

矩尺负载均衡管理系统

用户手册

杭州矩尺网络科技有限公司

2023 年 12 月

给用户的说明

免责与著作权声明：

本文档仅用于向用户提供相关产品信息，矩尺网络科技有限公司对本文档中的信息不做任何明示或暗示的承诺。

对于文档涉及的可能或已经由矩尺网络科技有限公司所享有的知识产权（包括但不限于专利权、专利申请权、商标权、著作权），本文档中任何表述均不构成矩尺网络科技有限公司对用户的许可和授权。在未得到矩尺网络科技有限公司另行书面许可的情况下，用户不得出于任何目的、以任何形式或手段（包括但不限于电子的、机械的、影印、录制等）复制、发行、传播、许可他人使用本文档的任何内容。

本文档中作为范例而向用户阐述的公司、组织、产品、域名、e-mail 地址、徽标、人员、地点和事件均为虚构，不与任何真实的公司、组织、产品、域名、e-mail 地址、徽标、人员、地点和事件产生直接或间接的联系。

目录

1	前言.....	1
1.1	编写目的.....	1
1.2	适用范围.....	1
1.3	文档负责单位.....	1
2	产品介绍.....	1
2.1	产品特点.....	1
2.2	应用场景功能列表.....	3
2.3	产品技术架构.....	4
2.3.1	应用服务均衡场景.....	4
2.3.2	应用服务器健康检查.....	4
2.3.3	负载均衡算法.....	5
2.3.4	优先级分组.....	6
2.3.5	温暖上线.....	6
2.3.6	会话保持机制.....	6
2.3.7	源地址转换.....	7
2.3.8	溯源.....	7
2.3.9	SSL 卸载.....	8
2.3.10	分发策略与分发规则.....	8
2.3.11	应用性能优化.....	8
2.4	部署架构.....	9
2.4.1	旁路模式.....	9
2.4.2	串行模式.....	10
2.5	设备高可用性.....	11
2.5.1	主备切换.....	11
3	基础配置流程介绍.....	11
3.1	系统初始化.....	11
3.2	基础网络配置.....	12
3.3	平台与集群管理.....	13
3.4	单台设备管理.....	14
3.5	负载均衡业务管理.....	14
3.5.1	TCP 类型负载均衡业务.....	14
3.5.2	TCP/SSL 类型负载均衡业务.....	15
3.5.3	HTTP 类型负载均衡业务.....	16
3.5.4	HTTPS 类型负载均衡业务.....	17
4	详细操作手册.....	18
4.1	设备上架.....	18
4.1.1	环境要求.....	18
4.1.2	产品面板.....	18
4.1.3	操作步骤.....	20
4.2	系统登录与退出.....	23

4.2.1	密码修改.....	24
4.3	状态显示.....	24
4.4	网络接口名称.....	25
4.5	监控与告警.....	25
4.5.1	数据统计.....	31
4.5.1.1	设备性能.....	31
4.5.1.2	网络接口.....	31
4.5.1.3	设备会话.....	32
4.5.1.4	虚拟服务.....	32
4.5.1.5	服务器池.....	33
4.5.1.6	源地址转换.....	33
4.5.1.7	服务器节点.....	34
4.6	SLB 本地负载.....	34
4.6.1	网络地图.....	34
4.6.2	域名解析.....	35
4.6.3	服务器池.....	37
4.6.3.1	服务器池节点.....	45
4.6.4	虚拟服务.....	47
4.6.5	健康检查.....	52
4.6.5.1	ICMP 协议健康检查策略.....	54
4.6.5.2	TCP 协议健康检查策略.....	55
4.6.5.3	TCP 半连接健康检查.....	56
4.6.5.4	UDP 协议健康检查策略.....	57
4.6.5.5	HTTP 协议健康检查策略.....	57
4.6.5.6	HTTPS 协议健康检查策略.....	58
4.6.5.7	DNS 协议健康检查.....	59
4.6.5.8	MYSQL 健康检查.....	60
4.6.5.9	自定义脚本.....	61
4.6.6	分发规则.....	62
4.6.7	策略配置.....	63
4.6.7.1	分发策略.....	63
4.6.7.2	七层策略.....	66
4.6.7.3	四层策略.....	73
4.6.7.4	SSL 策略.....	77
4.6.7.5	会话保持策略.....	79
4.6.8	流量组管理.....	82
4.6.8.1	浮动 IP.....	82
4.6.8.2	流量组.....	84
4.6.8.3	SNAT 地址池.....	87
4.6.9	应用失效保障页面.....	89
4.7	平台系统.....	90
4.7.1	设备管理.....	90
4.7.2	SLB 集群管理.....	93

4.7.2.1	集群网络策略.....	93
4.7.2.2	集群配置.....	95
4.7.3	登陆管理.....	97
4.7.4	SSL 证书管理.....	99
4.7.5	事件日志.....	101
4.7.6	邮件管理.....	102
4.7.7	配置管理.....	104
4.7.8	升级.....	105
4.7.9	SNMP 配置.....	107
4.8	单台设备页面.....	110
4.8.1	设备管理.....	111
4.8.2	路由管理.....	117
4.8.2.1	路由表.....	117
4.8.2.2	静态路由.....	118
4.8.2.3	OSPF.....	119
4.8.3	本地 IP.....	121
4.8.4	网络接口.....	124
4.8.5	网口聚合.....	126
4.8.6	Vlan 管理.....	128
4.8.7	日志管理.....	131
4.8.8	数据统计.....	132
4.9	变更执行.....	132

1 前言

1.1 编写目的

本操作手册旨在用于矩尺负载均衡管理系统明确本软件的功能、软件的作用、功能的操作，帮助用户理解及操作本软件。

1.2 适用范围

本文档叙述的功能操作仅限于矩尺负载均衡管理系统使用，适用于公司最终用户、操作维护人员等，通过该文档对系统有统一的理解，最终用户能够按照文档的要求来使用矩尺负载均衡管理系统。

1.3 文档负责单位

本文档由杭州矩尺网络科技有限公司软件研发中心起草、撰写、发布。由软件研发中心负责维护与解释。

2 产品介绍

2.1 产品特点

➤ 提升应用可靠性

矩尺负载均衡设备消除了应用单点故障，保障了应用始终可用，可以帮助应用更快捷的进行容量扩展，并为应用虚拟化部署及云服务的实现提供了保障。

➤ 提供最优的服务

矩尺负载均衡设备全面监控、动态跟踪应用服务性能，提供多种负载均衡策略为应用服务，保证业务可以根据自己的特性和要求始终选择最佳资源。

➤ 保护关键数据

矩尺负载均衡设备支持 SSL 卸载功能，具备强劲的 SSL 处理能力，支持全面的加密算法配置以及证书管理，不仅提供端到端的 SSL 加密，保护客户数据，并且可降低应用服务压力，提升应用访问速度。

➤ 统一管理和配置

矩尺为负载均衡设备提供了统一的管理操作平台，便捷的 GUI 配置界面，通用的配置场景模板，支持 RBAC、资源组分配、设备统一管理、设备批量升级及批量操作。

➤ 应用智能代理

矩尺负载均衡设备为用户提供应用全代理服务，支持应用协议版本转换、常用应用协议转换，既可以为应用版本平滑升级提供保障，又可以增强应用的访问兼容性。

➤ 应用性能智能监控

矩尺负载均衡设备可以提供全面应用数据收集，通过基于大数据平台的数据治理及数据展现，深化展现应用性能，为智能化管理和调度应用提供了保障。

➤ 提供应用级防护

内嵌应用级防火墙功能，保护 Web 应用和 Web 服务免遭应用攻击，帮助企业提供全面的应用防护能力，保护企业的应用和数据安全。

➤ 开放平台架构

矩尺负载均衡设备采用开放平台架构，可以通过 API 与第三方云平台、操作管理平台、应用性能管理平台、大数据平台、安全运营平台等进行无缝对接。

➤ 支持云原生环境

在云原生环境中，为 kubernetes 提供 Load Balance 服务或者 Ingress Controller 服务，并可在 Kubernetes 系统中提供 Service Mesh 服务。

➤ 定制化开发增值服务

矩尺网络科技为客户提供基于负载均衡设备的定制化开发服务，帮助用户优化应用场景，提供可持续发展的应用增值服务。

2.2 应用场景功能列表

序号	功能名称	功能描述
1	应用服务均衡场景	基于负载均衡算法将每个连接快速的分配到相应的可用服务器，支持场景包括： <ul style="list-style-type: none">● L4 负载均衡● L7 负载均衡
2	应用服务器健康检查	通过健康检查判断后端服务的可用性，类型包括 <ul style="list-style-type: none">● http, https● tcp● icmp● 上传自定义脚本满足特殊需求
3	负载均衡算法	支持多重负载均衡算法将所有流量均衡的分配到各个服务器，类型包括： <ul style="list-style-type: none">● 轮询● 最小连接数● 基于源地址的一致性 Hash
4	会话保持机制	为访问用户选择曾连接上的特定服务器，实现无缝地处理用户请求；减少新建连接。类型包括： <ul style="list-style-type: none">● 基于源地址● 基于 Hash● 基于 Cookie Insert● 基于 Cookie Hash● 基于 Cookie Passive
5	源地址转换	对发起访问的客户端 IP 进行地址转换，可以支持： <ul style="list-style-type: none">● 设备接口 IP● 自定义地址池中的 IP
6	溯源	对进行了源地址转换的客户端进行溯源，支持主要方式包括： <ul style="list-style-type: none">● x-forward-for● proxy protocol
7	部署架构	在网络架构中可以根据需求进行灵活部署，支持架构包括： <ul style="list-style-type: none">● 旁路模式● 串行模式
8	http 重定向	对于 https 提供服务的应用，将客户端的 http 访问重定向至 https
9	SSL 卸载	将应用访问过程中 SSL 的加解密工作转到负载均衡设备上，从而减少服务器端的性能压力。

10	应用性能优化	通过应用性能优化机制，缩短服务器响应时间，主要包括： <ul style="list-style-type: none">● TCP 连接复用● HTTP 压缩
11	应用失效保障页面	应用业务失效后，返回一个告警或者提醒页面
12	访问控制	访问控制白名单、黑名单、设备限速、并发连接限制、基本认证 Realm

2.3 产品技术架构

2.3.1 应用服务均衡场景

➤ L4 负载均衡

在实现 L4 服务器负载均衡的场景中，矩尺负载均衡设备负责将客户端的请求转发给服务器，然后客户端与服务器之间建立 TCP 连接，此时矩尺负载均衡设备所扮演的设备类似于一台路由器或者防火墙。

➤ L7 负载均衡

基于七层内容的调度机制，使得管理员可以通过应用层的内容交换来分配服务器资源，以实现用户请求调度的多元化和个性化，业务应用的场景十分广泛。例如，基于 URL、HOST、COOKIE、USER_AGENT 等 HTTP 头部内容的匹配策略来选择服务器，或者通过对 HTTP 头部进行请求改写和应答改写，执行页面跳转和丢弃等操作，实现不同业务系统之间的交互联动。在 L7 服务器负载均衡的场景中，矩尺负载均衡设备先与客户端建立 TCP 连接，获取到访问请求的报文之后，再根据报文中所带的应用层内容来选择合适的服务器并与之建立 TCP 连接，此时矩尺负载均衡设备所扮演的角色类似于一台代理服务器。

2.3.2 应用服务器健康检查

矩尺负载均衡设备可以通过健康检查判断后端服务的可用性，避免服务分发到不可用的服务器上，支持多种方式。

➤ 基于设备网络通信状态的健康检查

通过 PING 等方式监控服务器的运行状况，一旦出现 ping 无回包，都可以实时将访问请求分配到其他正常的服务器之上。

➤ **基于 L4 协议的健康检查**

通过检查服务器 TCP、UDP 端口的通信情况来确定应用的运行情况，一旦检查失败，都可以实时将访问请求分配到其他正常的服务器之上。

➤ **基于 L7 应用层协议的健康检查**

通过监控服务器的应用层协议的运行情况，比如 http、https、grpc 等，发送指定的代码并判断返回值确定当前应用的健康状态，来确定服务的运行情况，一旦检查失败，都可以实时将访问请求分配到其他正常的服务器之上。

➤ **基于上次脚本完成健康检查**

通过上传自定义脚本，综合监控服务器的运行状态，满足健康检查的复杂要求，例如多条件健康检查、关联应用健康检查。

2.3.3 负载均衡算法

矩尺负载均衡设备支持多重负载均衡算法将所有流量均衡的分配到各个服务器，以达到充分利用服务器资源的目的，而且保证各个服务器均衡的承担流量处理任务，从而有效地避免服务器处理任务“不平衡”现象的发生。

➤ **轮询**

实现机制：按照请求的先后顺序将用户请求基于节点权重循环地分配到每台服务器。一旦某台服务器出现故障将不在为其分配任务，直至服务器恢复正常。属于静态负载均衡算法。

适用场景：服务器集群中各台服务器的性能有明确预期。

➤ **最小连接数**

实现机制：监控服务器的连接数，按照请求的先后顺序将用户请求分配到连接数最小的服务器上。一旦某台服务器出现故障将不在为其分配任务，直至服务器恢复正常。属于动态负载均衡算法。

适用场景：各台服务器的性能存在差异，并且不同用户发起的连接保存时长差异较大。

2.3.4 优先级分组

通过启用优先级分组, 允许用户对服务器池中的节点设置优先级。这样, 当相同优先级的高优先级分组中节点可用时, 就不会使用低优先级节点。

2.3.5 温暖上线

将新购置或维护后的服务器添加到服务器时, 设备可以通过温暖上线方式, 避免新服务器由于激增流量的冲击而导致系统故障, 实现服务器的平滑进入。当新服务器上线后, 在其恢复时间内, 设备不会向该服务器发送请求; 而在随后的温暖时间以内, 设备则会逐渐地增加分配到该服务器地请求, 使新服务器地压力缓慢增加到稳定状态, 从而保证服务器在启动期间以及应用程序初始化时都能提供不间断服务。

2.3.6 会话保持机制

通过会话保持机制可以识别客户与服务器之间交互过程的关连性, 在实现负载均衡的同时, 还可保证一系列相关连的访问请求会保持分配到同一台服务器之上。

➤ 基于源地址的会话保持机制

设备在作负载均衡时是根据访问请求的源地址作为判断关联会话的依据, 对来自同一 IP 地址的所有访问请求在做负载均时都会被保持到一台服务器上去。

➤ 基于 Cookie hash 的会话保持机制

使用 Hash 方式, 会根据配置的 cookie 名称, 将指定名称的 cookie 值进行 hash, 并将该值和选中的服务器节点保存在会话保持列表中, 设置超时时间, 后续请求在超时时间内携带了之前的 cookie, 与会话保持列表中的记录进行对比, 如果匹配则按照记录进行转发, 如果不匹配或者超出超时时间则执行新的负载算法。

➤ 基于 Cookie 插入的会话保持机制

利用 HTTP 协议中的 Cookie 功能来实现会话保持功能。当客户端的请求中带有设备设置的 Cookie 信息，则设备根据 Cookie 中的信息来选择服务器；当客户端的请求中没有 Cookie 信息，则设备按照算法选择服务器，同时，在服务器响应的 response 头部中，插入 Cookie 信息来实现会话保持，值为特定加密后的数据。

➤ **基于 Cookie Passive 的会话保持机制**

实现机制与 Cookie Insert 类似，都是通过客户端存储的 Cookie 信息来作为访问请求的调度依据；不同的地方在于，该 cookie 由后端服务器生成，同时与负载设备约定好相同的加密算法和私钥。

2.3.7 源地址转换

源地址转换是只在客户端访问的过程中，设备将客户端的 IP 地址转换成特定 IP 进行真实服务器的访问，此方案既可以保护内网 IP 的安全性，又可以解决设备旁路部署的来回路径不一致问题。

➤ **转换成设备接口 IP**

将客户端 IP 地址转换成设备物理接口地址发起对真实服务器的访问，访问真实服务器的实际源地址为设备接口 IP。

➤ **转换成自定义地址池中的 IP 地址**

将客户端 IP 地址转换成自定义地址池中的某个 IP 地址，访问真实服务器的实际源地址为地址池中的 IP 地址。

2.3.8 溯源

设备支持对源地址转后后的客户端进行溯源，即保持原有实际源地址的可读性。

➤ **x-forward-for**

HTTP 协议自带，在 HTTP 扩展头部中插入客户端实际源 IP 地址信息。

➤ proxy protocol

在 4 层末尾和 7 层开头之间插入客户端实际源 IP 地址信息。

2.3.9 SSL 卸载

SSL 卸载技术是通过将应用访问过程中 SSL 的加解密过程转到负载均衡设备之上，从而减少服务器端的性能压力，提升客户端的访问响应速度。矩尺负载均衡设备具有强劲的 SSL 处理能力，不但能够实现端到端的 SSL 加密，同时支持全面的加密算法配置，并可管理服务器证书。

矩尺负载均衡设备通过对服务器的 SSL 卸载处理，在减少服务器性能消耗的同时，节省应用系统服务器数量，降低了业务系统的硬件投资，并大幅度缩短用户请求的响应时间从而极大提升了用户的访问体验。

2.3.10 分发策略与分发规则

在同一个虚拟服务内，可以创建多条具备不同优先级的分发规则，每条分发规则可以指定请求路由到不同的服务器池，亦或是返回重定向响应等，这样命中虚拟服务的请求就会根据分发规则转发不同的服务器池。其中，每条分发规则包含多条分发策略，而分发策略是基于源地址、URL、COOKIE 等请求信息生效的。

2.3.11 应用性能优化

➤ TCP 连接复用

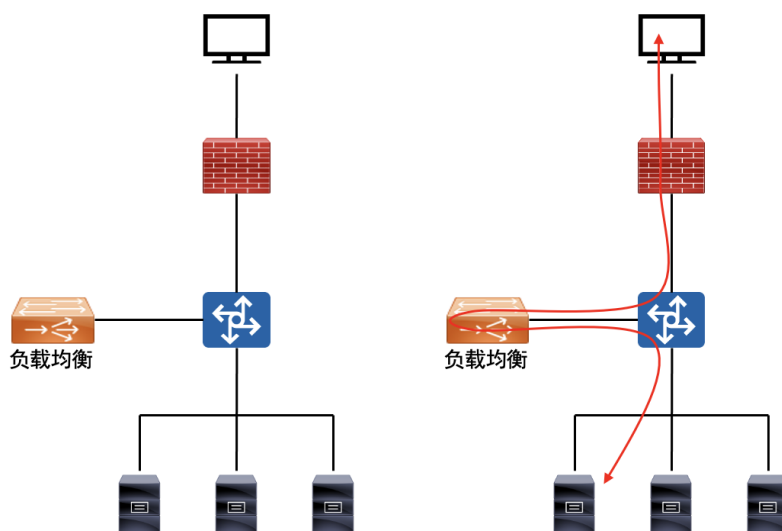
将众多客户端访问请求捆绑处理，通过将前端多个客户的 HTTP 请求复用到后端与服务器建立的一个 TCP 连接上，不用一对一的方式把每一个 HTTP/TCP 连接从客户端传递到服务器，减少与服务器之间由于新建 TCP 连接所带来的延迟，并能够最大限度的降低客户端请求对后端服务器并发连接数的需求。解决 TCP/IP 协议在处理 HTTP 请求时的低效率问题，通过该技术，能够大大改善现有系统的总体性能。

