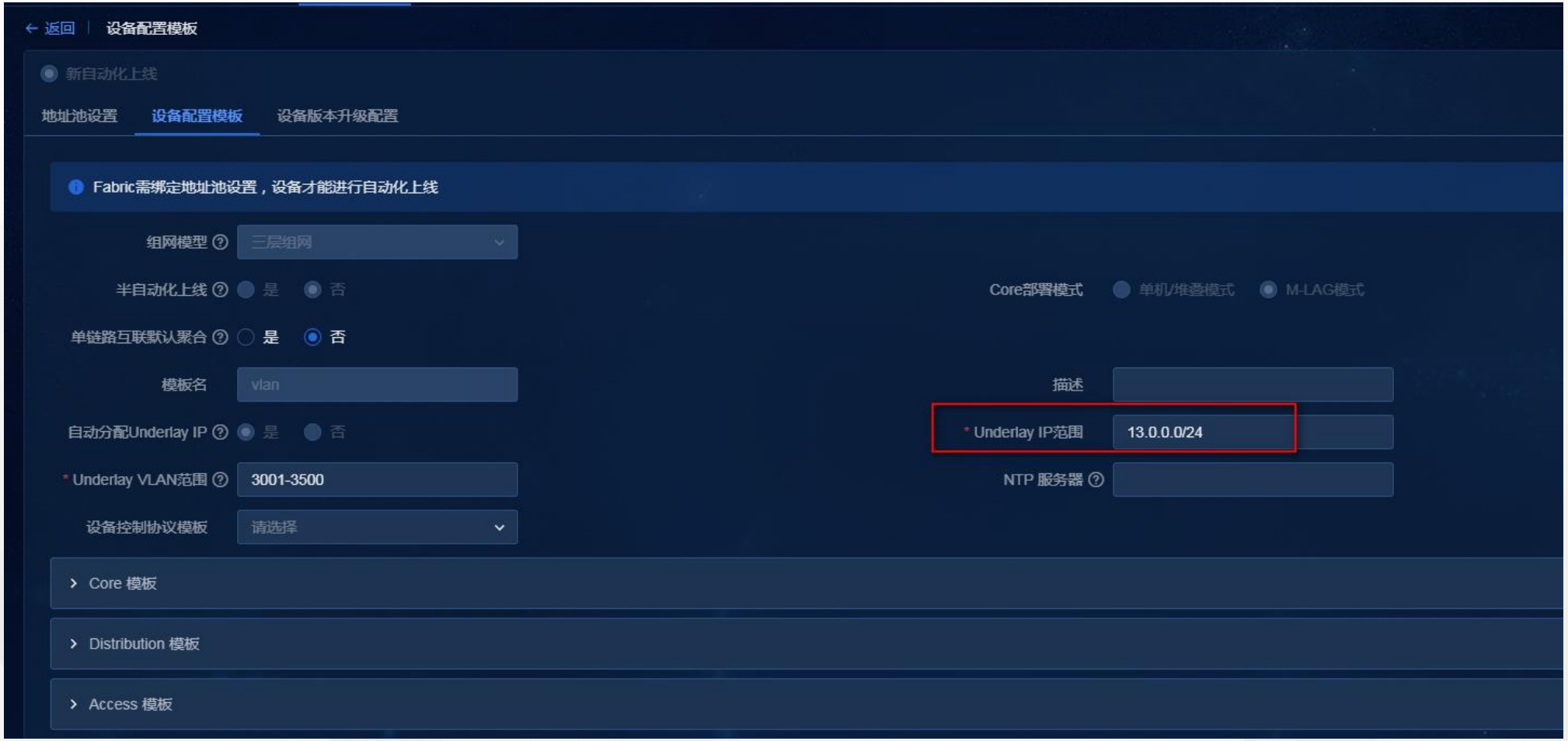
2. 当选择“seed模式”为开启时，自动化上线绑定地址池为“园区管理网络地址池”

- 园区管理vlan池
- 园区管理ip池

Vlan Seed组网自动化模板配置

H3C 数字化解决方案领导者

3. 配置新自动化上线模板，underlay ip为必填项。Core与Distribution环回口地址网段



Vlan Seed组网自动化拓扑配置

4、手动纳管border设备上线，创建待纳管，新自动化拓扑页展示手动配置的待纳管节点

- 上行口配置：控制器校验控制器配置的和设备是否一致
- Seed配置：单border组网，可配置待纳管或已纳管的border设备为seed;

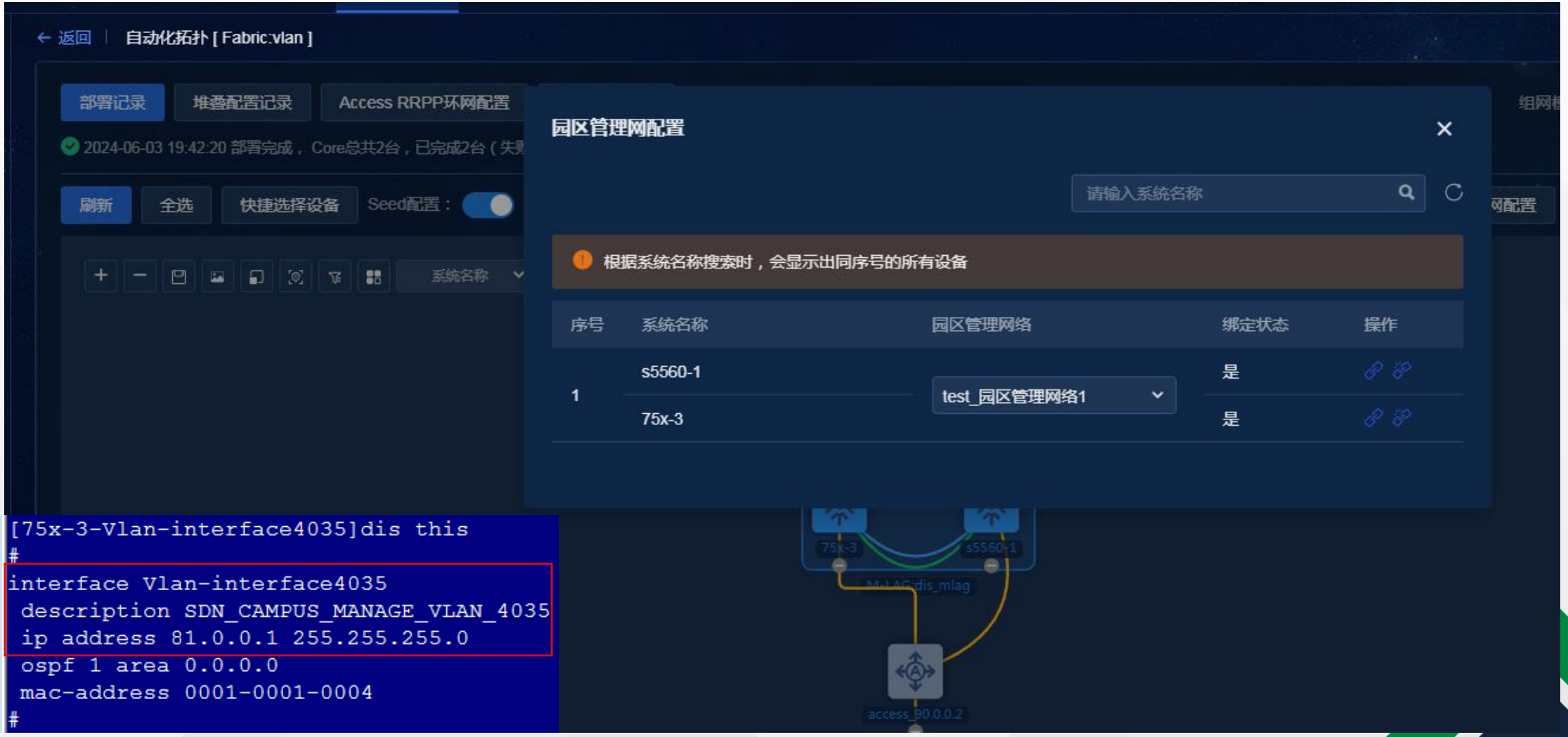
mlag组网，需配置border设备为mlag后，同时选择mlag的两个成员设备为seed