➤ HTTP 压缩

通过标准的 HTTP 压缩技术 (HTTP Compression)，对指定的内容进行压缩，从而可以在不增加额外的网络带宽的情况下加快用户的响应速度，提高整体系统的性能。

2.4 部署架构

2.4.1 旁路模式

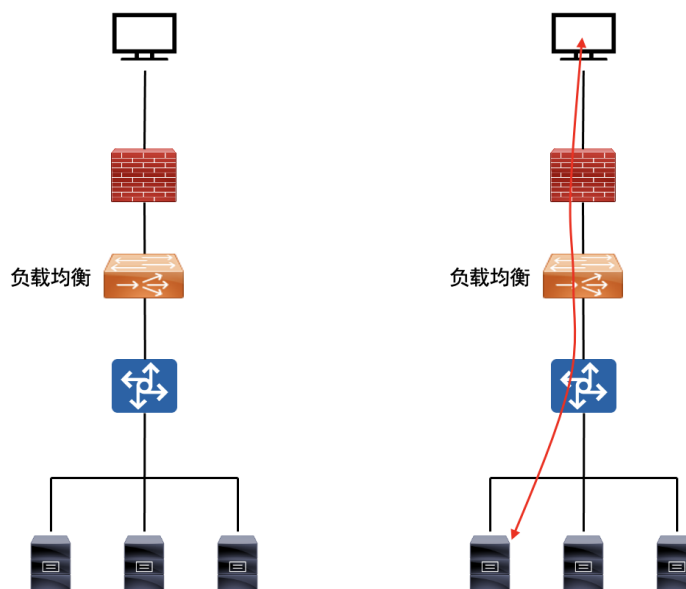


负载均衡设备以旁路模式部署到网络之中，此种模式不会改变客户的网络结构，同时设备上架时不会造成业务的中断，可以实现设备的快速简单部署。数据流如下所示：

步骤	说明
1	客户端发送服务访问请求，此时的源 IP 为客户端 IP、目的 IP 为负载均衡设备定义的虚拟服务器 IP
2	负载均衡设备接收到访问请求后，根据定义的负载均衡算法判断出应该将访问请求分发给哪台服务器
3	负载均衡设备使用 SNAT 技术分发访问应用请求，此时的源 IP 为 SNAT IP、目的 IP 为真实服务器 IP
4	真实服务器处理接收到的访问请求，回复响应数据，此时的源 IP 为真实服务器 IP、目的 IP 为 SNAT IP

5	负载均衡设备接收响应数据，反向 SNAT 将源 IP 后转回真实客户端 IP 再转发给客户端，此时的源 IP 为虚拟服务器 IP、目的 IP 为客户端 IP
---	--

2.4.2 串行模式



负载均衡设备以路由模式部署到网络之中，此种模式将负载均衡设备串行部署到网络架构中，需要对网络架构进行适配调整，但此种部署方式可以规避源地址转换，从而简化应用溯源的难度。数据流如下所示：

步骤	说明
1	客户端发送服务访问请求，此时的源 IP 为客户端 IP、目的 IP 为负载均衡设备定义的虚拟服务器 IP
2	负载均衡设备接收到访问请求后，根据定义的负载均衡算法判断出应该将访问请求分发给哪台服务器
3	负载均衡设备使用 SNAT 技术分发访问应用请求，此时的源 IP 为 SNAT IP、目的 IP 为真实服务器 IP
4	真实服务器处理接收到的访问请求，回复响应数据，此时的源 IP 为真实服务器 IP、目的 IP 为 SNAT IP
5	负载均衡设备接收响应数据，反向 SNAT 将源 IP 后转回真实客户端 IP 再转发给客户端，此时的源 IP 为虚拟服务器 IP、目的 IP 为客户端 IP

2.5 设备高可用性

矩尺负载均衡设备提供设备自身高可用性支持，采用冗余结构防止由于自身设备故障带来的业务停机。两台设备只有一台在处理流量，另外一台不处理流量处于备份状态，随时准备接管主设备的业务处理。

2.5.1 主备切换

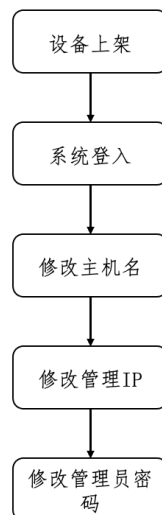
矩尺平台的高可用分为管理面主备切换和业务面主备切换，其中，管理面在【平台系统】/【设备管理】中切换主节点，业务面在【SLB 本地负载】/【流量组管理】/【流量组】中，基于创建的流量组实现每个流量组内的主节点切换。

管理面主备切换参见“4.7.1 设备管理”章节的“主备切换”介绍；

业务面主备切换参见“4.6.8.2 流量组”章节的“主设备切换按钮”介绍。

3 基础配置流程介绍

3.1 系统初始化



➤ 设备上架

矩尺负载均衡 NM-L-1000 为一台 2U 设备，使用自带导轨进行安装上架。

➤ 系统登入

使用管理口 IP 进行 web 登陆，出厂 IP 地址为 192.168.1.245。

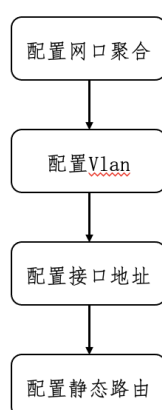
➤ 修改主机名

进入“平台系统→设备管理”，修改主机名及管理 IP。

➤ 修改管理员密码

点击 web 右上角，修改管理员密码。

3.2 基础网络配置



➤ 配置网口聚合（可选）

进入“网络管理→网口聚合”菜单配置网口聚合，实现网络接口冗余或带宽增加。

➤ 配置 Vlan

进入“网络管理→VLAN 管理”配置 Vlan，实现网络接口 Vlan 标签的 tag 或 untag 透传。

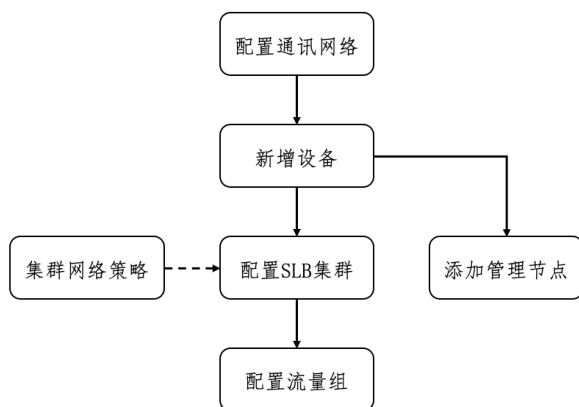
➤ 配置接口地址

进入“网络管理→接口地址”配置 Vlan 的接口 IP 地址。

➤ 配置静态路由

进入“网络管理→路由管理”，选择“静态路由表”添加所需的静态路由。

3.3 平台与集群管理



➤ 配置通讯网络

矩尺负载均衡管理系统使用通讯网络构建平台统一管理的数据传输及状态监控网络，通讯网络可复用业务网络或者管理网络。

➤ 新增设备

进入“平台系统→设备管理”，点击列表上方【新增】按钮，可将其他设备增加至此设备管理系统中，实现统一管理。

➤ 添加管理节点（可选）

将新增的设备添加为管理节点，组成双机互备的高可用管理集群。

➤ 配置 SLB 集群

进入“平台系统→SLB 集群管理→集群配置”可新增 SLB 集群，将平台中的设备添加进入一个 SLB 集群，实现集群管理，SLB 集群需要调用集群网络策略。

➤ 集群网络策略

进入“平台系统→SLB 集群管理→集群网络策略”可新增、修改、删除集群网络策略。

➤ 配置流量组

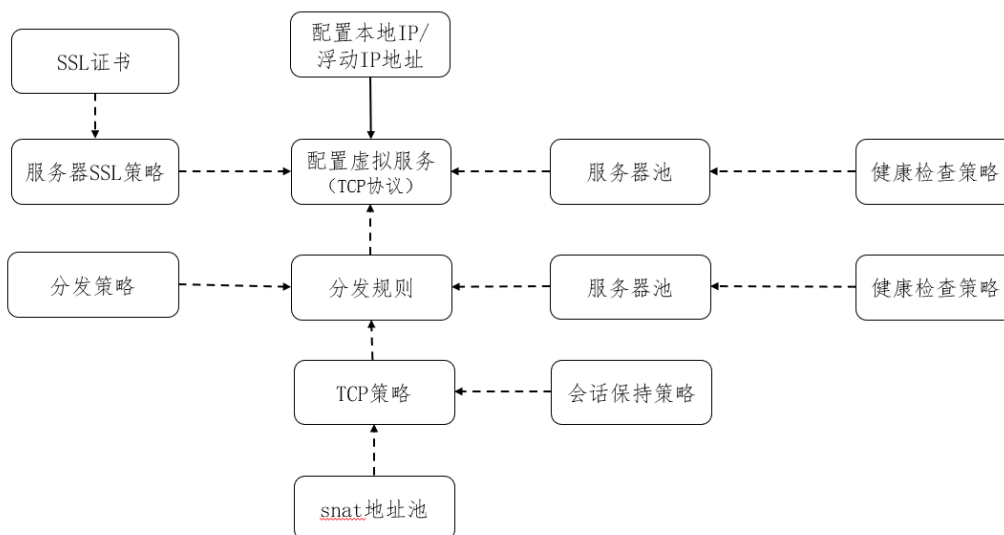
进入“SLB 本地负载→流量组管理→流量组”，为负载均衡业务配置流量组，实现负载均衡业务双机功能。

3.4 单台设备管理

我们的管理系统将新开一个页面展示单台设备信息和配置这台设备的网络，具体功能有设备信息、路由管理、本地 IP、网络接口、网口聚合、VLAN 管理、日志管理、数据统计。详情见 4.6 章节。

3.5 负载均衡业务管理

3.5.1 TCP 类型负载均衡业务



➤ 配置本地 IP/浮动 IP 地址

根据单机或者双机部署，为负载均衡业务配置本地 IP 或者浮动 IP 地址，该 IP 地址作为后续虚拟服务监听地址使用。

➤ 配置虚拟服务

进入“SLB 本地负载→虚拟服务”，新增虚拟服务，配置虚拟服务类型选择 TCP 协议，为该虚拟服务选择服务器池、TCP 策略及配置其他相关参数。

➤ 服务器池

进入“SLB 本地负载→服务器池”，配置服务器池相关服务节点（节点地址路由可达），并为其选择监控检查策略。

➤ 健康检查策略

进入“SLB 本地负载→健康检查”配置健康检查策略，为服务器池提供健康检查支持。

➤ TCP 策略

进入“SLB 本地负载→策略配置→四层策略”配置 TCP 策略，为其选择会话保持策略、配置 snat 方式并选择 snat 地址池、配置溯源等其他配置参数。

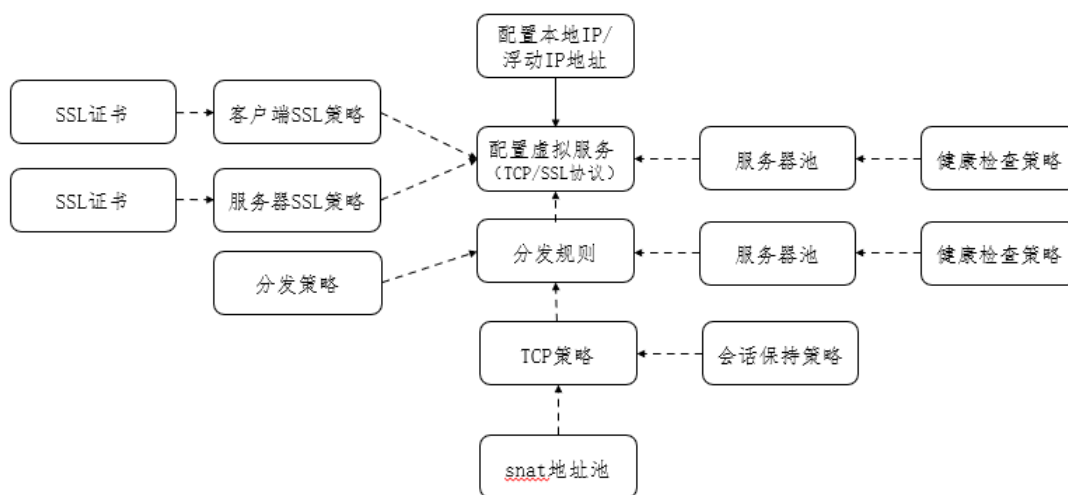
➤ 会话保持策略

进入“SLB 本地负载→策略配置→会话保持策略”根据会话保持要求配置基于源地址、基于 cookie 等方式的会话保持策略。

➤ snat 地址池

进入“SLB 本地负载→流量组管理→SNAT 地址池”，为本地负载均衡业务流程配置源地址转换地址池，可以使用本地 IP 或者自定义 IP（要求外部访问路由可达）。

3.5.2 TCP/SSL 类型负载均衡业务



TCP/SSL 类型负载均衡业务相较于 TCP 类型负载均衡业务需要配置 SSL 证书及 SSL 策略。

➤ 配置虚拟服务

进入“SLB 本地负载→虚拟服务”，新增虚拟服务，配置虚拟服务类型选择 TCP/SSL 协议，为该虚拟服务选择服务器池、TCP 策略及配置其他相关参数。

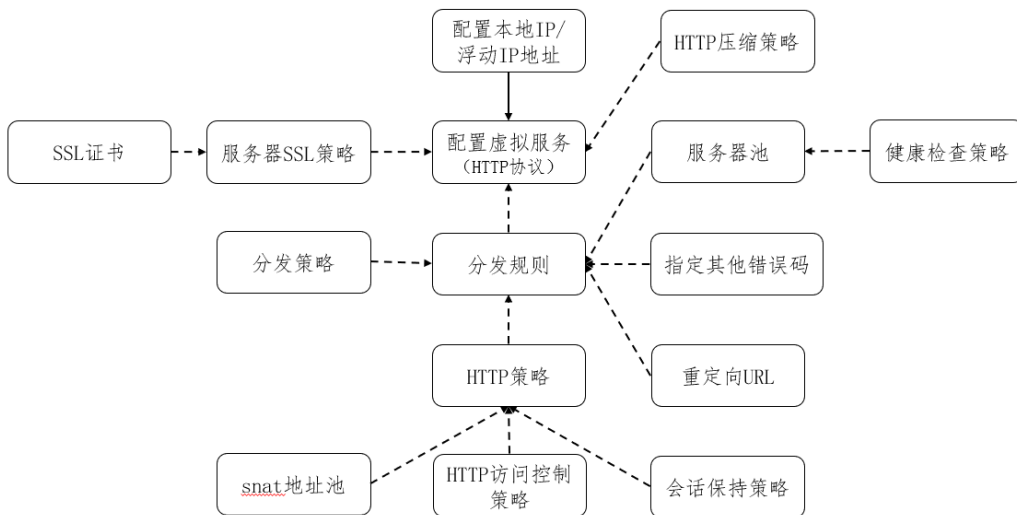
➤ SSL 证书

进入“平台系统→SSL 证书管理”，可为客户端访问负载均衡设备提供证书。

➤ SSL 策略

进入“SLB 本地负载→策略配置→SSL 策略”，为 SSL 策略配置控制 SSL 安全套件、Session 缓存、Session Ticket 等参数。

3.5.3 HTTP 类型负载均衡业务



➤ 配置本地 IP/浮动 IP 地址

根据单机或者双机部署，为负载均衡业务配置本地 IP 或者浮动 IP 地址，该 IP 地址作为后续虚拟服务监听地址使用。

➤ 配置虚拟服务

进入“SLB 本地负载→虚拟服务”，新增虚拟服务，配置虚拟服务类型选择 HTTP 协议，为该虚拟服务选择 HTTP 通配策略或者按照详细访问的 URL 增加 URL 策略。

➤ HTTP 策略

进入“SLB 本地负载→策略配置→七层策略”下的 HTTP 策略页签，为其选择 HTTP 策略及配置其他相关参数。

➤ 服务器池

进入“SLB 本地负载→服务器池”，配置服务器池相关服务节点（节点地址路由可达），并为其选择监控检查策略。

➤ 健康检查策略

进入“SLB 本地负载→健康检查”配置健康检查策略，为服务器池提供健康检查支持。

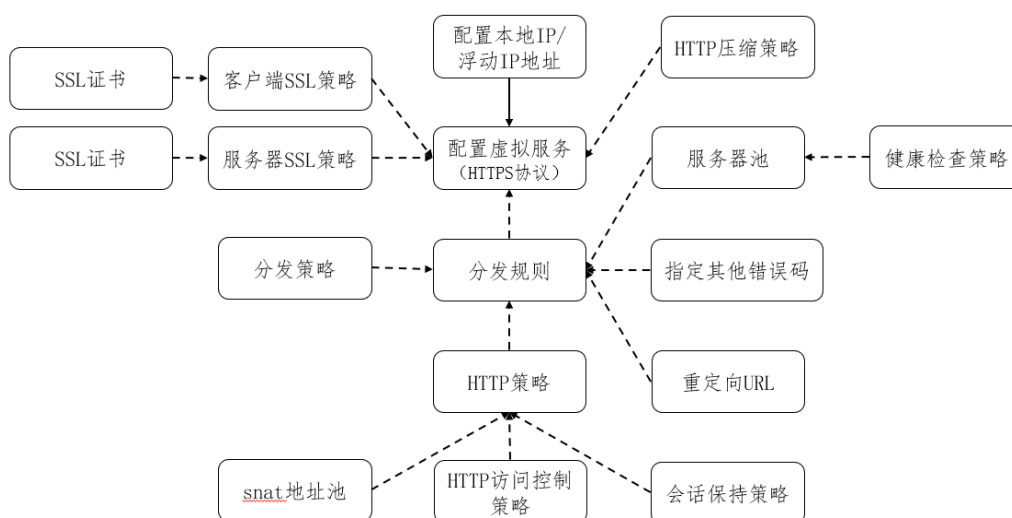
➤ 会话保持策略

进入“SLB 本地负载→策略配置→会话保持策略”根据会话保持要求配置基于源地址、基于 cookie 等方式的会话保持策略。

➤ snat 地址池

进入“SLB 本地负载→流量组管理→SNAT 地址池”，为本地负载均衡业务流程配置源地址转换地址池，可以使用本地 IP 或者自定义 IP（要求外部访问路由可达）。

3.5.4 HTTPS 类型负载均衡业务



HTTPS 类型负载均衡业务相较于 HTTP 类型负载均衡业务需要配置 SSL 证书及 SSL 策略。

➤ 配置虚拟服务

进入“SLB 本地负载→虚拟服务”，新增虚拟服务，配置虚拟服务类型选择 HTTPS 协议，为该虚拟服务选择 HTTP 通配策略或者按照详细访问的 URL 增加 URL 策略。

➤ SSL 证书

进入“平台系统→SSL 证书管理”，可为客户端访问负载均衡设备提供证书。

➤ SSL 策略

进入“SLB 本地负载→策略配置”，为 SSL 策略配置控制 SSL 安全套件、Session 缓存、Session Ticket 等参数。

4 详细操作手册

4.1 设备上架

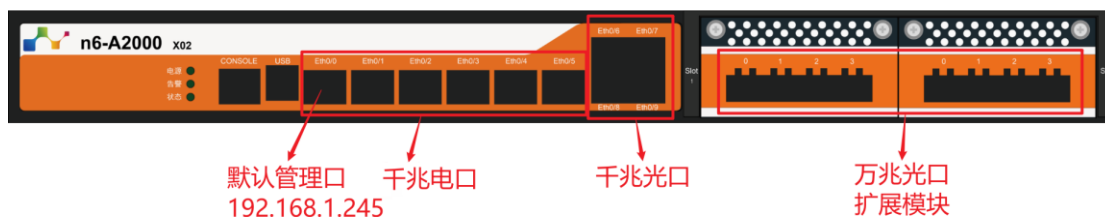
4.1.1 环境要求

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施，保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

4.1.2 产品面板

目前矩尺拥有以下两款负载均衡设备，分别是 n6-A2000 X02 和 n6-A2000 A02。

n6-A2000 X02 型号，拥有 6 个千兆电口、4 个千兆光口，右侧是 8 个万兆光口扩展模块，如下图所示：



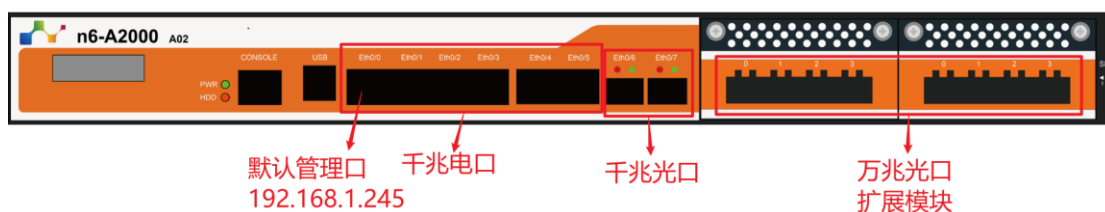
- Console：串口使用（仅定位疑难问题使用）。

当设备无法访问时，可以使用 USB 转串口调试线，连接设备串口。您可以使用 xshell 等工具的 serial 连接方式，其中频率设置为 115200，即可通过 SHELL 方式连接到设备。设备初始用户名 root，密码 n6_normae。如需修改密码，参见“4.8.1 设备管理”章节的**修改命令行密码**。

- USB：USB 插口，可用于系统恢复或数据导出。
- eth0/0-9：板载网络模块的 10 个网口。

面板右侧是两个万兆光口扩展模块，每个模块的 1，2，3，4 分别标记该模块四个网口。

n6-A2000 A02 型号，拥有 6 个千兆电口、2 个千兆光口，右侧是 8 个万兆光口扩展模块，如下图所示：



- Console：串口使用（仅定位疑难问题使用）。

当设备无法访问时，可以使用 USB 转串口调试线，连接设备串口。您可以使用 xshell 等工具的 serial 连接方式，其中频率设置为 115200，即可通过 SHELL 方式连接到设备。设备初始用户名 root，密码 n6_normae。如需修改密码，参见“4.8.1 设备管理”章节的**修改命令行密码**。

- USB：USB 插口，可用于系统恢复或数据导出。

- eth0/0-7：板载网络模块的 8 个网口。

面板右侧是两个万兆光口扩展模块，每个模块的 1，2，3，4 分别标记该模块四个网口。

面板最左侧的 LED 屏幕会在不同的操作情况下显示不同的文字信息。

- ◆ 启动/关机：显示设备序列号和运行时间
- ◆ 正常状态：显示设备名称和管理地址
- ◆ 备份配置：显示备份文件名称和时间
- ◆ 恢复配置：显示“恢复配置中”及时间

4.1.3 操作步骤

准备工具

- ✧ 本地 Windows PC 或苹果机子一台
- ✧ RJ45 网线一根

请确认使用的本地机子网页浏览器为 Firefox 、Google Chrome、Microsoft Edge、或者 Safari，用于登录矩尺负载设备管理系统。

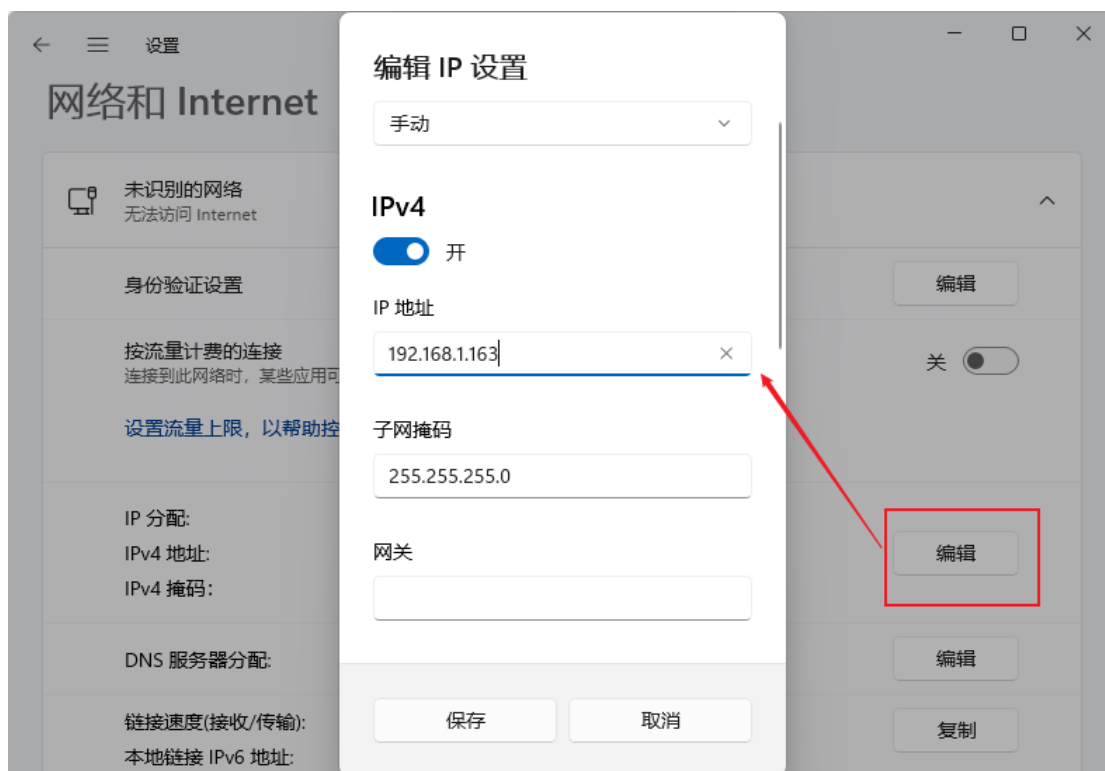
注意：默认使用 eth0/0 作为管理口。

1. 连接设备

使用准备好的网线将本地机子与矩尺负载设备的管理口相连，启动设备。

2. 配置本机网络

将本机 IP 配置为 192.168.1.x (windows 修改相应以太网的 IP 设置)。

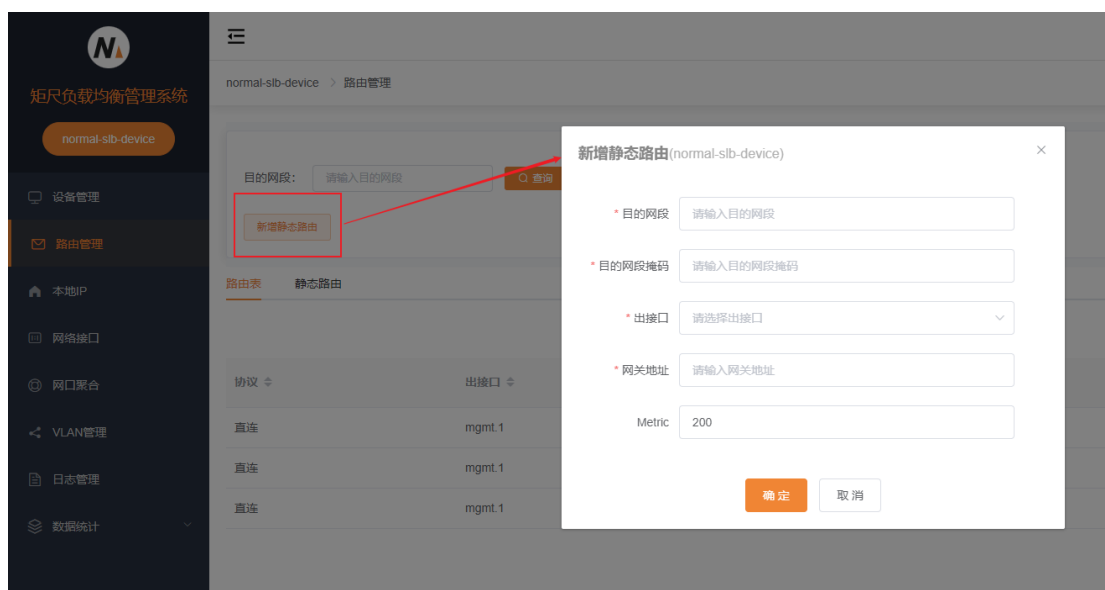


3. 登录设备

打开浏览器在地址栏输入 <https://192.168.1.245>，初始登录用户名为 admin，密码为 default，登陆成功后自动跳转到设备管理页面，显示设备状态为在线。

4. 配置管理路由

进入单台设备管理页面，在路由管理中增加管理端网络的路由配置（例如出接口、网关地址等）。



5. 修改管理地址

进入这台设备的设备管理页面，修改管理地址为内网管理地址。



6. 连接上架

将设备管理口与内部局域网连接，完成上架。

7. 验证管理地址

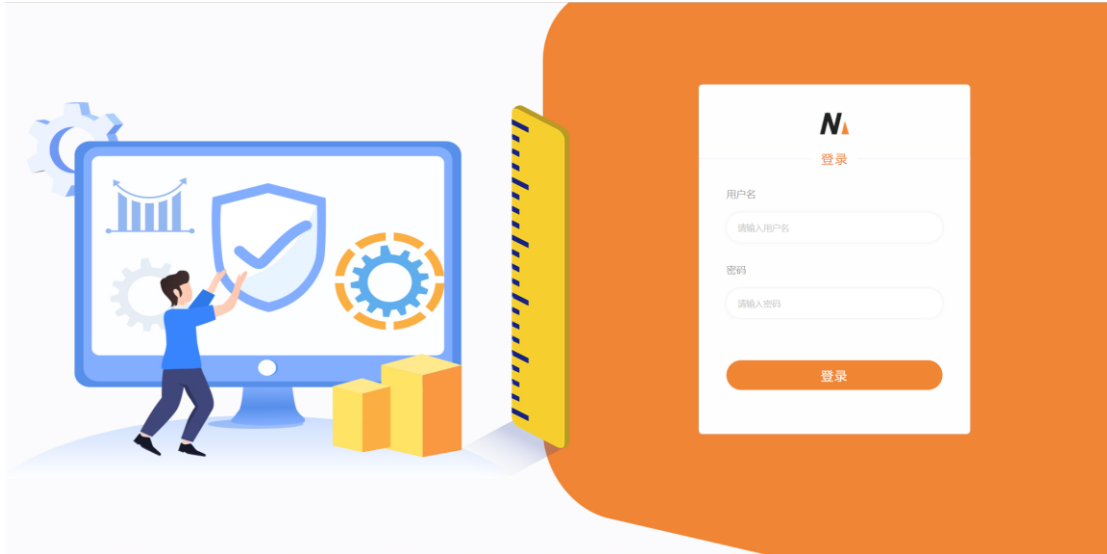
用内网同一网段内的机子登录修改后的管理地址，可正常登录矩尺负载设备管理系统。

8. 验证 ipmi 口

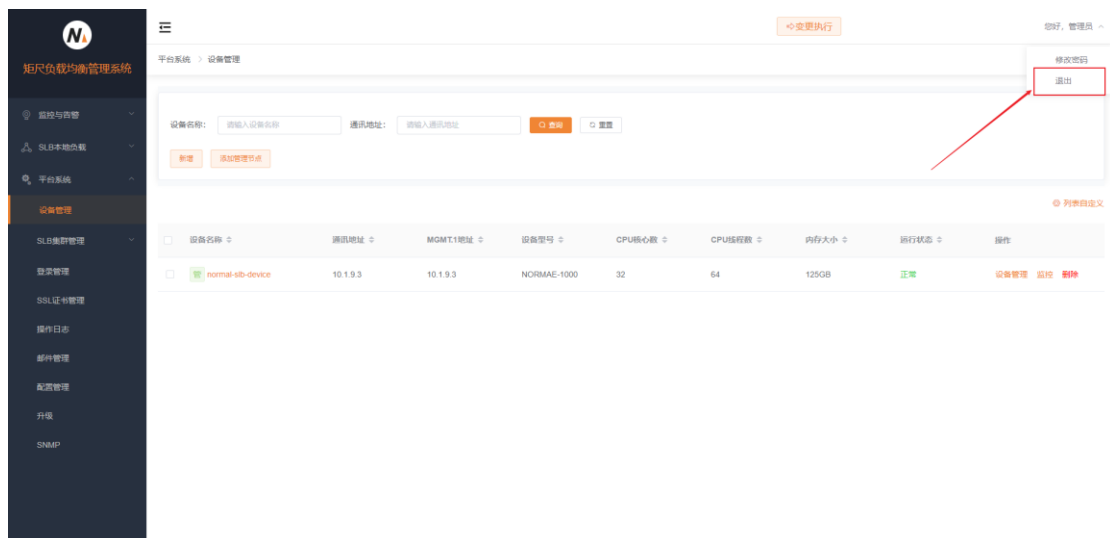
将本地机子 ip 地址修改为 192.168.1.x，用网线连接本机与矩尺负载均衡设备的 ipmi 口，浏览器登录 <https://192.168.1.246>，验证是否正常访问 ipmi 系统。

4.2 系统登录与退出

在浏览器中输入地址进行访问，输入正确的用户名密码后登录系统。



登录系统后点击右上角退出按钮即可退出系统，系统默认跳转至登录页面。







4.2.1 密码修改


用户修改登录密码时，鼠标移到右上角的用户名会弹出下拉列表，点击修改密码即可弹出修改密码窗口。



4.3 状态显示

-  表示可用
-  表示不可用
-  表示异常
-  表示可用但被用户禁用

 表示不可用且被用户禁用

 表示异常且被用户禁用

例如：

服务器池：健康状态绿色圆圈表示节点全部健康，橙色三角形表示池中大于一个但非所有节点健康，红色菱形表示全部节点未通过健康检查。

虚拟服务：监控状态绿色圆圈表示其下所有服务器池全部健康，橙色表示其下所有服务器池中所有节点大于一个但非全部健康，红色表示其下所有服务器池的所有节点未通过健康检查。

4.4 网络接口名称

矩尺负载均衡设备的网络接口以 eth(数字)/(数字) 格式命名，斜杠左边数字 0 表示板载网络模块，其他正整数表示扩展网络模块的序号（软负载仅包含板载网络模块），斜杠右边数字表示同一网络模块内的网口序号，如 eth0/0 表示板载第一个网口，序号从左到右依次增加。

4.5 监控与告警

矩尺负载均衡管理系统对于服务器池、服务器节点、虚拟服务、设备状态都配备了监控系统，为数据统计和故障查找提供了直观有效的图形界面。

➤ 分析

在每一个模块的详情页面切换到导航中的【分析】标签进入该模块监控界面。



详见后面章节各模块中的【分析】介绍。这里主要介绍统一的交互功能：
导航的右边可切换时间，可选时间为：过去 1 小时、过去 6 小时、过去 1 天、过去 1 周。



我们将监控分析界面划分为五个区域，



B 区横坐标上方出现的事件点（系统事件为蓝色，操作事件为绿色），和线段上出现的黄色异常标记，它们表示该点之前一小段时间范围内发生的事件或异常集合。可点击图标查看详细信息，展示在 E 区的列表中（事件列表包括时间、资源类型、资源名称、事件类型、描述、详情；异常列表包括时间、异常类型、资源类型、资源名称、时间序列、偏差值）。