- 选择seed节点后，下发vlan1及dhcp relay相关配置

Vlan Seed组网自动化拓扑配置

5. 下行distribution和access设备空配置上线，能自动获取vlan1并创建待纳管

6. distribution设备选择绑定园区管理网，下发下行access管理网关配置



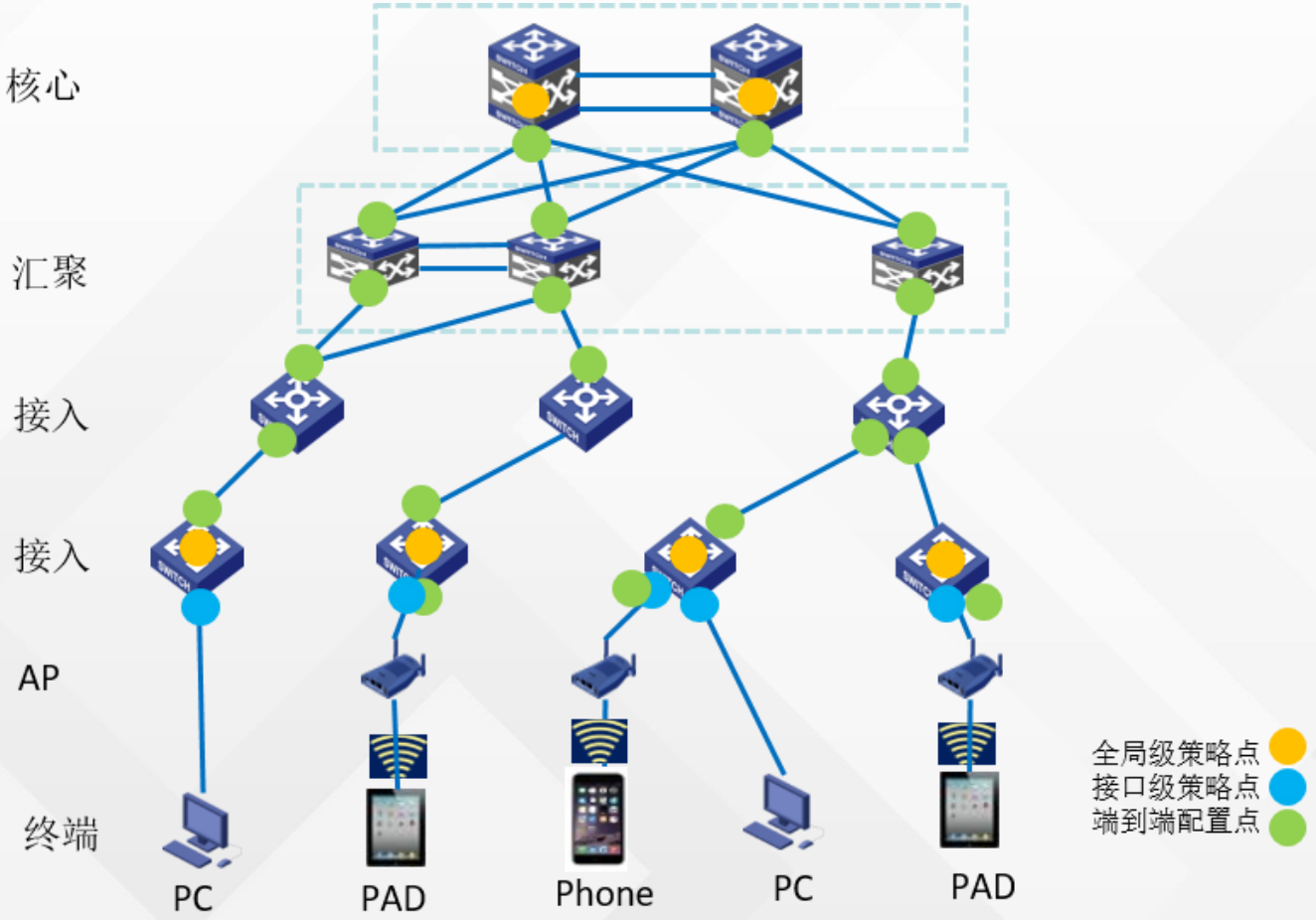
Vlan Seed组网网元部署纳管

7. 选择access自动化部署，获取对应管理网ip及纳管成功

H3C
数字化解决方案领导者

传统网QoS

传统网支持QoS



客户痛点及需求

- Vlan组网关键业务流量无法高优保证
- 流氓应用难以降低优先级
- 无法支持端到端保证

方案应用场景

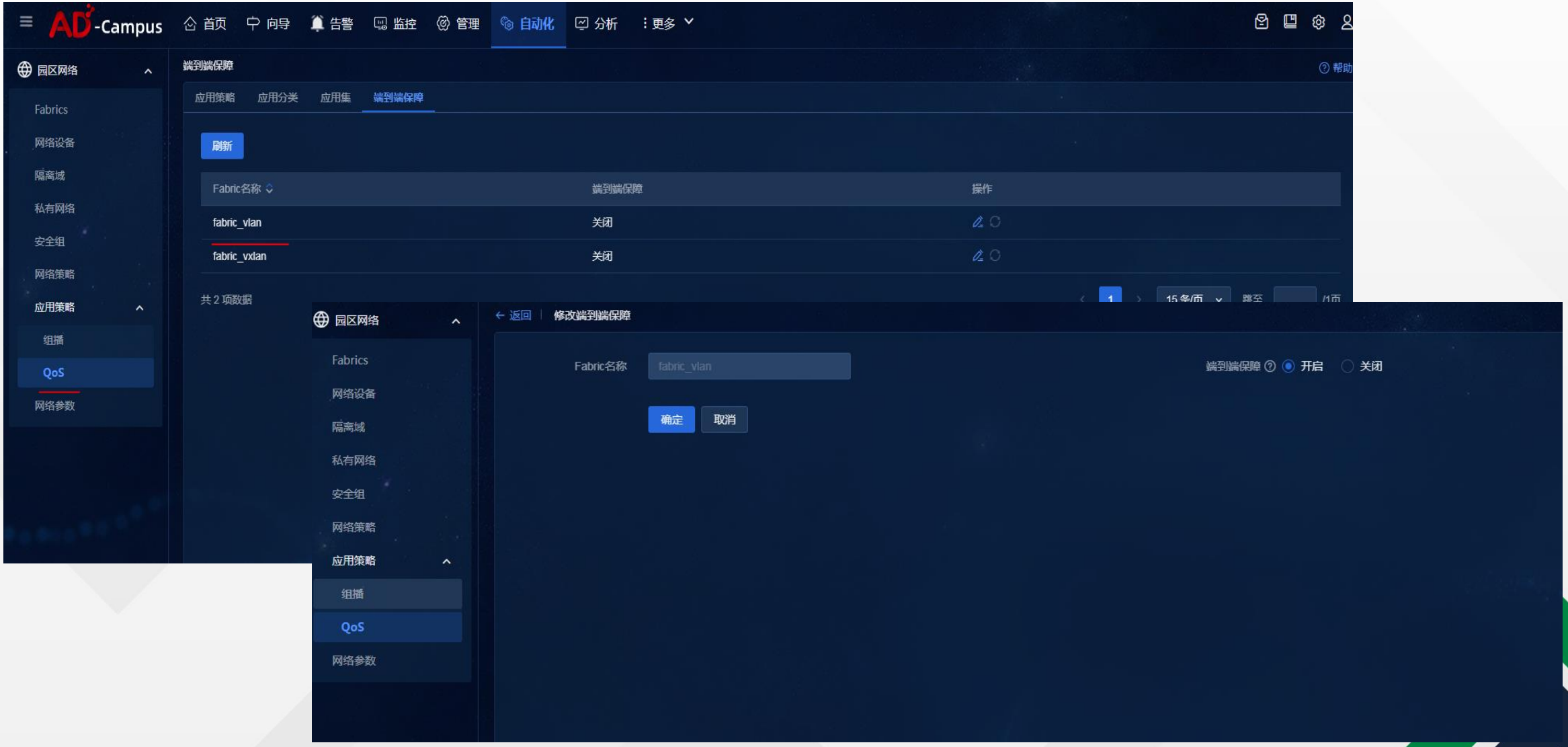
- 适用于教育、企业、医疗等众多园区场景