C 区高亮文字可点击跳转至对应名称的分析页面：



D 区每一个小折线图可点击查看大图，会在 B 区切换展示。每个小标题下面数字是当前的指标，当鼠标移入后所有图表都会联动展示该时间点对应的数值。

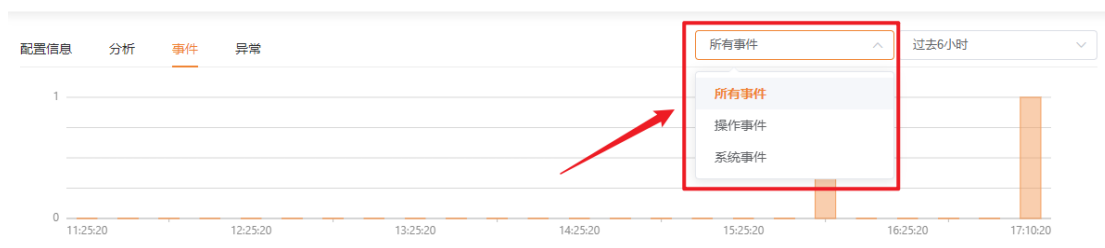


➤ 事件

在每一个模块的详情页面切换到导航中的【事件】标签进入该模块事件界面。



切换到【事件】标签时，右侧会多出一个事件类型选择框，可选“所有事件”、“操作时间”、“系统事件”。



事件界面分为两个区域：

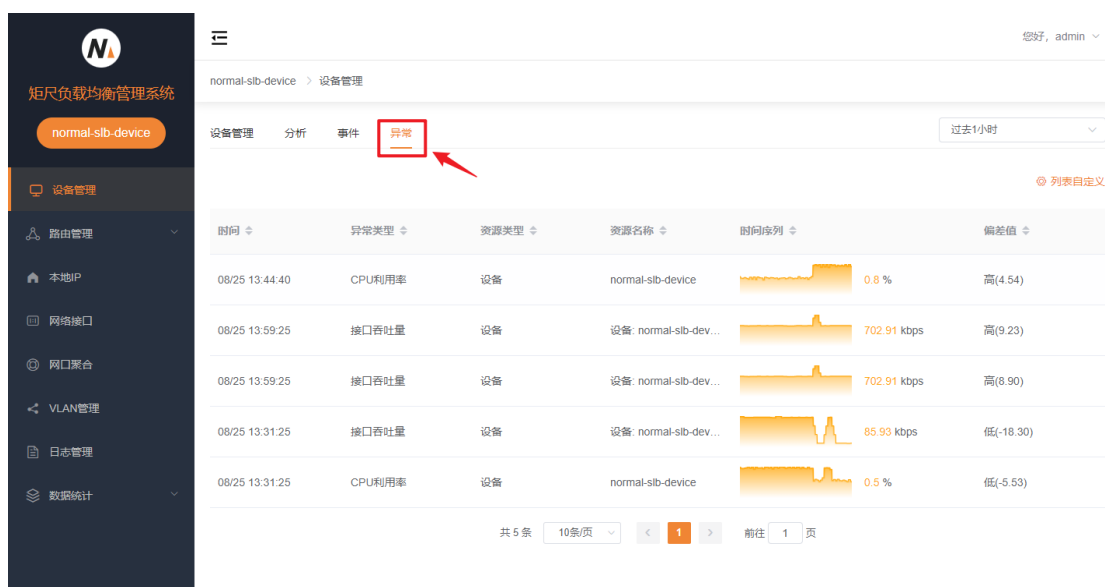


A 区是该资源类型在当前选择的时间段内对应事件类型下的所有的事件直方图，横轴表示时间，纵轴表示事件数量。B 区是对应的事件列表默认展示全部。可点击柱子在 B 区展示该段柱子时间范围内的事件，同时列表左上方时间会切换为这根柱子表示的时间段。



➤ 异常

在每一个模块的详情页面切换到导航中的【异常】标签进入该模块异常界面。



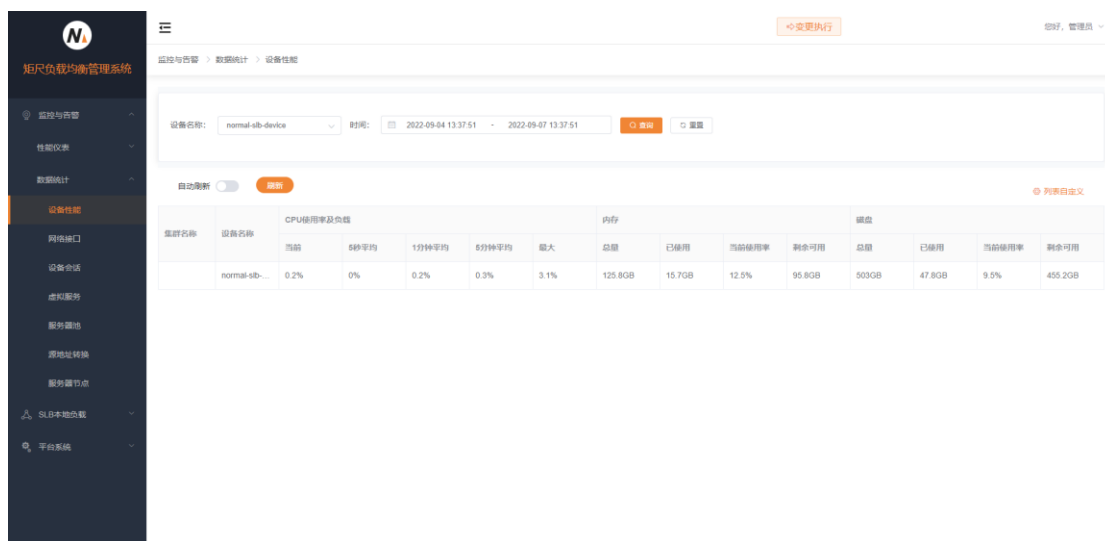
在【异常】标签下，展示的是所选时间范围内，该资源类型产生的所有异常的列表。表字段包括时间、异常类型、资源类型、资源名称、时间序列、偏差值。其中时间序列为一条折线图，表示该条异常产生时的数据波动，图形右侧数值表示当前数值，当鼠标移入图形时数值会变成鼠标所在时间点的数值。

4.5.1 数据统计

数据统计菜单主要以表格形式展示各项数据指标。

4.5.1.1 设备性能

点击“监控与告警→数据统计→设备性能”菜单，可以查看所有设备或者选择一台设备查看设备性能数据，包括从CPU使用率及负载、内存、磁盘三个维度进行统计的表格。



集群名称	设备名称	CPU使用率及负载					内存				磁盘			
		当前	5秒平均	1分钟平均	5分钟平均	最大	总量	已使用	当前使用率	剩余可用	总量	已使用	当前使用率	剩余可用
	normal-slb-device	0.2%	0%	0.2%	0.3%	3.1%	125.8GB	15.7GB	12.5%	95.8GB	503GB	47.8GB	9.5%	455.2GB

4.5.1.2 网络接口

点击“监控与告警→数据统计→网络接口”菜单，可以查看所有设备或者选择一台设备查看网络接口数据，包括从接口速率、字节、报文、错误、丢包、冲突等六个维度进行统计的表格。

设备名称	聚合接口	接口名称	连接状态	接口速率	字节		报文		错误		丢包		冲突
					接收	发送	接收	发送	接收	发送	接收	发送	
normal-slb-d...	-	1.0	打开	40000Mb/s	119.9MB	68.3MB	139.29万	85.85万	0B	0B	0	0	0
	-	2.0	打开	40000Mb/s	102.8MB	65.5MB	92.45万	75.33万	0B	0B	0	0	0

4.5.1.3 设备会话

点击“监控与告警→数据统计→设备会话”菜单，可以查看所有设备或者选择一台设备查看设备会话数据，包括从 Client 侧会话、Server 侧会话、Server 侧 SSL 连接三个维度进行统计的表格。

集群名称	设备名称	Client侧会话				Server侧会话				Server侧SSL连接	
		会话数/秒	会话合计	HTTP请求速率	HTTP请求合计	会话新建速率	会话合计	HTTP请求速率	HTTP请求合计	SSL新建速率	SSL连接合计
暂无数据											

4.5.1.4 虚拟服务

点击“监控与告警→数据统计→虚拟服务”菜单，可以查看所有虚拟服务或者选择一个虚拟服务查看虚拟服务数据，包括从开启状态、监控状态、传输速率、流量合计、会话、SSL 连接六个维度进行统计的表格。

N

矩尺负载均衡管理系统

监控与告警

性能仪表

数据统计

设备性能

网络接口

设备会话

虚拟服务

服务器节点

SLB本地负载均衡

平台系统

监控与告警

数据统计

虚拟服务

虚拟服务: 选择虚拟服务

时间: 2022-09-04 13:51:03 - 2022-09-07 13:51:03

查询

重置

自动刷新

刷新

列表自定义

流量组	虚拟服务	启动状态	监控状态	传输速率		流量合计		会话				SSL连接	
				输入速率	输出速率	输入	输出	会话新建速率	会话合计	HTTP请求速率	HTTP请求合计	SSL新建速率	SSL连接合计
	动态服务器...	开启		26.6B/秒	7.7B/秒	6.6MB	1.9MB	0	0	2.9次/分钟	1.25万	0	0

4.5.1.5 服务器池

点击“监控与告警→数据统计→服务器池”菜单，可以查看所有服务器池或者选择一个服务器池查看服务器池数据，包括从开启状态、监控状态、传输速率、流量合计、会话、SSL 连接六个维度进行统计的表格。

N

矩尺负载均衡管理系统

监控与告警

性能仪表

数据统计

设备性能

网络接口

设备会话

虚拟服务

服务器池

源地址转换

服务器节点

SLB本地负载均衡

平台系统

监控与告警

数据统计

服务器池

服务器池: 请选择虚拟服务

时间: 2022-09-04 13:54:33 - 2022-09-07 13:54:33

查询

重置

自动刷新

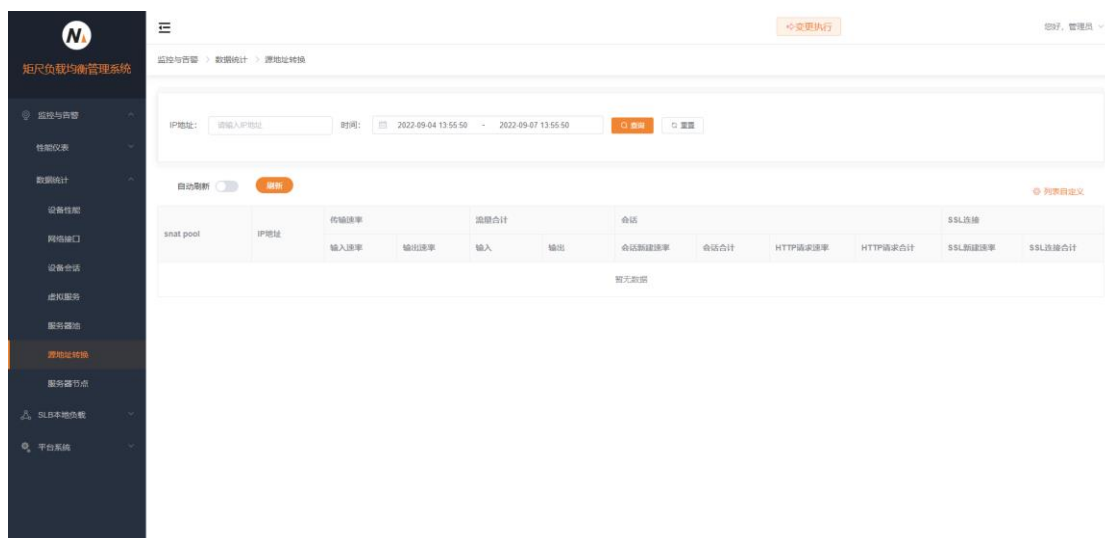
刷新

列表自定义

服务器池		开启状态	监控状态	传输速率		流量合计		会话		SSL连接			
				输入速率	输出速率	输入	输出	会话新建速率	会话合计	HTTP请求速率	HTTP请求合计	SSL新建速率	SSL连接合计
<div>resty-test-pool-mih</div>	开启	<div></div>		0.3B/秒	0.1B/秒	88KB	20.1KB	0	0	2.4次/小时	174.25	2.4次/小时	0
10.1.9.3.55455	开启	<div></div>		0.1B/秒	0B/秒	27.2KB	6.3KB	0	0	18.4次/天	55.09	18.4次/天	0
10.1.9.3.55456	开启	<div></div>		0.2B/秒	0.1B/秒	56.8KB	13.7KB	0	0	1.7次/小时	119.17	1.7次/小时	0

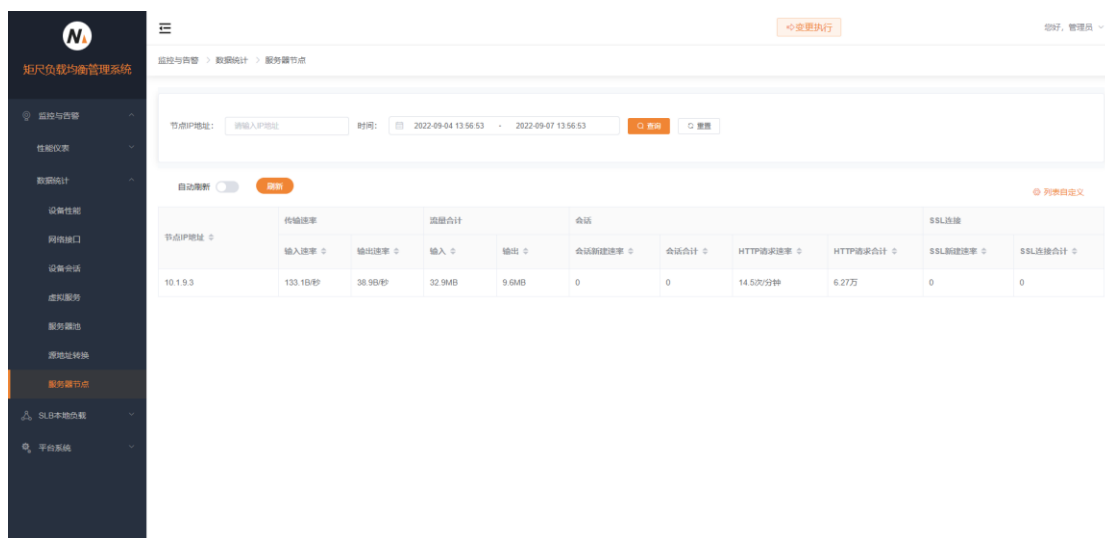
4.5.1.6 源地址转换

点击“监控与告警→数据统计→源地址转换”菜单，可以查看所有 IP 地址或者输入 IP 地址查询对应源地址转换数据，包括从传输速率、流量合计、会话、SSL 连接四个维度进行统计的表格。



4.5.1.7 服务器节点

点击“监控与告警→数据统计→服务器节点”菜单，可以查看所有 IP 地址或者输入节点 IP 地址查看节点数据，包括从传输速率、流量合计、会话、SSL 连接四个维度进行统计的表格。

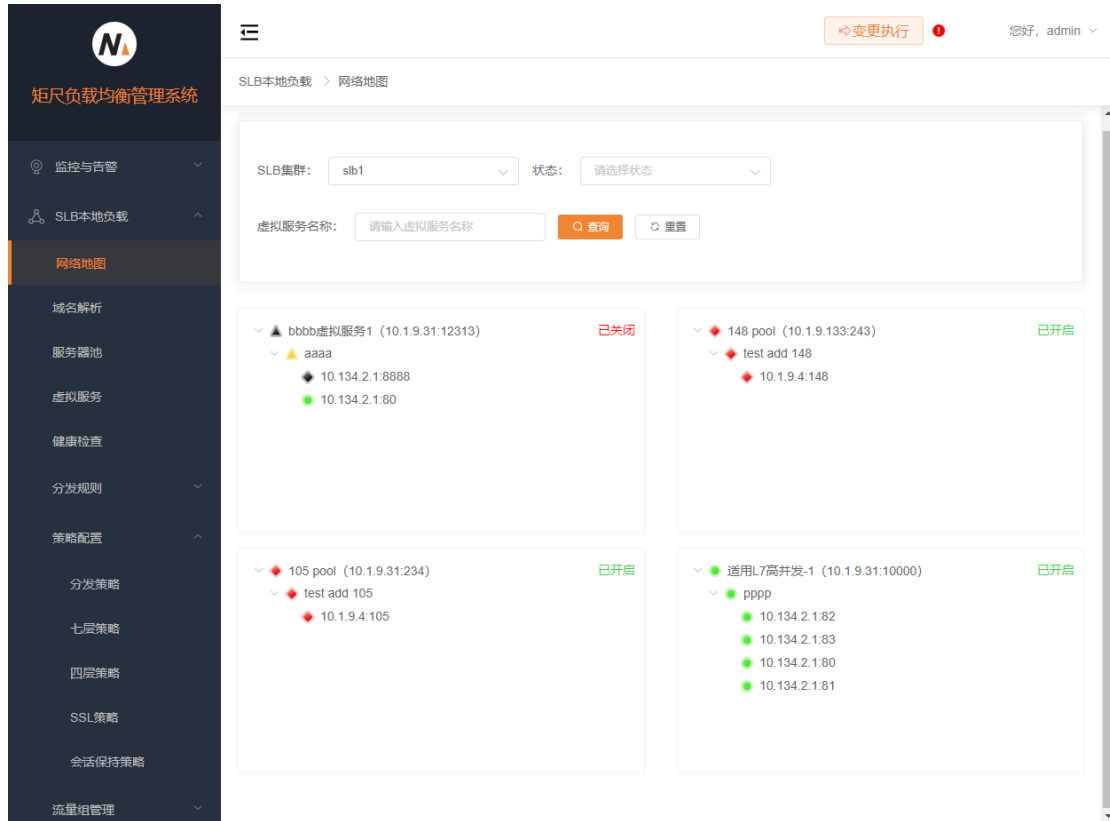


4.6 SLB 本地负载

4.6.1 网络地图

网络地图可以直观的展示每个虚拟服务及其使用的服务器池的状态。

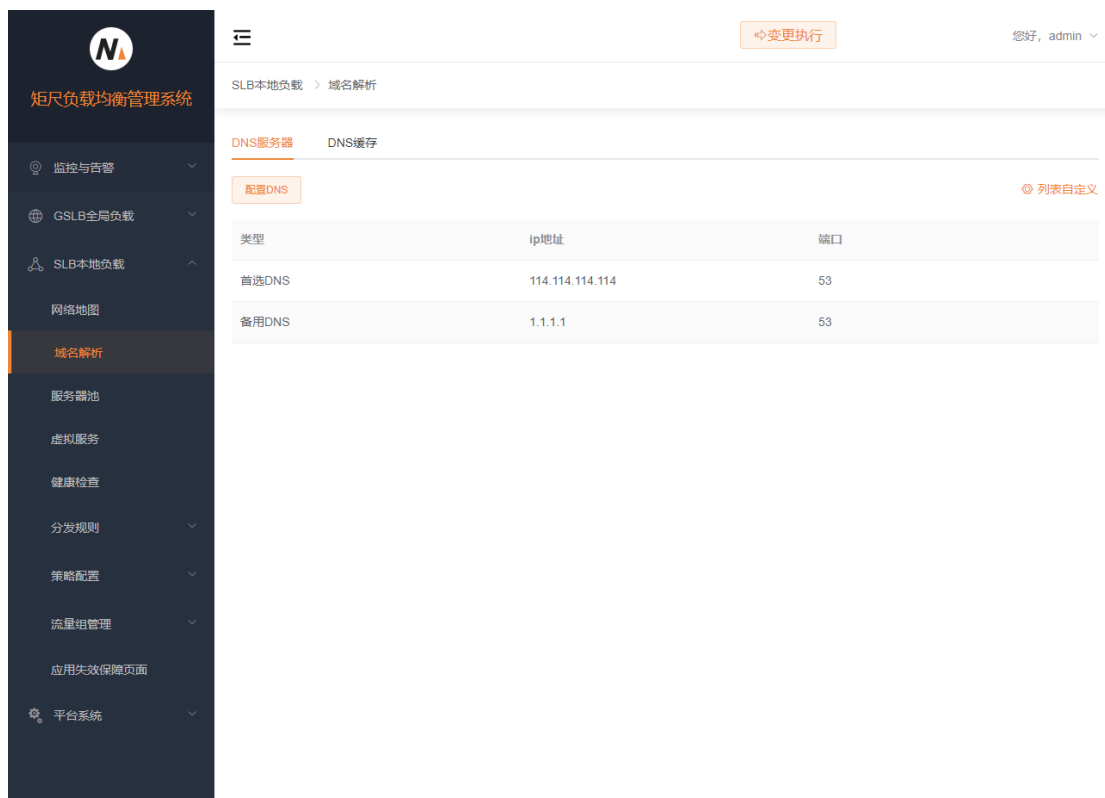
点击“SLB 本地负载→网络地图”菜单，默认展示当前已选择的 SLB 集群下已创建的虚拟服务的启用状态和监控状态。状态介绍详见【4.3 状态显示】章节



4.6.2 域名解析

点击“SLB 本地负载→域名解析”菜单，头部有两个 tab 标签：DNS 服务器、DNS 缓存。

默认展示 DNS 服务器配置列表。



修改 DNS 配置： 点击左上角【配置 DNS】按钮



查看 DNS 缓存： 点击头部标签“DNS 缓存”切换到 DNS 缓存列表，默认展示列表字段：域名、IP 地址、TTL，可按域名查询。

矩尺负载均衡管理系统

- 监控与告警
- GS LB全局负载均衡
- SLB本地负载均衡
- 网络地图
- 域名解析**
- 服务器池
- 虚拟服务
- 健康检查
- 分发规则

SLB本地负载均衡

域名解析

DNS服务器

DNS缓存

域名: 请输入域名

查询

重置

批量失效

列表自定义

<input type="checkbox"/>	域名	IP 地址	TTL	操作
<input type="checkbox"/>	qq.com	113.108.81.189	153	失效
<input type="checkbox"/>	baidu.com	110.242.68.66	253	失效
<input type="checkbox"/>	tt.com	75.2.32.234	65	失效

缓存失效：DNS 缓存列表中，在对应缓存条目右边点击【失效】按钮可使这条缓存失效。如果想要一次性失效多条，可点击左边多选框，勾选所有想要失效的缓存后，点击左上角【批量失效】按钮即可。

4.6.3 服务器池

服务器池是将两台或多台节点机(服务器)构成一种松散耦合的计算节点的集合，通过负载均衡算法的设置实现各个节点机的处理请求先后机制。

点击“SLB 本地负载→服务器池”菜单，默认按照服务器池创建时间倒序排列展示所有服务器池信息列表。吞吐量数字部分表示当前数据，当鼠标移入折线图时数字变为鼠标所在的纵坐标值。

矩尺负载均衡管理系统

- 监控与告警
- SLB本地负载均衡
- 网络地图
- 服务器池**
- 虚拟服务
- 健康检查
- 分发规则
- 策略配置
- 流量组管理
- 应用失效保障页面
- 平台系统

SLB本地负载均衡

服务器池

服务器池名称: 请输入服务器池名称

查询

重置

新增

列表自定义

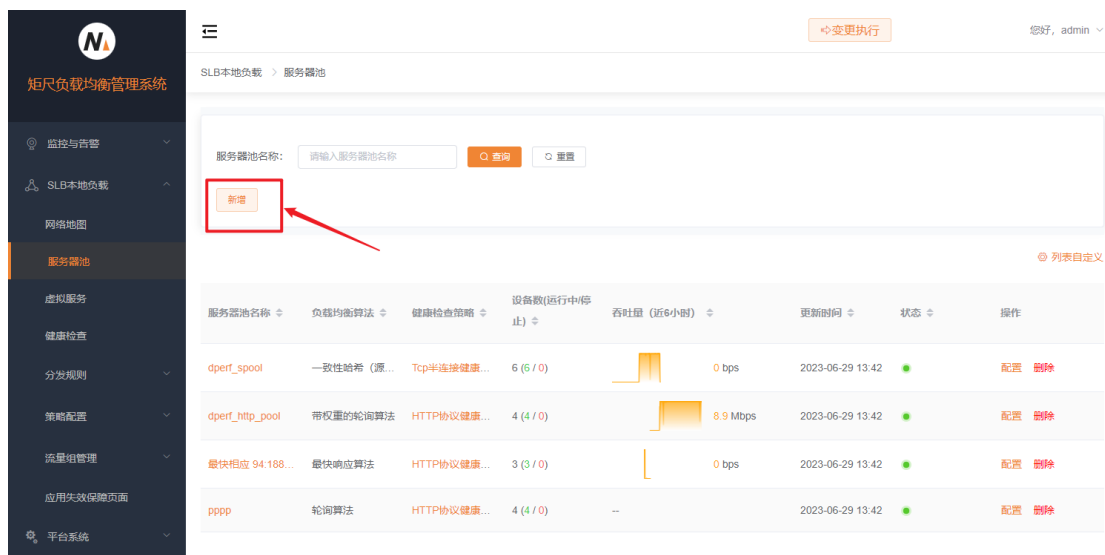
服务器池名称	负载均衡算法	健康检查策略	设备数(运行/停止)	吞吐量 (近6小时)	更新时间	状态	操作
dperf_spool	一致性哈希 (源...	Tcp半连接健康...	6 (6 / 0)	0 bps	2023-06-29 13:42	●	配置 删除
dperf_http_pool	带权重的轮询算法	HTTP协议健康...	4 (4 / 0)	8.9 Mbps	2023-06-29 13:42	●	配置 删除
最快响应 94.188...	最快响应算法	HTTP协议健康...	3 (3 / 0)	0 bps	2023-06-29 13:42	●	配置 删除
pppp	轮询算法	HTTP协议健康...	4 (4 / 0)	--	2023-06-29 13:42	●	配置 删除

● 查询区域：

可通过“服务器池名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域：

新增服务器池： 点击列表上方【新增】按钮，弹框打开服务器池新增页面，可添加/配置新的服务器池信息。



注：服务器池可以跨 SLB 集群使用。

服务器池可以设置开启状态，且每个服务器节点也可以设置开启状态。

➤ 优先级分组

通过启用优先级分组, 允许用户对服务器池中的节点设置优先级。这样, 当相同优先级的高优先级分组中节点可用时, 就不会使用低优先级节点。

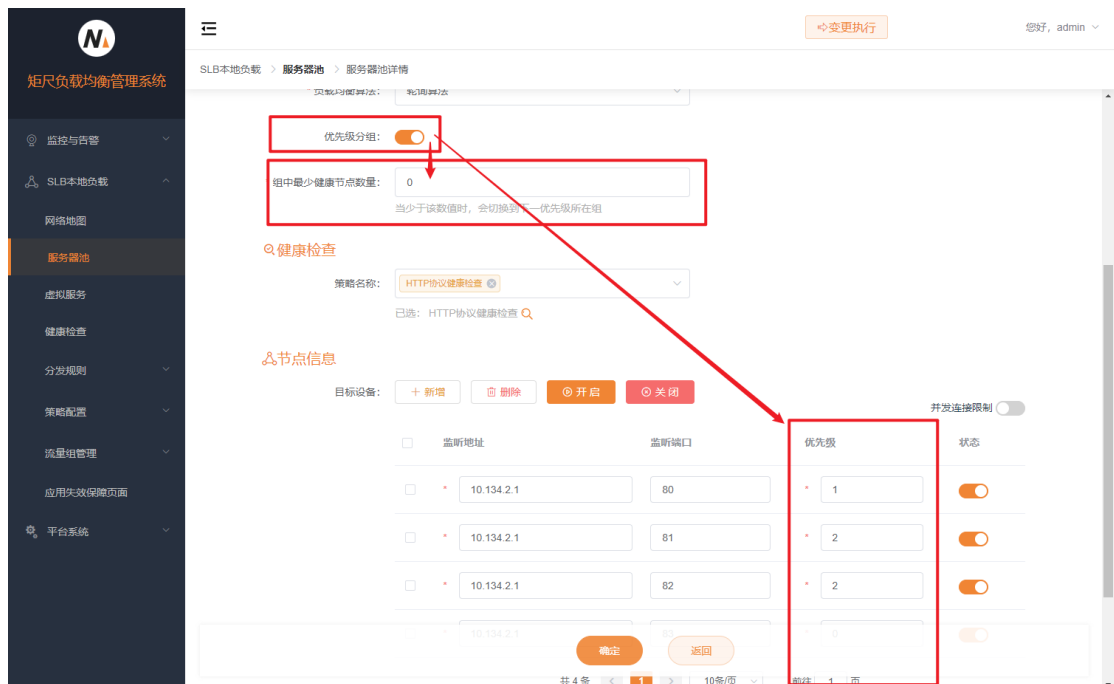
1. 节点的优先级是从 0 到 65535 的数字。数字越大, 优先级越高。默认每个节点优先级是 0。

2. 用户可以不设置优先级, 默认不启用该功能; 一旦启用后, 必须设置组中最少健康节点数量 n, 默认值是 0。它表示:

(1) 对于相同优先级的节点, 自动成为一组。

(2) 当最高优先级的健康节点数大于等于 n 时, 只使用这些健康节点; 次高优先级的节点都不使用。

(3) 一旦最高优先级的健康节点数小于 n, 那么将只使用次高优先级的节点服务



➤ 温暖上线

恢复时间：配置恢复时间后，当启用该真实服务时，设备会等待“恢复时间”后再给该真实服务分配流量。取值范围 0-600 秒，默认为 0 秒，即默认此功能关闭。

温暖时间：配置温暖时间后，设备为该真实服务分配的流量会根据温暖时间的长短缓慢增长，温暖时间越长，速率增长越平缓。取值范围 0-600 秒，默认为 10 秒，即默认此功能开启。

矩尺负载均衡管理系统

SLB本地负载 > 服务器池 > 修改服务器池

基础信息

* 服务器池名称: test123

描述: 请输入服务器池描述

温暖上线: ☒

* 恢复时间: 0 秒
取值范围0-600秒, 0表示此功能关闭

* 温暖时间: 10 秒
取值范围0-600秒, 0表示此功能关闭

* 负载均衡算法: 轮询算法

优先级分组: ☒

* 组中最少健康节点数量: 1
当少于该数值时, 会切换到下一优先级所在组

确定 取消

监听地址 监听端口 权重 状态

➤ 负载均衡算法

可选轮询算法、带权重的轮询算法、一致性哈希（源地址）算法、最小连接数算法、最快响应算法。

当选择带权重的轮询算法或最小连接数算法时，下方节点池会开启权重配置（0-100）；当选择一致性哈希（源地址）算法时，可配置哈希类型和哈希键，将基于哈希键进行负载均衡算法，可选哈希类型：URI、COOKIE、URL 参数、HEADER、源地址。

* 负载均衡算法: 一致性哈希（源地址）算法

* 哈希类型: URI

* 哈希键: 请输入哈希键

修改服务器池：在服务器池列表中点击右侧【配置】按钮，可进入这个服务器池修改页面：

矩尺负载均衡管理系统

- 监控与告警
- SLB本地负载均衡
- 网络地图
- 服务器池
- 虚拟服务
- 健康检查
- 分发规则
- 策略配置
- 流量组管理
- 应用失效保障页面
- 平台系统

SLB本地负载均衡

服务器池

服务器池名称:

查询

重置

新增

列表自定义

服务器池名称	负载均衡算法	健康检查策略	设备数(运行中/停止)	吞吐量 (近6小时)	更新时间	状态	操作
dperf_spool	一致性哈希 (源...	Tcp半连接健康...	6 (6 / 0)	0 bps	2023-06-29 13:45	●	配置 删除
dperf_http_pool	带权重的轮询算法	HTTP协议健康...	4 (4 / 0)	9.0 Mbps	2023-06-29 13:45	●	配置 删除
最快响应 94.188...	最快响应算法	HTTP协议健康...	3 (3 / 0)	0 bps	2023-06-29 13:45	●	配置 删除
pppp	轮询算法	HTTP协议健康...	4 (4 / 0)	--	2023-06-29 13:45	●	配置 删除

服务器池详情： 点击服务器池列表的服务器池名称可进入这个服务器池详情页面，每个服务器池详情页面分 4 个模块：配置信息、服务器节点、分析、事件。

矩尺负载均衡管理系统

- 监控与告警
- SLB本地负载均衡
- 网络地图
- 服务器池
- 虚拟服务
- 健康检查
- 分发规则
- 策略配置
- 流量组管理
- 应用失效保障页面
- 平台系统

SLB本地负载均衡

服务器池

服务器池名称:

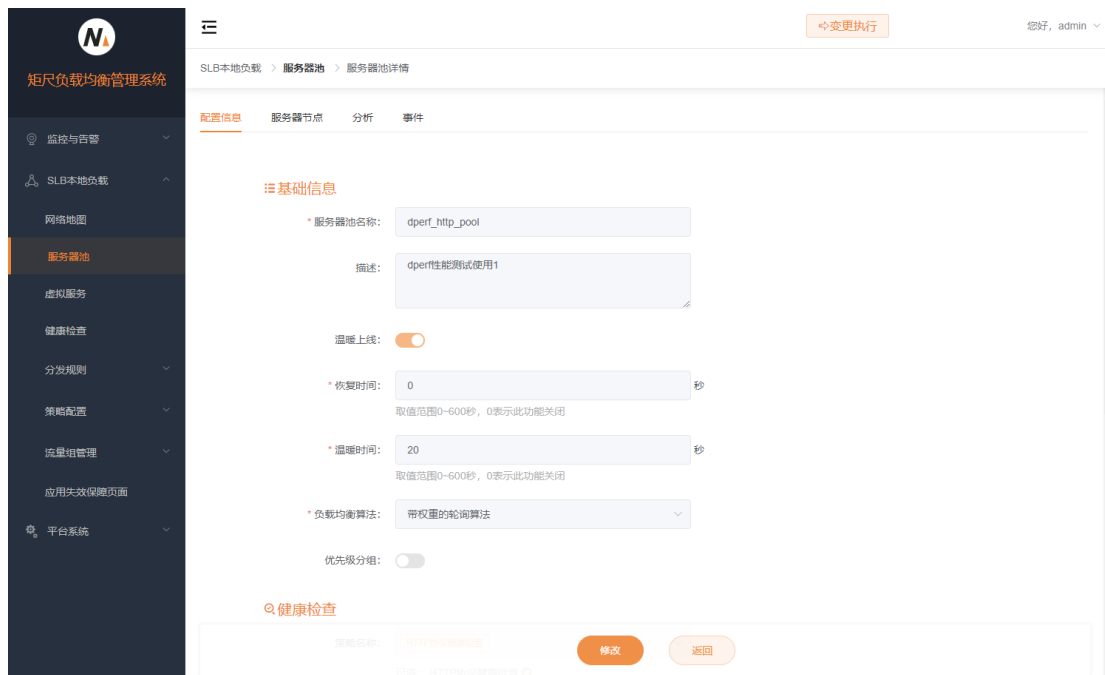
查询

重置

新增

列表自定义

服务器池名称	负载均衡算法	健康检查策略	设备数(运行中/停止)	吞吐量 (近6小时)	更新时间	状态	操作
dperf_spool	一致性哈希 (源...	Tcp半连接健康...	6 (6 / 0)	0 bps	2023-06-29 13:46	●	配置 删除
dperf_http_pool	带权重的轮询算法	HTTP协议健康...	4 (4 / 0)	9.0 Mbps	2023-06-29 13:46	●	配置 删除
最快响应 94.188...	最快响应算法	HTTP协议健康...	3 (3 / 0)	0 bps	2023-06-29 13:46	●	配置 删除
pppp	轮询算法	HTTP协议健康...	4 (4 / 0)	--	2023-06-29 13:46	●	配置 删除



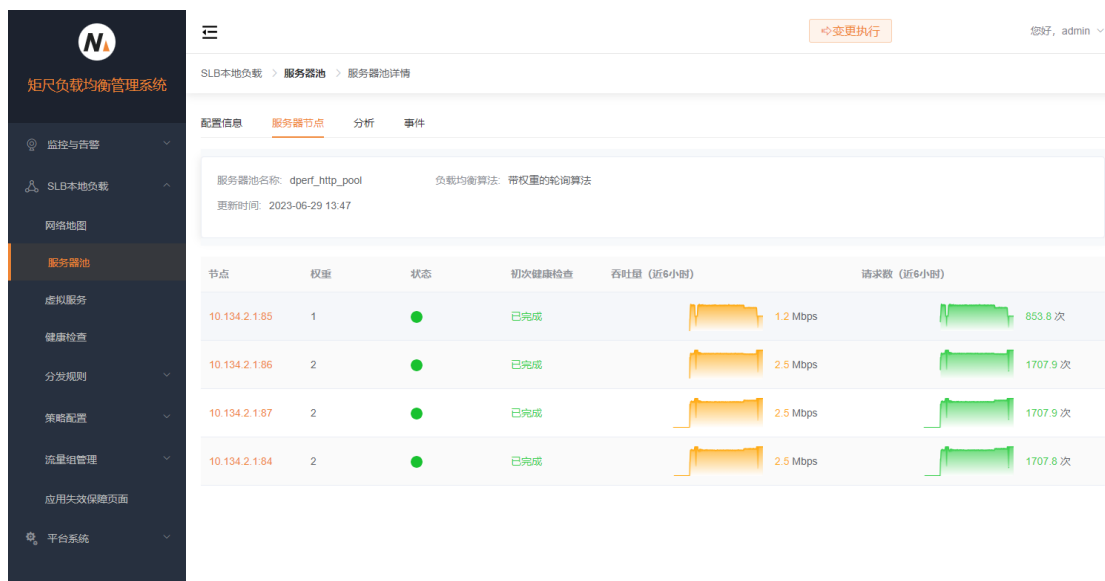
➤ 配置信息

查看该服务器池的具体配置：

➤ 服务器节点

可查看服务器池下所有节点信息，包括节点名称、监听地址、监听端口、节点状态、是否完成初次健康检查、近 6 小时吞吐量、近 6 小时请求数。表中折线图数字部分表示当前数据，当鼠标移入折线图时数字变为鼠标所在的纵坐标值。