- 对特殊业务要求高优保障的场景

市场价值

- 满足用户对于特性业务高优保障需求
- 提供端到端QoS保障，降低用户配置端到端保障复杂度
- 控制器提供设备及和接口级QoS策略，方便用户灵活配置

配置过程

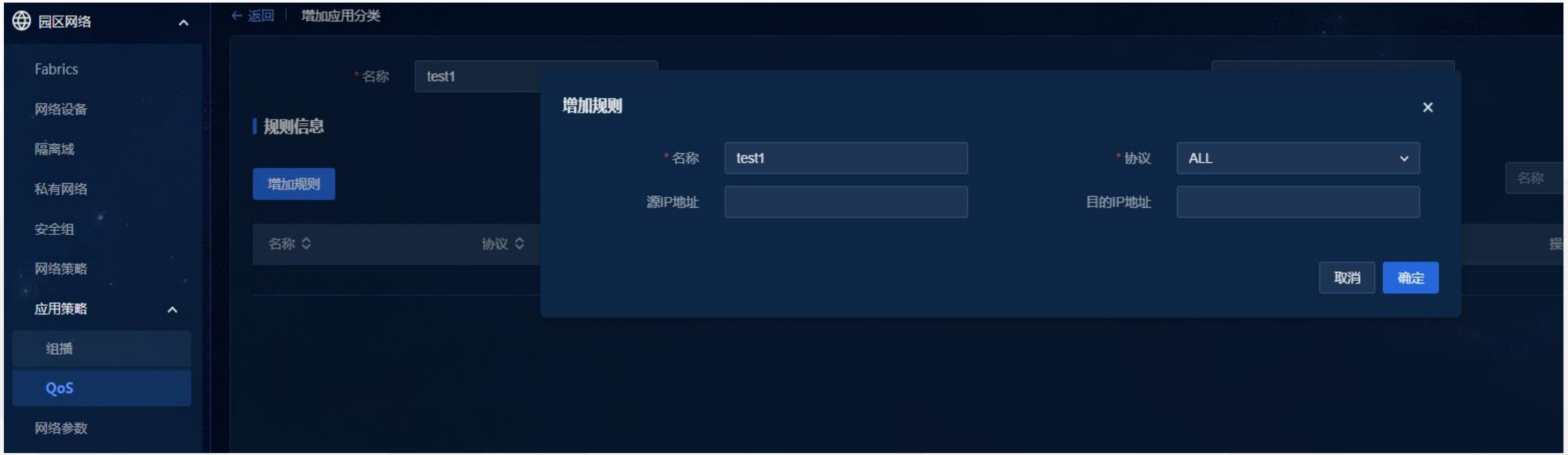
开启端到端保障



配置过程

H3C
数字化解决方案领导者

增加应用分类，选择协议、源目IP、源目端口

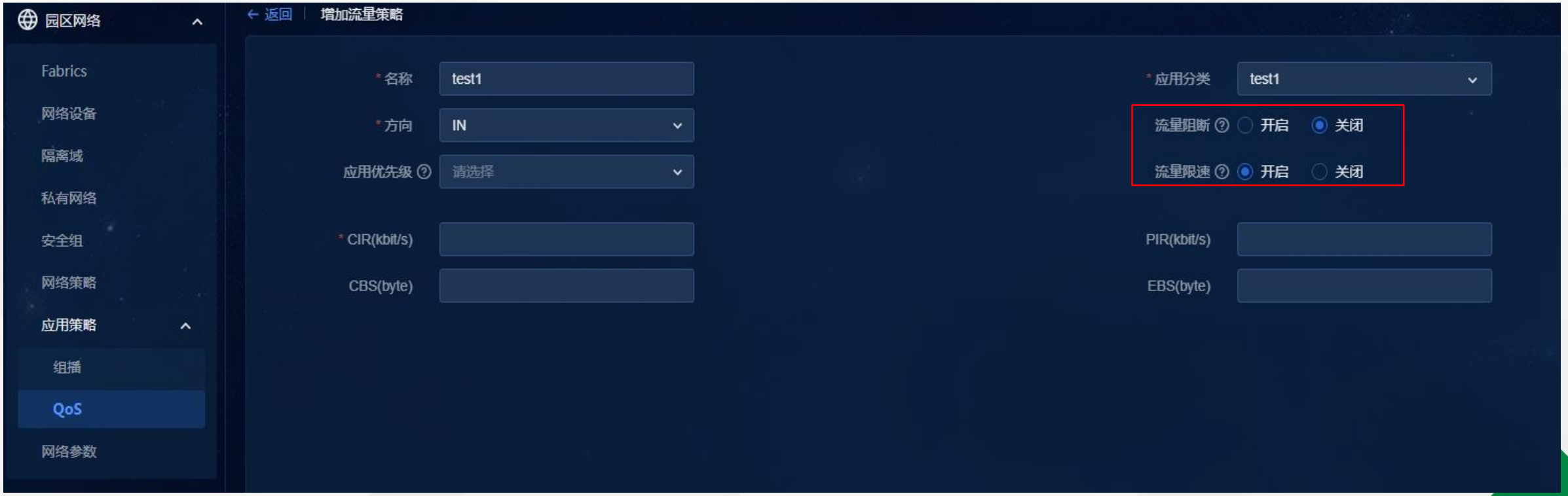


配置过程

增加应用策略

配置应用策略，方向选IN，即下发入方向的QoS策略。

支持开启流量限速、流量阻断功能并指定各参数。



配置过程

H3C
数字化解决方案领导者

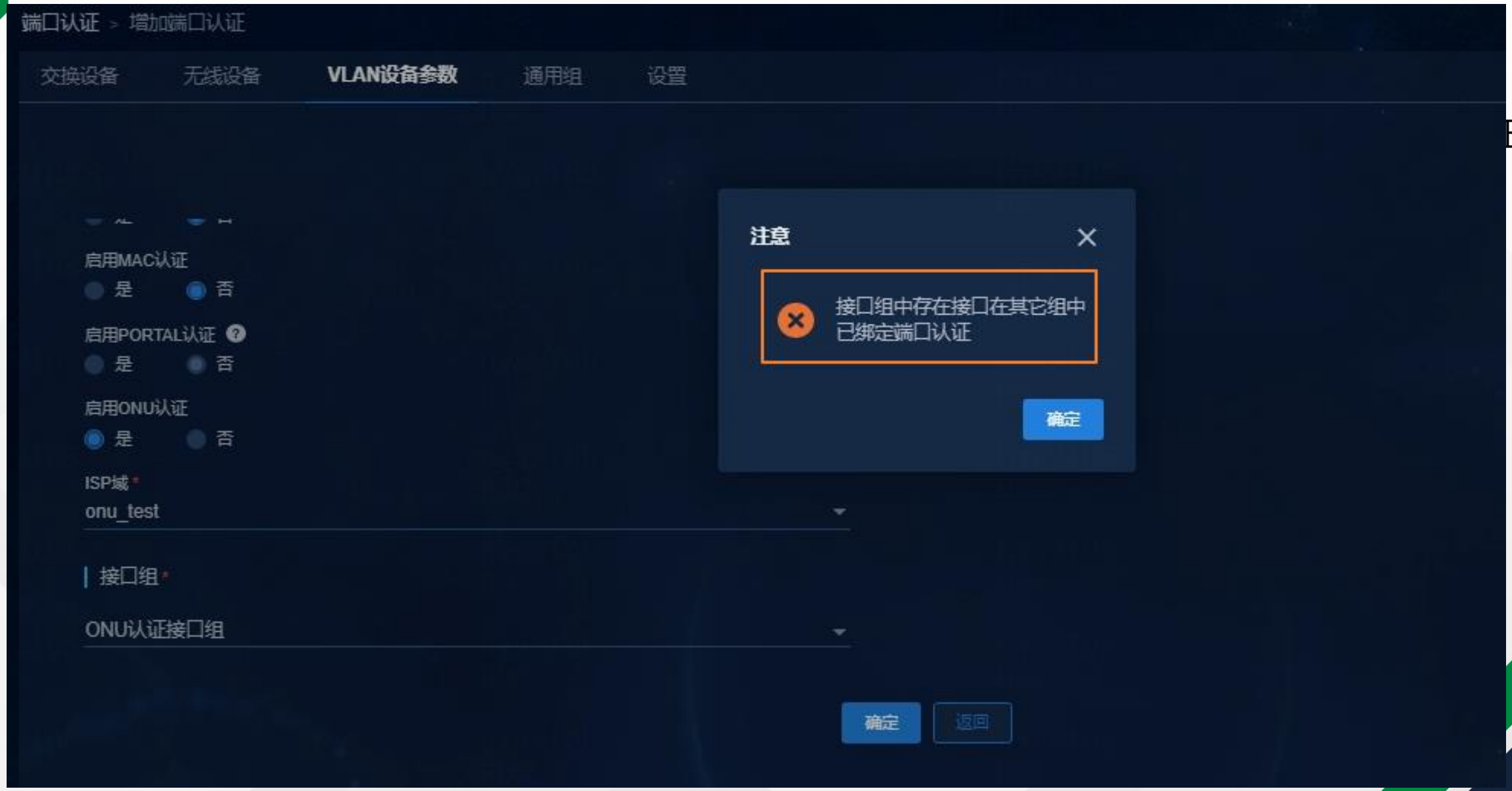
增加网络范围