查看服务器池节点详情：在节点列表中，点击节点名称或折线图可进入该节点分析页面。



➤ 分析



交互功能参见“4.5 监控与告警”章节。

A 区各字段含义如下：

- ◆ 服务器时延：负载均衡与服务器之间的 TCP RTT 时延；
- ◆ 应用响应：从负载均衡开始转发请求，到服务器返回第一个报文的间隔时间；
- ◆ 总时间：处理一个请求的总耗费时间；

C 区展示引用该服务器池的虚拟服务列表：

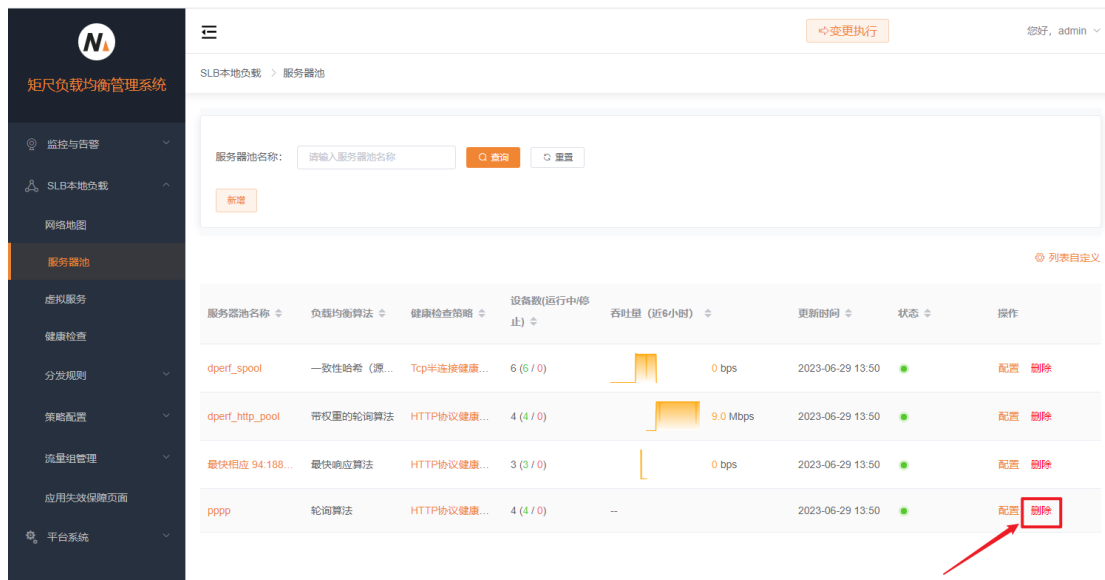
D 区展示该服务器池对应时间段内“端到端时延”、“新建连接”、“吞吐量”、“HTTP 请求”。

➤ 事件

服务器池事件，详见“4.5 监控与告警”章节的“事件”介绍。

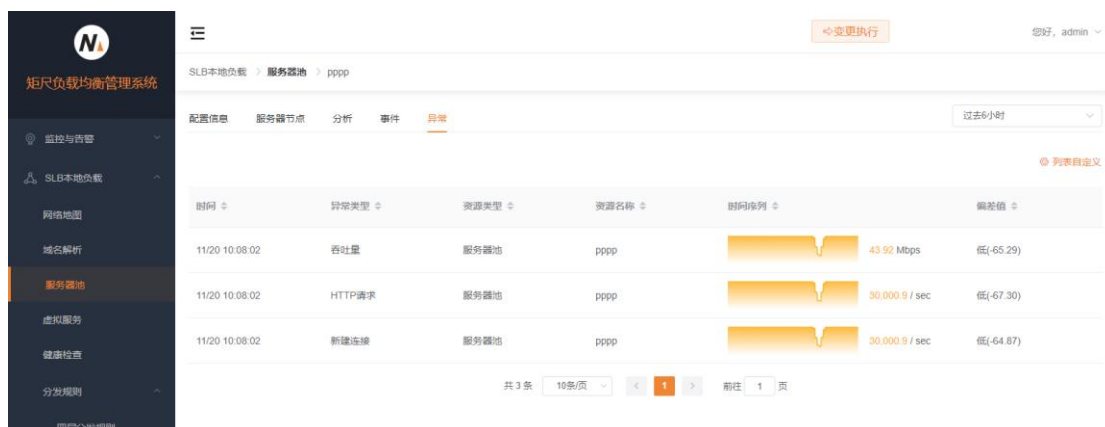


删除服务器池：服务器池列表中，在要删除的服务器池条目右边点击【删除】按钮，可对这条服务器池进行删除操作。



➤ 异常

服务器池异常，详见“4.5 监控与告警”章节的“异常”介绍。



4.6.3.1 服务器池节点

服务器池节点详情页面分为 2 个模块：分析、事件。

➤ 分析



交互功能参见“4.5

监控与告警”章节。

A 区展示节点健康状态监测，绿色向上箭头表示健康，当变为红色向下箭头时状态异常，当右侧详情按钮可点击时可查看具体信息；

健康监测	状态	详情
71健康检查3秒端口80	↑	🔍

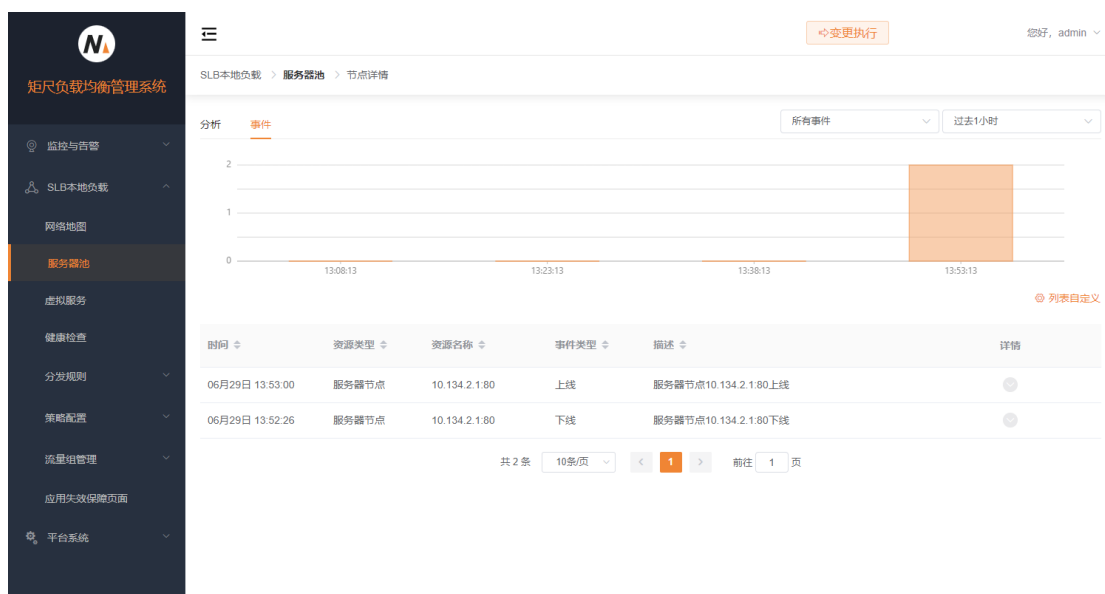
C 区展示该节点所在的服务器池信息，下拉框可选择切换到不同节点。



D 区展示该节点对应时间段内“端到端时延”、“吞吐量”、“新建连接”、“每秒请求数”。

➤ 事件

服务器池节点事件，详见“4.5 监控与告警”章节的“事件”介绍。



➤ 异常

服务器池节点异常列表，详见“4.5 监控与告警”章节的“异常”介绍。

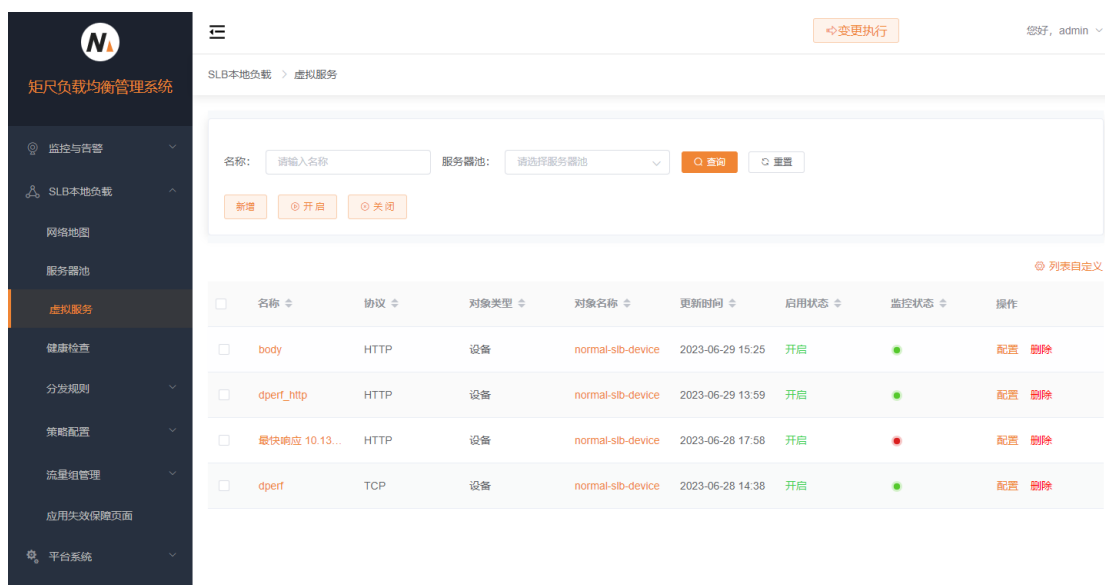


4.6.4 虚拟服务

虚拟服务功能实现，为每个虚拟服务器配置一个公共 IP 地址、多个端口，为所有入站客户端请求提供服务，同时可对客户端的 IP 段进行黑白名单设置、最大并发连接数限制。

虚拟服务既可以配置到包含多台设备的“流量组”中（适用于多台设备已经构建了 SLB 集群、流量组的场景），它将在流量组下的所有设备中生效；也可以配置到一台“设备”上，此时该虚拟服务将仅在指定设备上生效。

点击“SLB 本地负载→虚拟服务”菜单，默认展示按照用户创建时间倒序排列的虚拟服务列表。



● 查询区域：

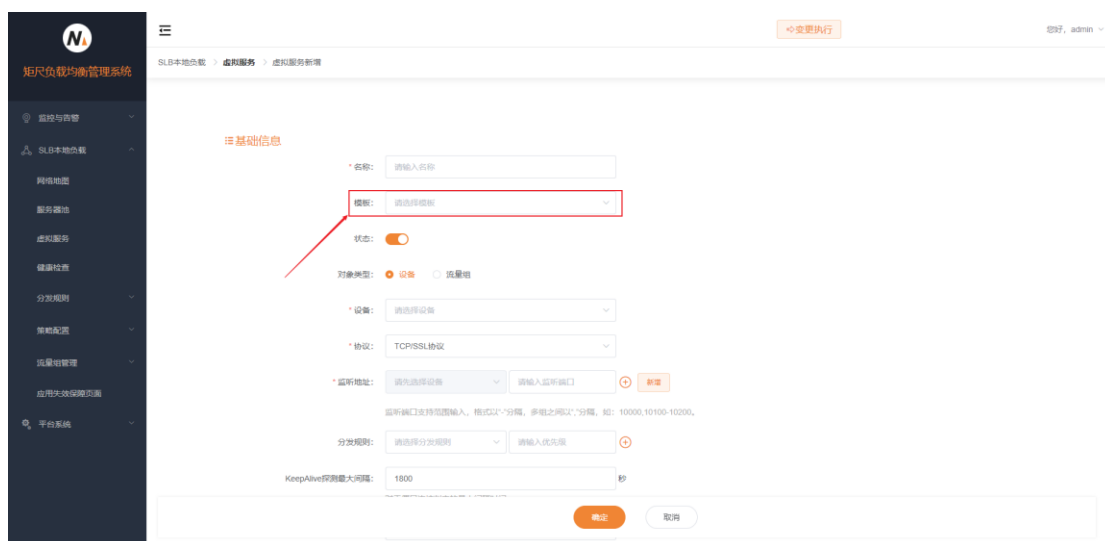
可通过“名称”、“服务器池”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域：

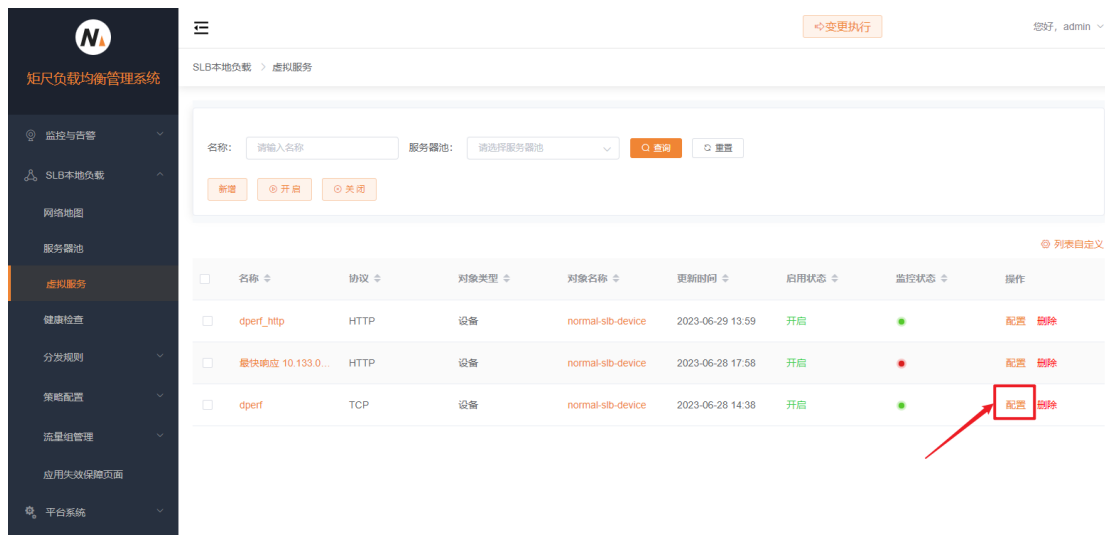
列表中，点击服务器池名称，跳转至服务器池的详情页。

新增虚拟服务：点击列表上方【新增】按钮，弹框打开虚拟服务新增页面，可添加/配置新的虚拟服务信息。

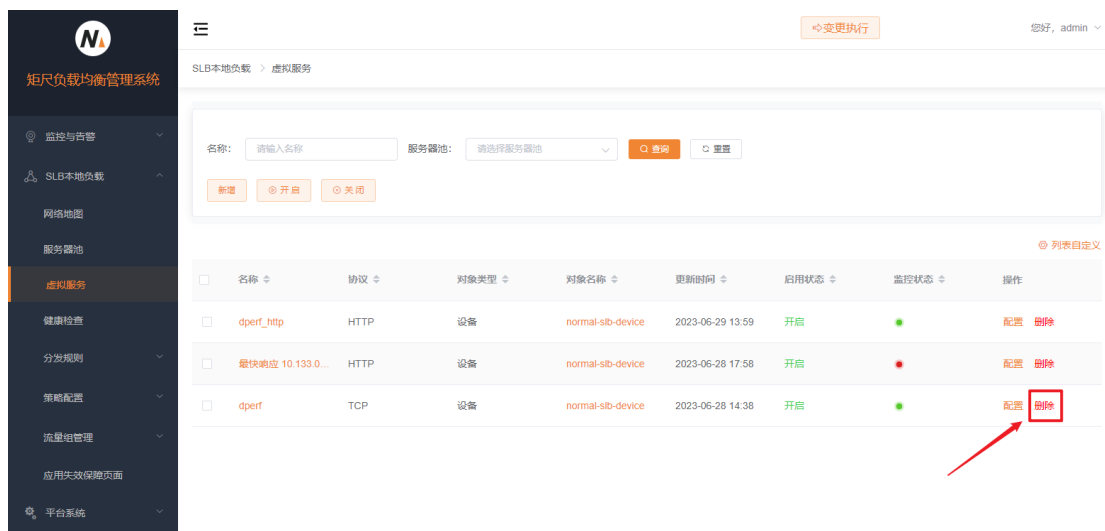
可选择模板快速填写虚拟服务信息：



修改虚拟服务：选择需要修改的虚拟服务信息，点击此用户所在行操作栏的【配置】按钮，进入虚拟服务修改页面。



删除虚拟服务：选择需要删除的虚拟服务信息，然后点击操作栏的【删除】按钮，可对路由虚拟服务进行删除操作。



虚拟服务详情：每个虚拟服务详情页面分 3 个模块：配置信息、分析、事件。

➤ 配置信息

可查看该虚拟服务下面所有配置：

虚拟服务配置

名称: test-002

状态: ☒ 开启

对象类型: ☒ 设备 ☐ 流量组

* 设备: normal-slb-device001-

* 协议: TCP协议

* 监听地址: 10.1.117.7 10100

监听端口支持范围输入，格式以“-”分隔，多组之间以“、”分隔，如：10000,10100-10200。

分发规则: rule-002 1

当满足规则的相同条件，优先级最高的将首先被选择

KeepAlive探测最大间隔: 1800 秒

返回

➤ 分析

端端时延 (当前)

客户端 337.19 ms → LB 0.647 ms → 服务器 0.835 ms → 应用程序 0 ms → 数据传输 0 ms → 总时间 1.082 ms

端端时延 ms

29日13:34:58

客户端时延 312.567 ms 服务器时延 447.318 ms 应用响应 668.163 ms 数据传输 0 ms 总时间 1100.854 ms

服务池列表

dperfl_http_pool 4 服务池

dperfl_http

端到端时延 312.567 ms

吞吐量 3.2 Mbps

新建连接 255.0 / sec

每秒请求数 1,774.9 / sec

虚拟服务监控统计的是双向流量，交互功能参见“4.5 监控与告警”章节。

A 区各字段含义如下：

端端时延 (当前)

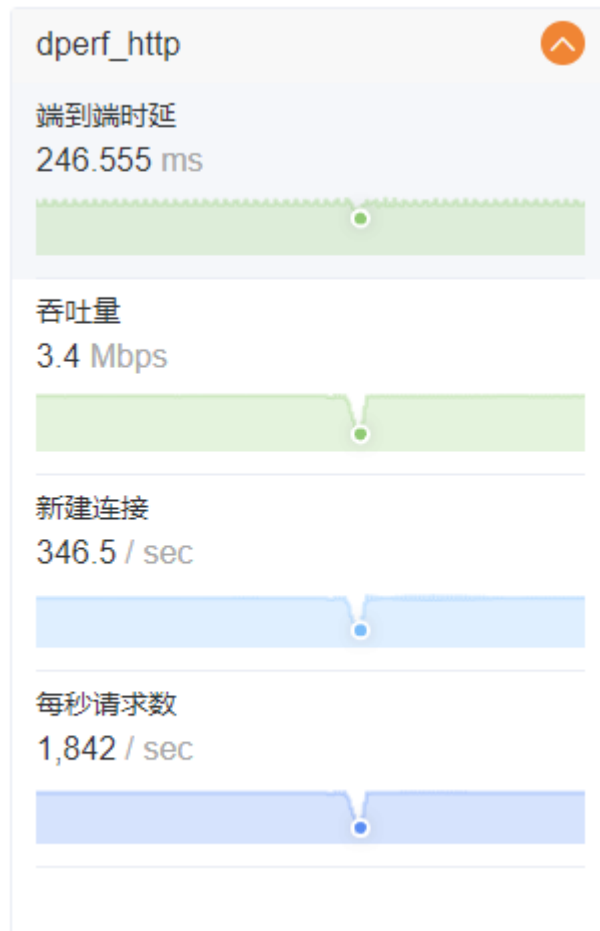
客户端 365.799 ms → LB 0.652 ms → 服务器 0.757 ms → 应用程序 0 ms → 数据传输 0 ms → 总时间 1.006 ms

- ◆ 客户端时延：四、七层有效，客户端与负载均衡之间的 TCP RTT 时延；
- ◆ 服务器时延：四、七层有效，负载均衡与服务器之间的 TCP RTT 时延；
- ◆ 应用响应：七层有效，从负载均衡开始转发请求，到服务器返回第一个报文的间隔时间；
- ◆ 数据传输：七层有效，服务器传输 HTTP 包体所用的时间；
- ◆ 总时间：四、七层有效，处理一个请求的总耗费时间；

C 区展示该虚拟服务下的服务器池列表信息，服务器池名称前的图标表示服务器池状态，右侧数字表示服务器池下的节点数量；



D 区展示该虚拟服务对应时间段内“端到端时延”、“吞吐量”、“新建连接”、“每秒请求数”。



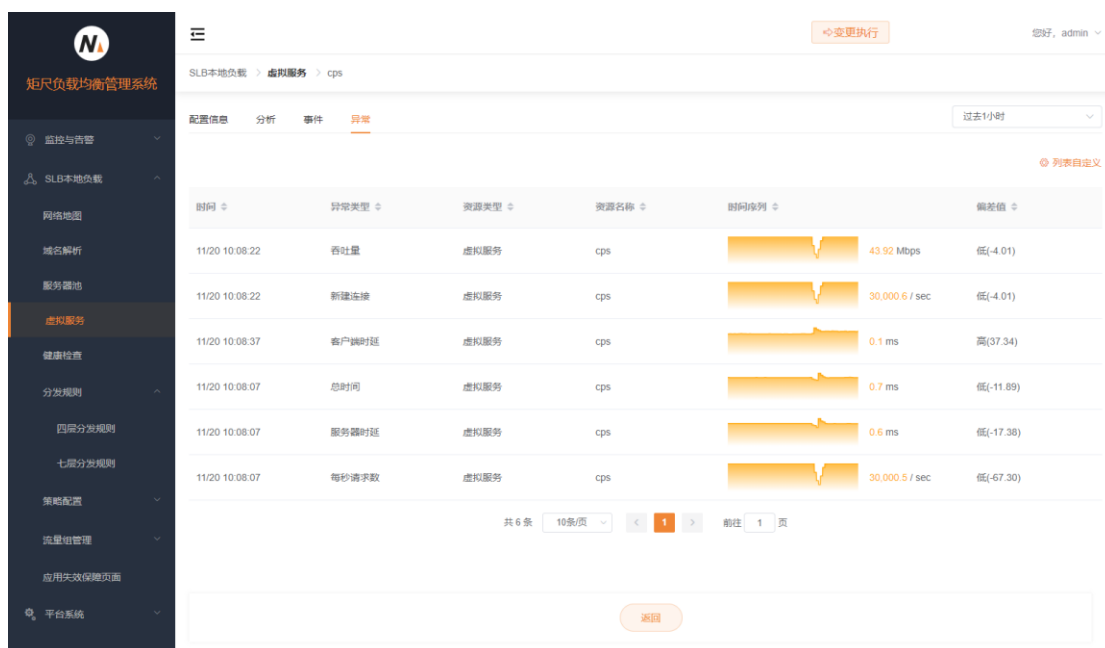
➤ 事件

虚拟服务事件，详见“4.5 监控与告警”章节的“事件”介绍。



➤ 异常

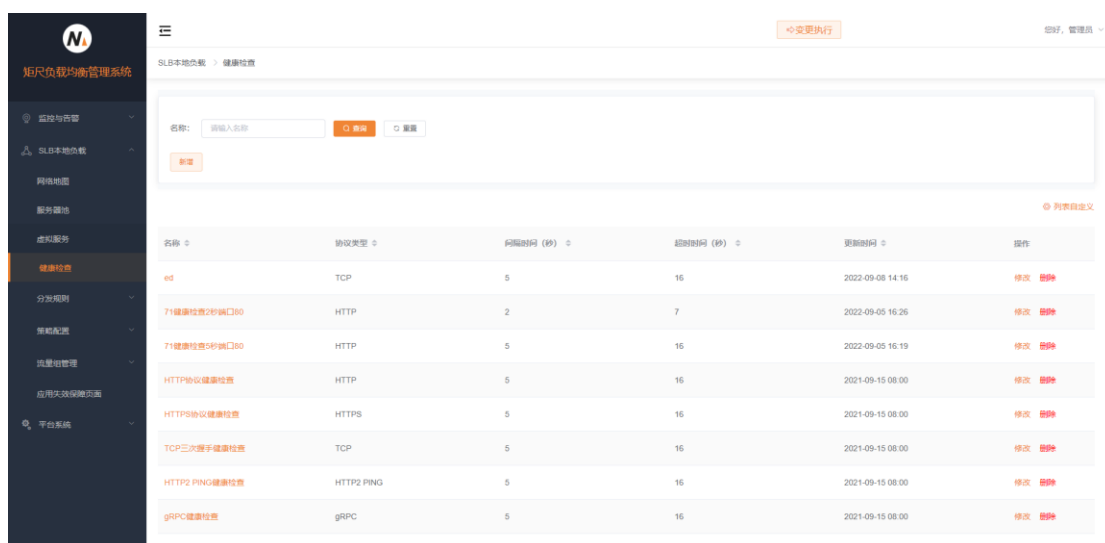
虚拟服务异常，详见“4.5 监控与告警”章节的“异常”介绍。



4.6.5 健康检查

健康检查实现针对多种协议（ICMP、TCP、HTTP、HTTPS、DNS、gRPC 等）配置不同的健康检查策略，服务器池配置时应用对应的健康检查策略，节点出现异常时即产生告警信息并通知相关人员及时处理。

点击“SLB 本地负载→健康检查”菜单，默认按照策略更新时间倒序排列展示所有健康检查策略信息列表



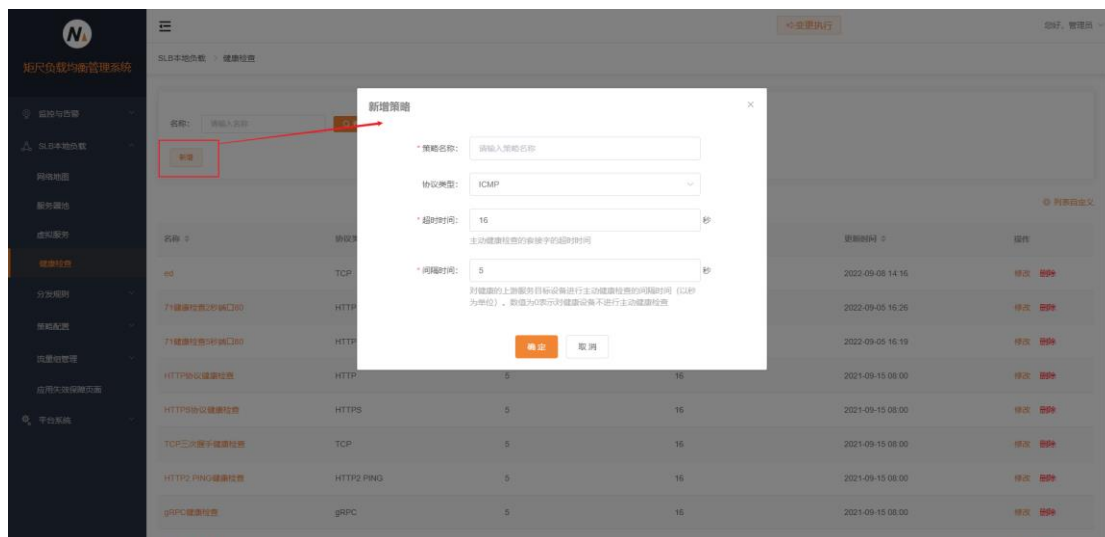
名称	协议类型	间隔时间 (秒)	超时时间 (秒)	更新时间	操作
elb	TCP	5	16	2022-09-08 14:16	修改 删除
71健康检查2秒端口80	HTTP	2	7	2022-09-05 16:26	修改 删除
71健康检查5秒端口80	HTTP	5	16	2022-09-05 16:19	修改 删除
HTTP80健康检查	HTTP	5	16	2021-09-15 08:00	修改 删除
HTTPS健康检查	HTTPS	5	16	2021-09-15 08:00	修改 删除
TCP三次握手健康检查	TCP	5	16	2021-09-15 08:00	修改 删除
HTTP2 PING健康检查	HTTP2 PING	5	16	2021-09-15 08:00	修改 删除
gRPC健康检查	gRPC	5	16	2021-09-15 08:00	修改 删除

● 查询区域：

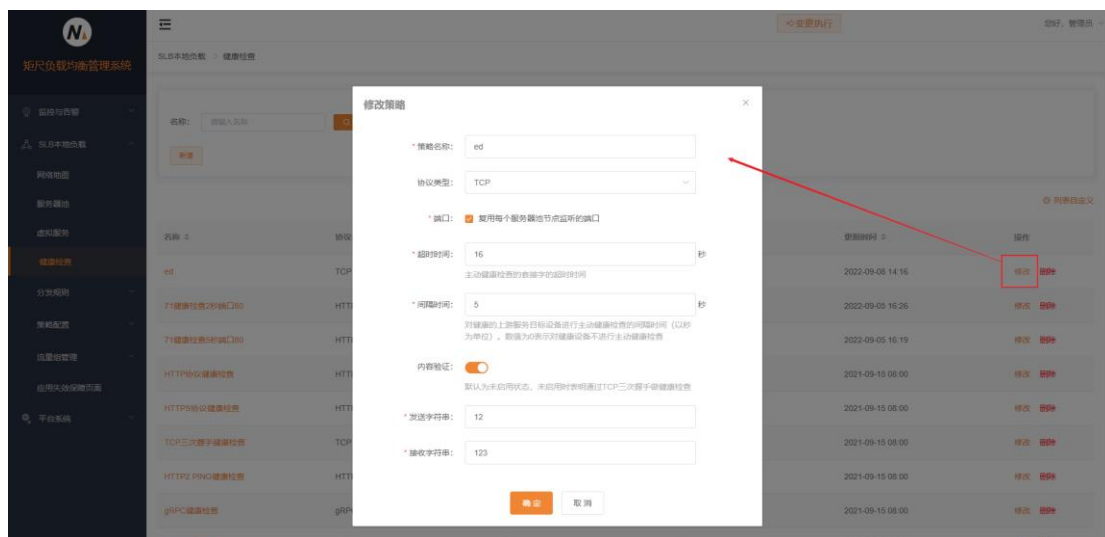
可通过“策略名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域：

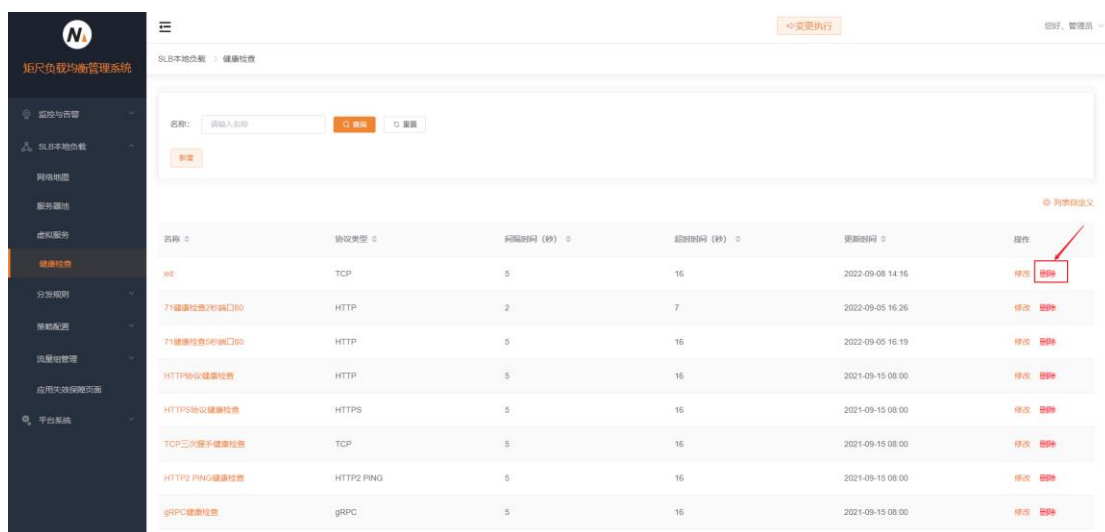
点击列表上方【新增】按钮，弹框打开健康检查策略新增页面，可添加/配置新的健康检查策略信息。



选择需要修改的健康检查策略信息，点击此用户所在行操作栏的【修改】按钮，弹框打开健康检查策略信息修改页面。



选择需要删除的健康检查策略信息，然后操作栏的【删除】按钮，可对健康检查策略信息进行删除操作。

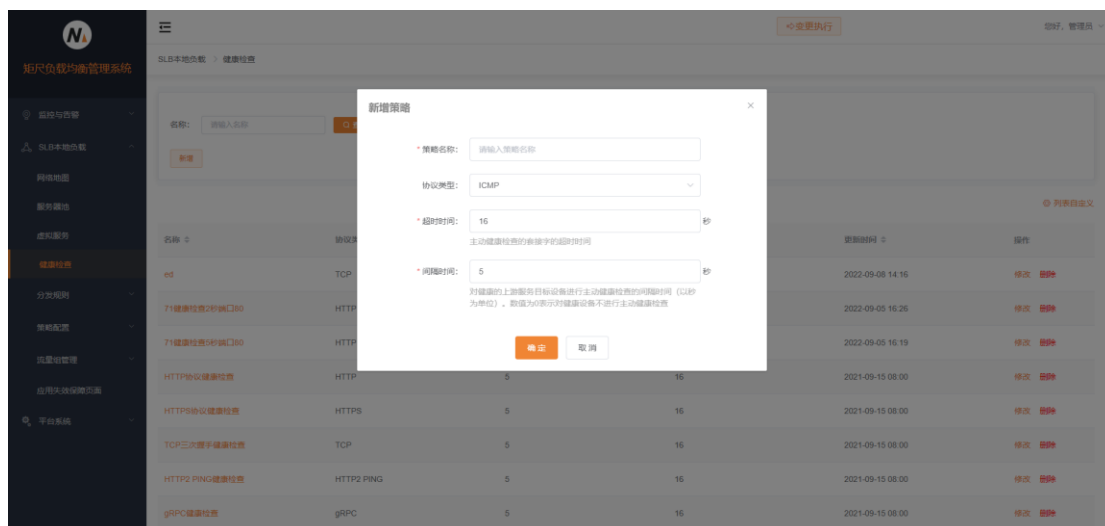


注：如果用户需要删除的健康检查策略已被服务器池、SLB 集群进行关联，则无法删除成功。

健康检查策略中的字段意义如下：

4.6.5.1 ICMP 协议健康检查策略

对服务器节点 IP（支持 IPv4、IPv6）进行 ICMP 协议健康检查（与 Ping 命令效果相同），在超时时间内响应则认为节点健康。

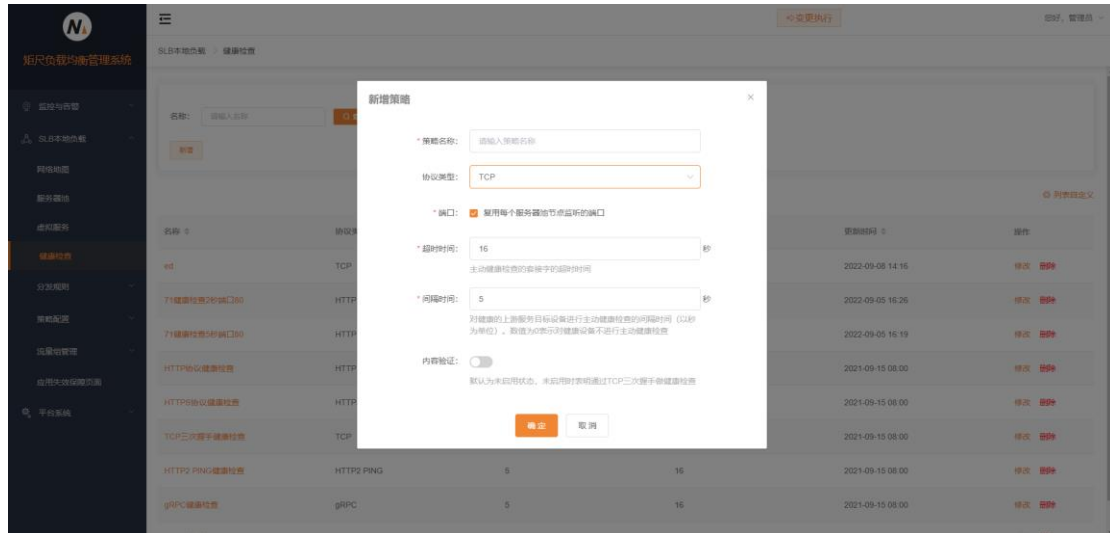


一般只需设置策略名称，其余字段可使用默认值，配置字段如下：

- 策略名称：健康检查策略的名称
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位），数值为 0 表示对健康设备不进行主动健康检查