增加设备网络范围，选择QoS策略下发的位置。支持下发在设备的全局或端口上，可以根据实际需求选择

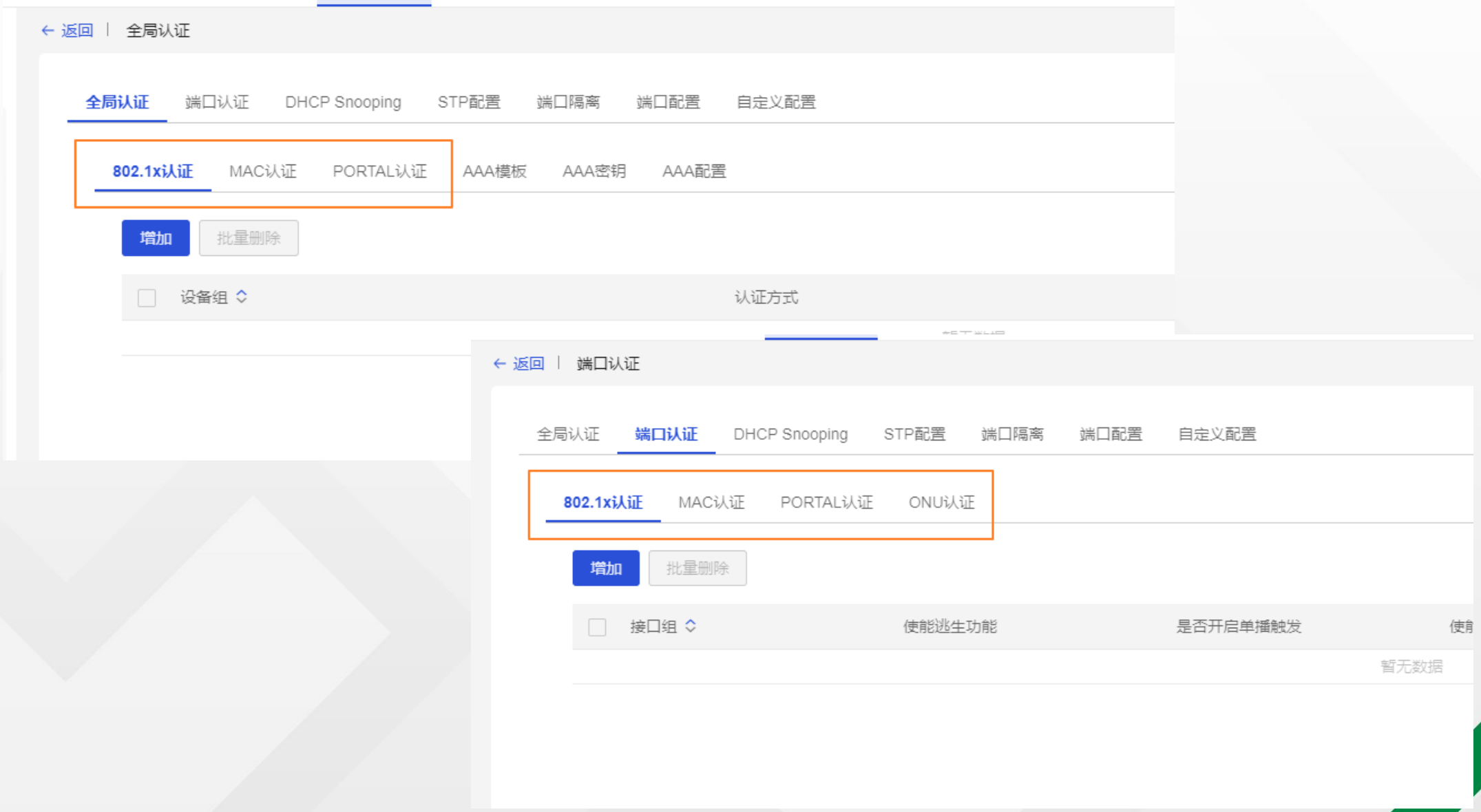
H3C
数字化解决方案领导者

VLAN场景适配

认证拆分--旧版本限制

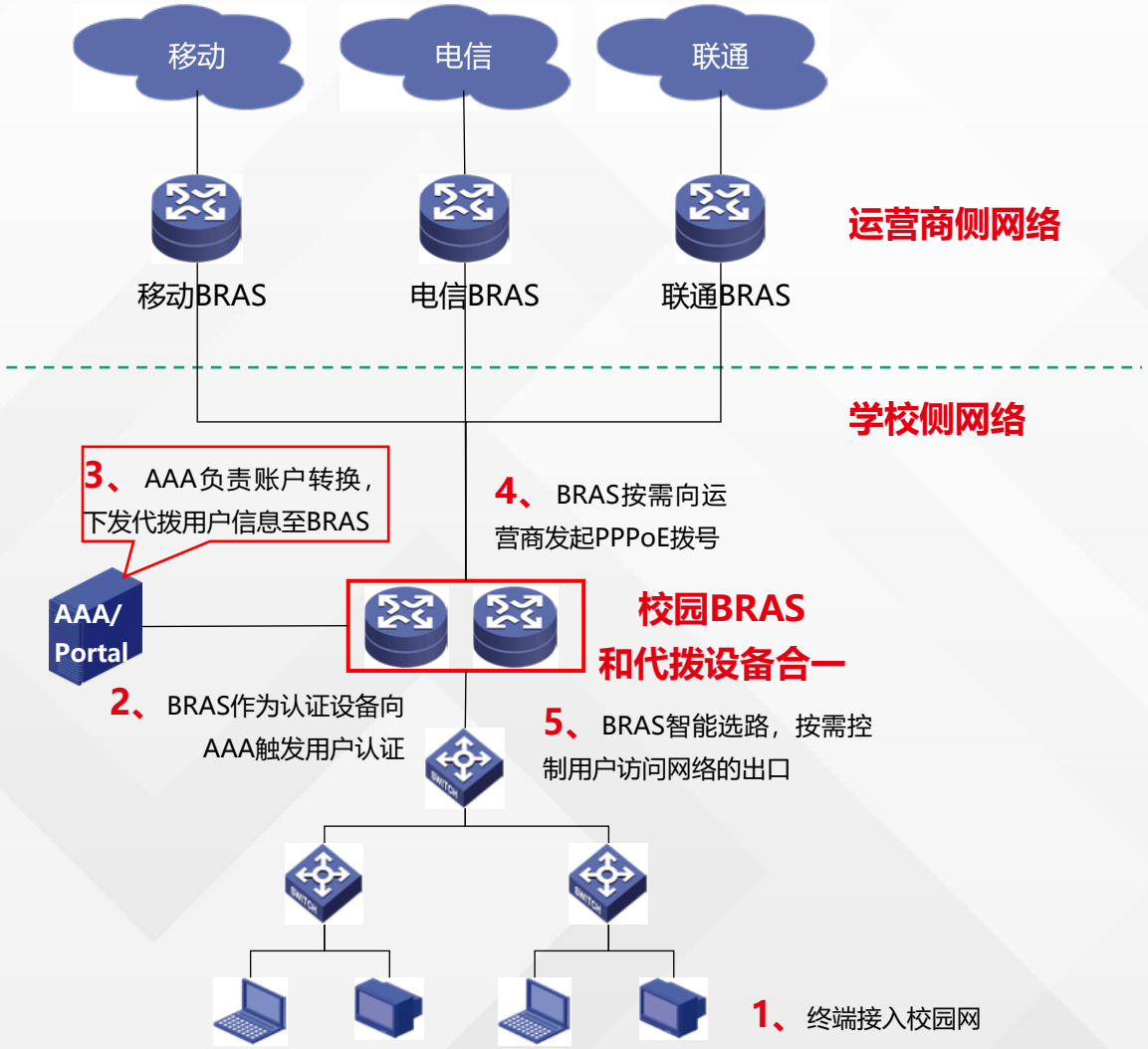

端口认证 > 增加端口认证
交换设备
无线设备
VLAN设备参数
通用组
设置
启用MAC认证
是
否
启用PORTAL认证
是
否
启用ONU认证
是
否
ISP域 *
onu_test
接口组 *
ONU认证接口组
确定
返回
注意
接口组中存在接口在其它组中已绑定端口认证
确定

认证拆分--新版本形式


← 返回 | 全局认证
全局认证
端口认证
DHCP Snooping
STP配置
端口隔离
端口配置
自定义配置
802.1x认证
MAC认证
PORTAL认证
AAA模板
AAA密钥
AAA配置
增加
批量删除
设备组
认证方式
← 返回 | 端口认证
全局认证
端口认证
DHCP Snooping
STP配置
端口隔离
端口配置
自定义配置
802.1x认证
MAC认证
PORTAL认证
ONU认证
增加
批量删除
接口组
使能逃生功能
是否开启单播触发
暂无数据

目录

PPPoE代拨：一体化代拨



背景：

高校和运营商联合运营场景下，通过在校园网BRAS设备上部署PPPoE代拨功能，为校园网用户提供自主选择运营商网络，以及自动发起PPPoE拨号上网的服务。可以简化校方和运营商的联合运营模式，为学生提供了极佳的网络体验。

组网方式：核心和代拨合一

- **接入方式**：不限（有线、无线均可）、接入区域不限（教学区、宿舍区）
- **核心和代拨**：合一，全部由校内BRAS做，准入准出全部在BRAS上，BRAS连接不同的运营商，BRAS作为代拨负责准出

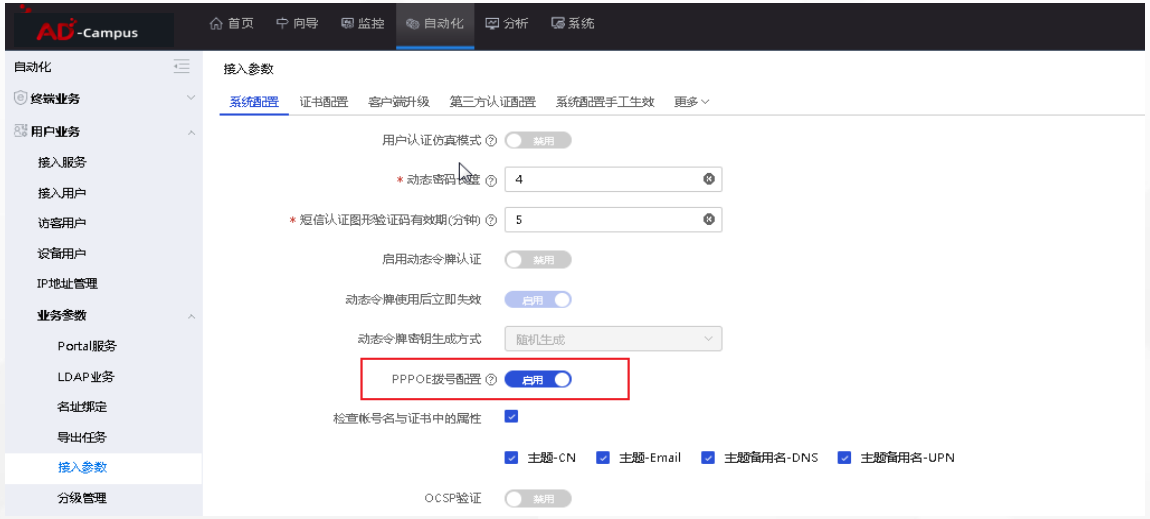
认证方式：全部在校园网核心BRAS

- **准入准出合一**：准入在校内BRAS上（目前BRAS与AD-Campus的组合可支持Portal认证和802.1x认证的BRAS代拨），一般采用学号作为用户名，认证通过后，BRAS再进行PPPoE拨号认证到各自的运营商的BRAS上，采用运营商的账号名作为用户名，AAA上会有学号和手机号码的对应关系。

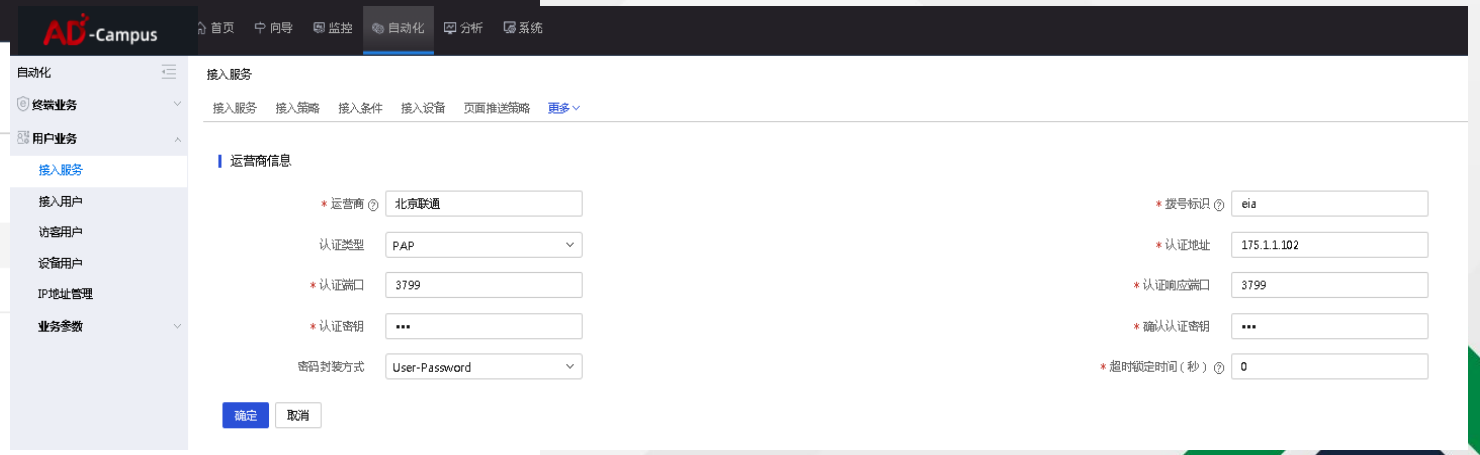
PPPoE代拨：一体化代拨

H3C 数字化解决方案领导者

1、配置代拨：在自动化>业务参数>接入参数>系统配置：启用代拨

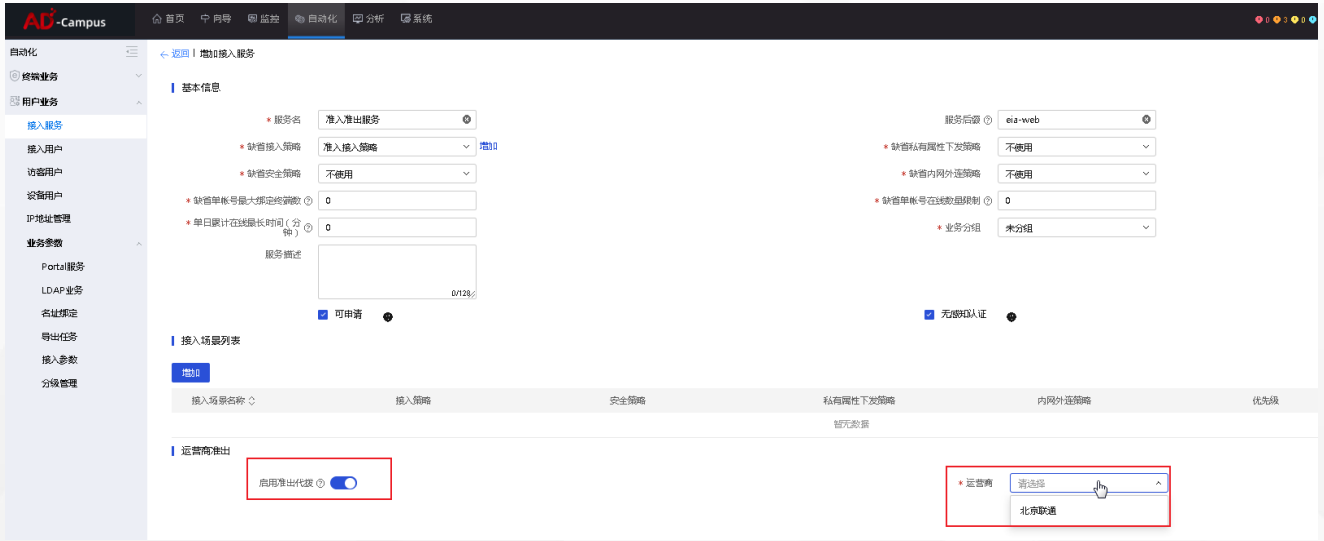


2、配置运营商：在自动化>用户业务>接入服务>更多>运营商配置：增加运营商相关拨号信息

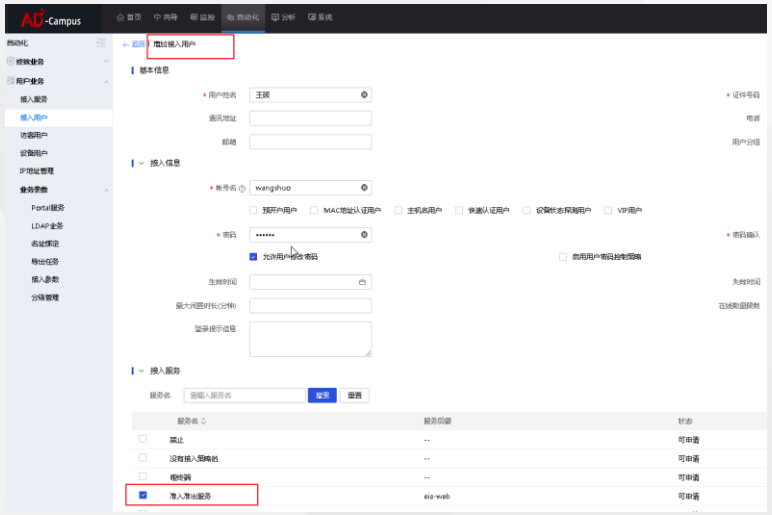


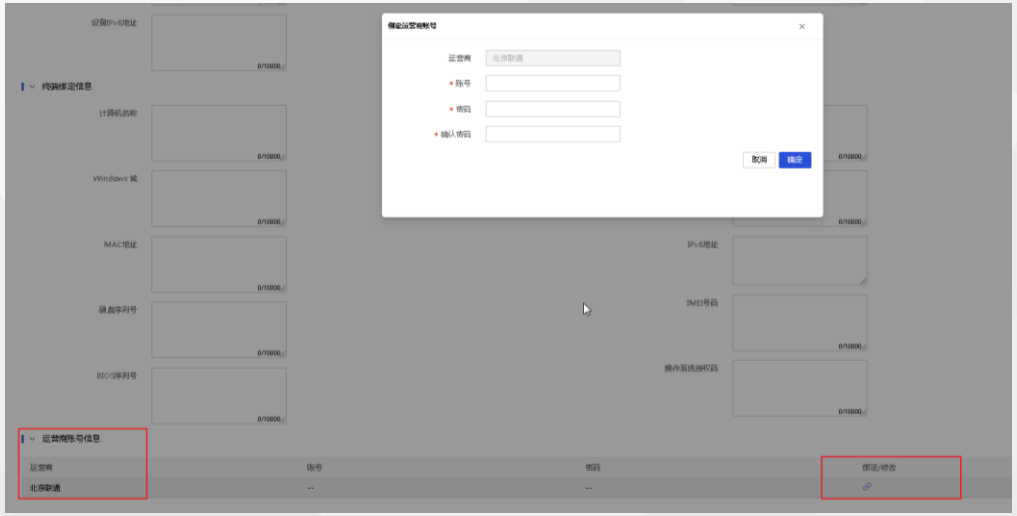
PPPoE代拨：一体化代拨

3、配置代拨服务：在自动化>用户业务>接入服务>接入服务：关联指定运营商配置准入服务，同时配置准入的接入策略



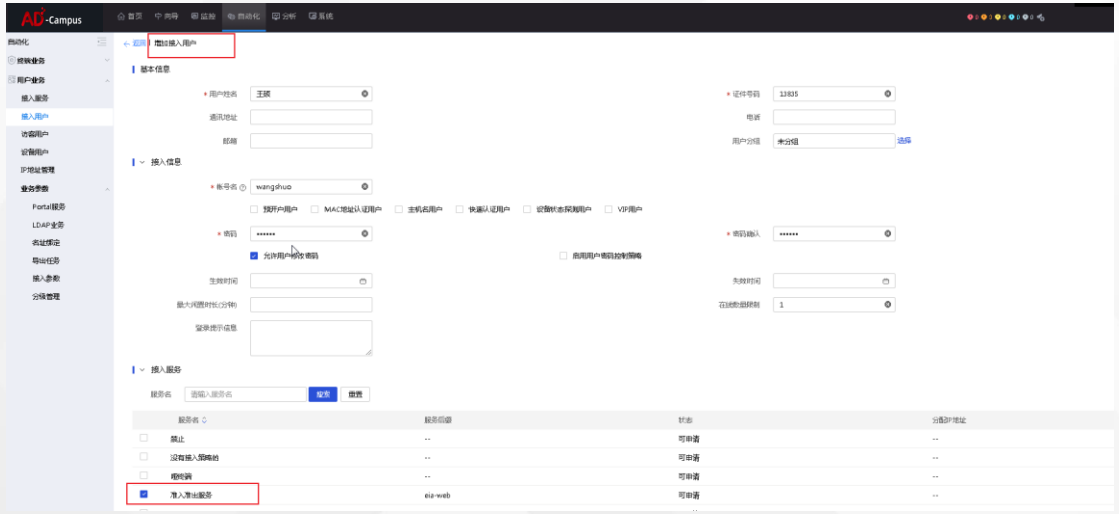
4、配置准入用户并绑定运营商账号：在自动化>用户业务>接入用户：添加接入用户并绑定运营商账号信息

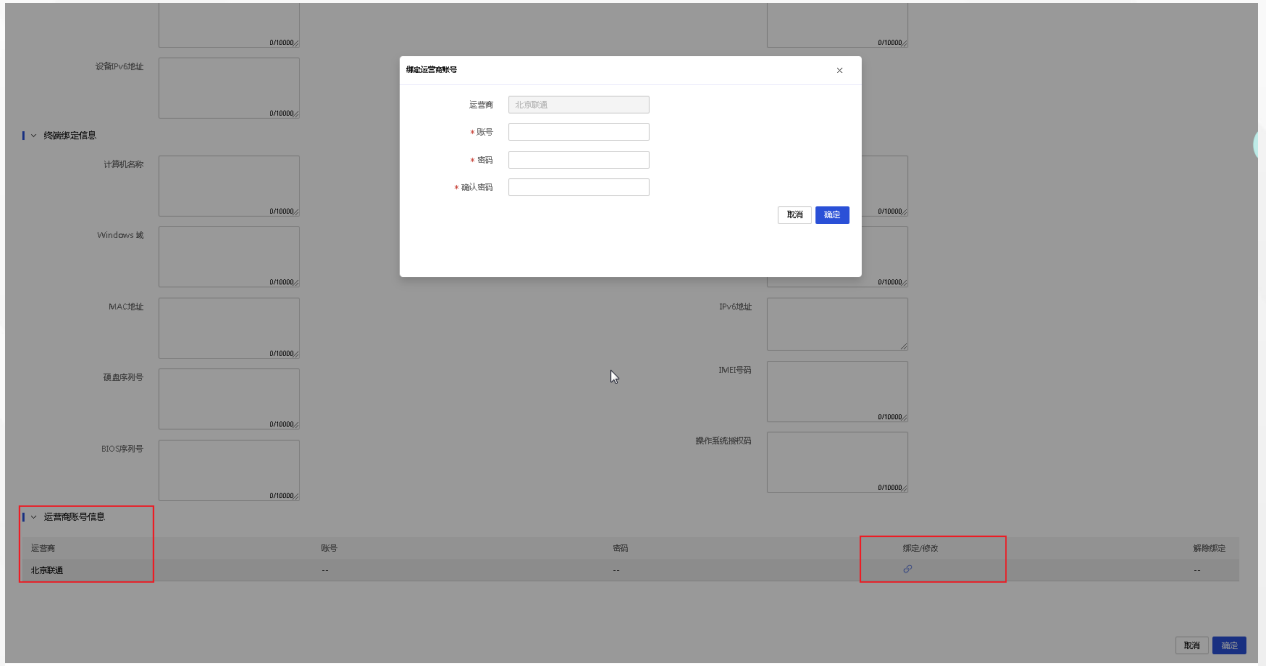




PPPoE代拨：一体化代拨

4、配置准入用户并绑定运营商账号：在自动化>用户业务>接入用户：添加接入用户并绑定运营商账号信息





PPPoE代拨：一体化代拨

H3C
数字化解决方案领导者

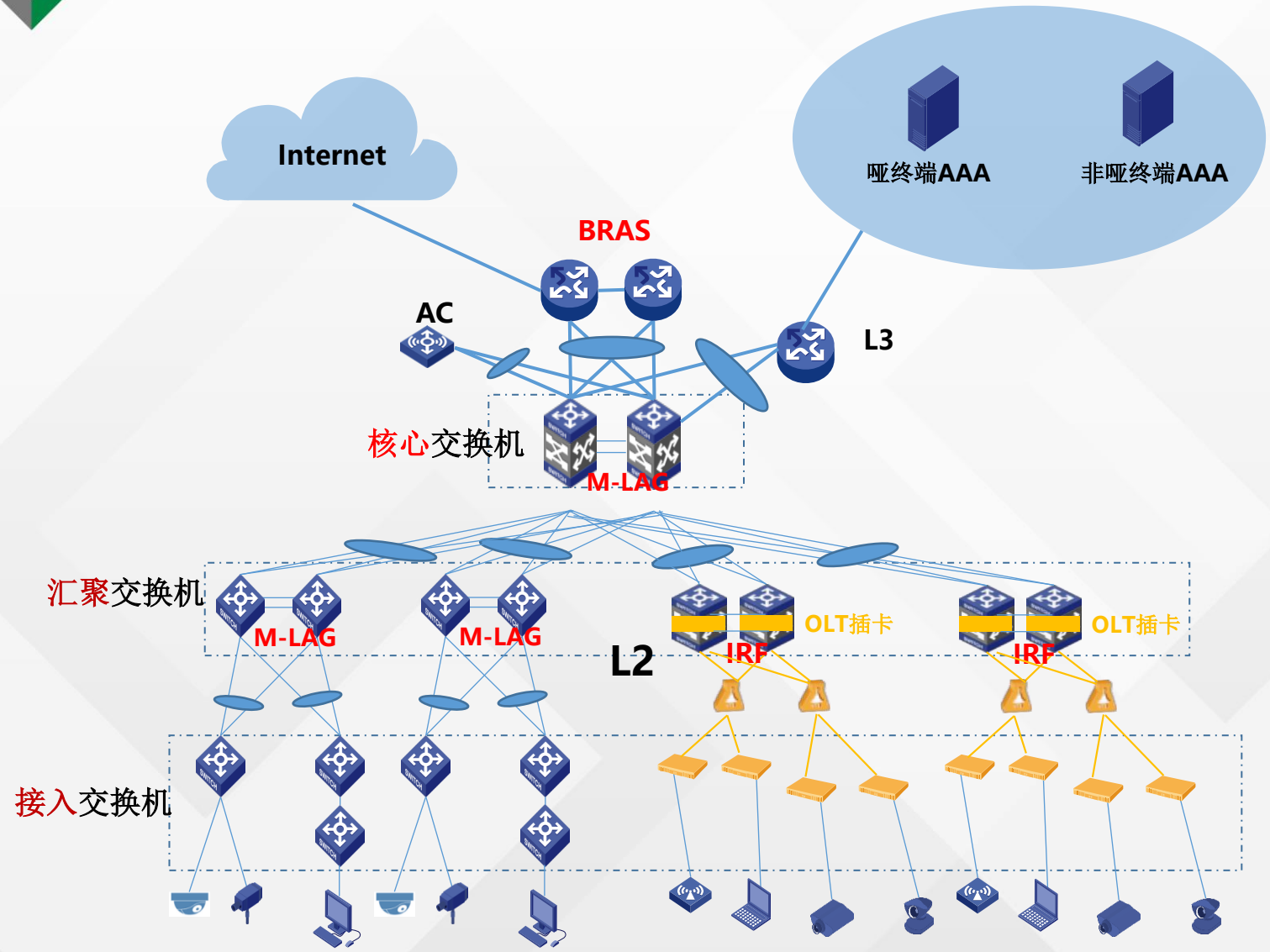
5、BRAS上进行业务配置后，终端即可实现一次登录完成校园网、运营商的两次认证

```
[Bras1]dis access-user
UserID     Interface                 IP address          MAC address     S-/C-VLAN
           Username                  Access type
           IPv6 address
0x29a0     RAGG2.101                 30.1.0.2            0cda-411d-11ab 101/-
           zpp001                    Web auth(D/D)
           30:1::8957:C402:E336:9464
0x29a1     XGE3/3/2                  66.1.1.2            0cda-411d-11ab -/-
           a001                      PPPoEA
           -
0x400014   -                         110.1.0.7           -              -/-
           admin                     SSH
           -
[Bras1]
```

注意事项：

- BRAS代拨功能有单板型号要求，BRAS用户认证的接口和与运影响连接的代拨接口都需要支持代拨功能的单板，具体支持情况请查看BRAS产品手册或联系BRAS产品咨询。
- BRAS准入认证支持IPv4、IPv6用户认证，但是Bras到运营商代拨的准出认证只支持IPv4认证，具体支持情况请联系BRAS产品咨询。
- 目前BRAS与AD-Campus的组合可支持Portal认证和802.1x认证的BRAS代拨。

BRAS哑终端认证拆分



使用场景：

校园网场景面对大量哑终端接入场景，第三方AAA（深澜/城市热点）对于哑终端管理能力较弱，BRAS又支持同时对接多个AAA服务器，因此本特性对哑终端按照静态IP上线or指定业务VLAN上线，使用EIA进行认证，非哑终端依然采用第三方AAA认证。

配置思路：

1. 哑终端上线对于BRAS启用IPoE静态用户认证（IP or 网段（必须项）、MAC、接口、VLAN），关联EIA的domain。
2. 非哑终端上线对于BRAS启用IPoE动态用户认证关联城市热点、深澜即可。静态用户认证优先级高于动态用户。

上述场景为哑终端和其他终端混接场景。

当可以指定边缘业务VLAN区分哑终端接入时，可以采用非静态用户认证接入方案。这样哑终端可以动态获取IP。

BRAS哑终端认证拆分

基于IP段哑终端上线：

#配置匹配指定静态IP地址段报文触发认证
ip subscriber session static ip 20.1.0.101 20.1.0.200 domain isp1 //domain isp1关联EIA

基于MAC段哑终端上线：

#用户认证接口下配置
interface Route-Aggregation3.201
ip address 20.1.0.1 255.255.0.0
proxy-arp enable
local-proxy-arp enable
ip subscriber initiator arp enable
vlan-type dot1q vid 201
ipv6 address 20:1::1/64
ipv6 address auto link-local
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
proxy-nd enable
local-proxy-nd enable
undo ipv6 nd ra halt
ip subscriber l2-connected enable　//二层接入模式认证模式
ip subscriber authentication-method dot1x high-priority web　//同时支持dot1x和web认证，具体支持情况需要路由器产线整体评估
ip subscriber password mac-address　//mac触发认证，用户名/密码使用mac地址进行认证
ip subscriber pre-auth domain mac　//domain mac关联EIA
ip subscriber username mac-address
ip subscriber initiator unclassified-ip enable matching-user　//使能未知源IP报文触发方式，静态IP触发认证时需要配置

H3C
数字化解决方案领导者

THANKS

www.h3c.com