4.6.5.2 TCP 协议健康检查策略

当服务器 IP 地址不支持 ICMP 协议或 ICMP 协议不满足健康检查需求时，且服务使用的是 TCP 协议，可使用 TCP 三次握手进行健康检查。

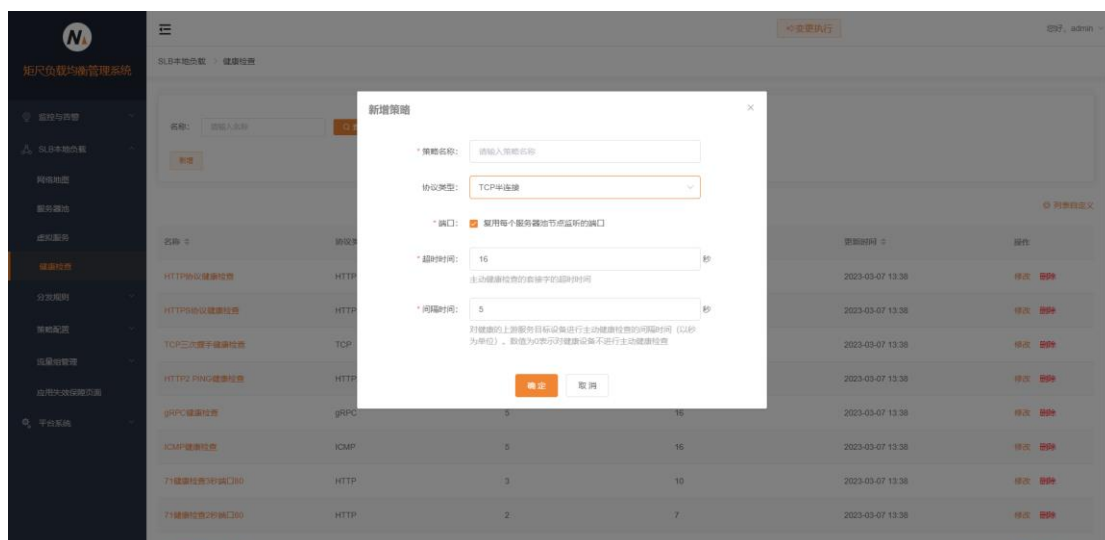


当不启用内容验证时，会根据是否接收到服务器的 SYN-ACK 包判断节点健康状态；当启用内容验证后，会根据发送和接收的字符串是否正确来判断节点健康状态。各字段含义如下：

- 策略名称：健康检查策略的名称；
- 端口
 - 复用监听端口：服务器节点端口使用服务器池中的监听端口。
 - 不复用监听商品：指定该健康检查策略的服务器节点目标端口。
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- 内容验证：默认为未启用状态，未启用时表明通过 TCP 三次握手做健康检查
- 发送字符串：启用内容验证后，向服务器发送的字符串内容
- 接受字符串：启用内容验证后，接收到服务器回复的字符串内容

4.6.5.3 TCP 半连接健康检查

TCP 检查建立连接后会发送 FIN 包关闭连接，为了减少完整的 TCP 健康检查的资源占用，可使用 TCP 半连接对服务器健康检查，TCP 半连接在收到 SYN-ACK 包后就判断节点健康，之后发送 RST 包重置连接。

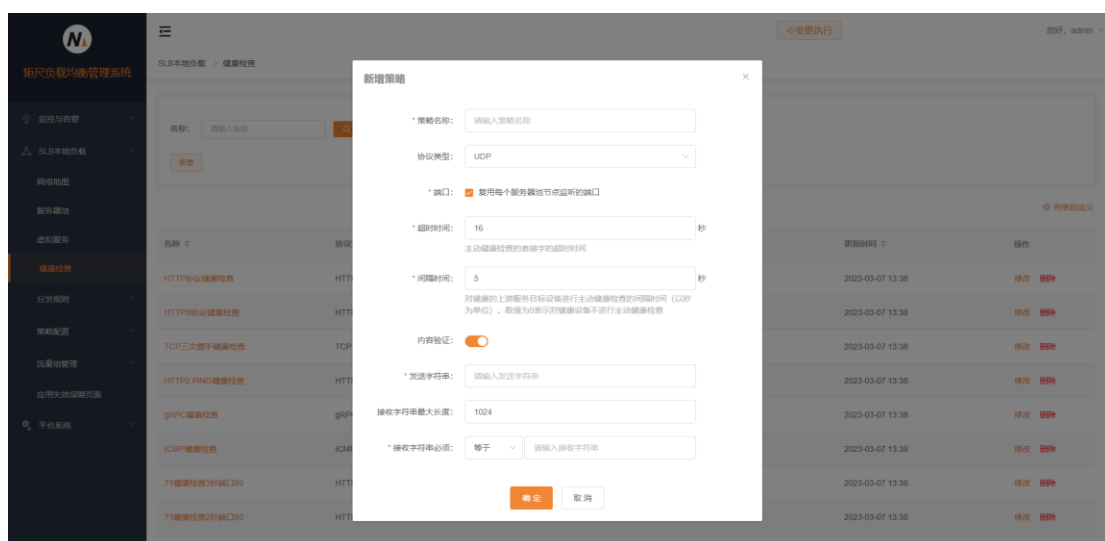


一般只需设置策略名称，其余字段可使用默认值，各字段含义如下：

- 策略名称：健康检查策略名称
- 端口
 - 复用监听端口：服务器节点端口使用服务器池中的监听端口。
 - 不复用监听商品：指定该健康检查策略的服务器节点目标端口。
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）

4.6.5.4 UDP 协议健康检查策略

当服务器禁用 ICMP 或 ICMP 协议不满足健康检查需求时，且服务使用的是 UDP 协议，可使用 UDP 对服务器发送探测报文，根据是否在超时时间内响应内容或报错信息来判断服务节点健康状态。

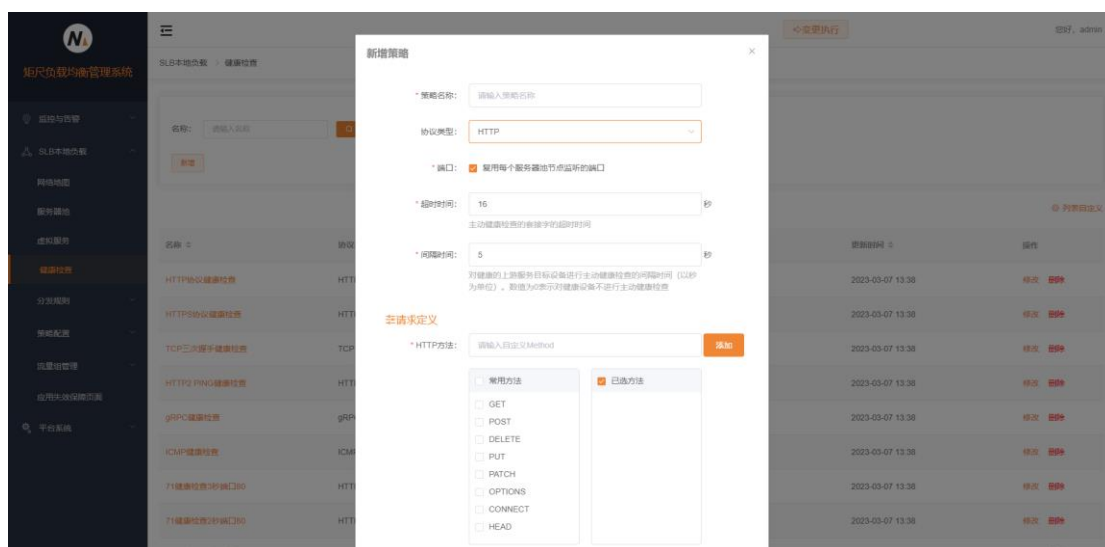


当不启用内容验证时，在超时时间内，如果未收到报错则判断节点为健康，如果收到 Connection refused 报错信息，则判断节点异常；当启用内容验证后，会根据接收的字符串是否正确匹配来判断节点健康状态。各字段含义如下：

- 策略名称：健康检查策略名称
- 端口
 - 复用监听端口：服务器节点端口使用服务器池中的监听端口。
 - 不复用监听商品：指定该健康检查策略的服务器节点目标端口。
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- 内容验证：是否发送验证字符串
- 发送字符串：发送内容（字符串）
- 接收字符串最大长度：接收响应的最大长度（单位：社区字节），超出后即认为失败
- 接收字符串必须：接收内容判断，选项包括：等于、包含，后跟字符串

4.6.5.5 HTTP 协议健康检查策略

如果有时端口可达但服务返回错误，在这种情况下，当服务使用的是 HTTP 协议，可配置 HTTP 协议健康检查。



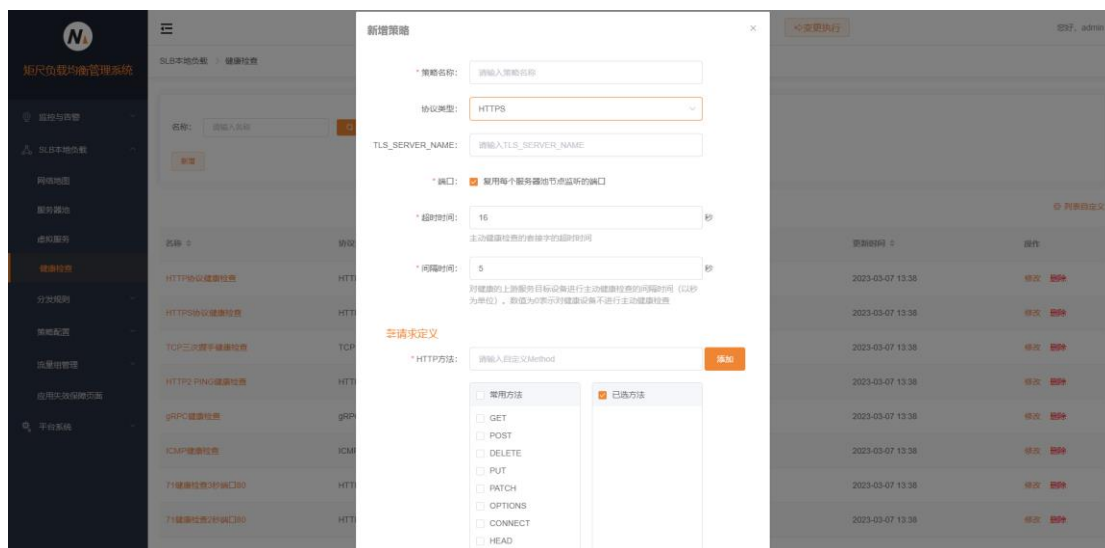
HTTP 健康检查协议中，可设定 HTTP 请求包，根据服务返回的响应是否匹配状态码、响应头部、响应包体来判断健康状态。各字段含义如下：

- 策略名称：健康检查策略名称
- 端口
 - 复用监听端口：服务器节点端口使用服务器池中的监听端口。

- 不复用监听商品：指定该健康检查策略的服务器节点目标端口。
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- HTTP 方法：进行健康检查的 HTTP 请求方法
- 请求路径：进行健康检查的 HTTP 请求 URL
- 请求头部（可选）：进行健康检查的 HTTP 请求 Header 头部
- 请求包体（可选）：进行健康检查的 HTTP 请求 Body 包体
- 响应码：基于服务器的响应码（可配置多个）判断节点是否健康
- 响应头部：基于 HTTP 响应中是否包含某个 HTTP 头部，判断节点是否健康
- 响应包体：对 HTTP 响应包体做字符串比较，以此判断节点是否健康

4.6.5.6 HTTPS 协议健康检查策略

如果有时端口可达但服务返回错误，在这种情况下，当服务使用的是 HTTPS 协议，可配置 HTTPS 协议健康检查。



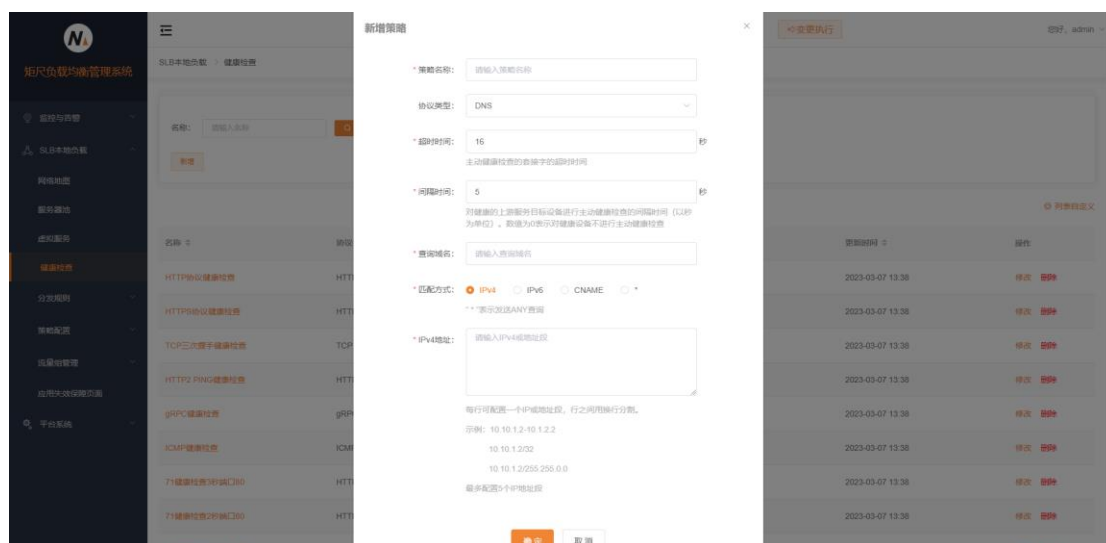
HTTPS 健康检查协议中，可设定 HTTPS 请求包，根据服务返回的响应是否匹配状态码、响应头部、响应包体来判断健康状态。与 HTTP 配置唯一不同的字段是 TLS_SERVER_NAME，各字段含义如下：

- 策略名称：健康检查策略名称
- HTTP 方法：进行健康检查的 HTTP 请求方法
- TLS_SERVER_NAME（可选）：指定 ClientHello 中的 SNI 域名
- 端口
 - 复用监听端口：服务器节点端口使用服务器池中的监听端口。

- 不复用监听商品：指定该健康检查策略的服务器节点目标端口。
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- 请求路径：进行健康检查的 HTTP 请求 URL
- 请求头部（可选）：进行健康检查的 HTTP 请求 Header 头部
- 请求包体（可选）：进行健康检查的 HTTP 请求 Body 包体
- 响应码：基于服务器的响应码（可配置多个）判断节点是否健康
- 响应头部：基于 HTTP 响应中是否包含某个 HTTP 头部，判断节点是否健康
- 响应包体：对 HTTP 响应包体做字符串比较，以此判断节点是否健康

4.6.5.7 DNS 协议健康检查

在对 DNS 服务器进行健康检查时，有时尽管服务端口可达，但它并不能准确地判断节点的健康状况。例如，DNS 端口可能是开放的，但是由于服务异常没有返回解析结果。此时可配置 DNS 协议健康检查。



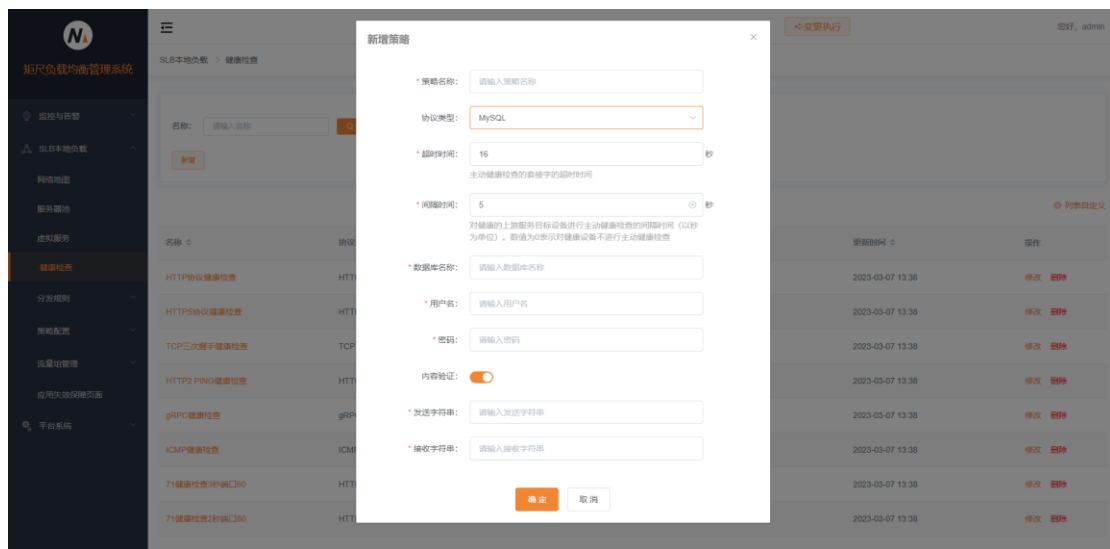
DNS 健康检查协议会向服务器节点发送 DNS 查询请求，当设置匹配方式 IPv4、IPv6、CNAME 时，如果返回结果匹配包含填写的所有内容，则认为节点健康，否则认为节点异常；当设置匹配方式为*时，返回任意查询类型结果都认为节点健康，如果超时没有返回则认为节点异常。各字段含义如下：

- 策略名称：健康检查策略名称
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- 查询域名：配置发送给节点的查询域名

- 匹配方式：可选匹配 IPv4、IPv6、CNAME 或*（*表示发送 ANY 查询）
- IPv4 地址：这意味着 DNS 请求是 A 请求
- IPv6 地址：这意味着 DNS 请求是 AAAA 请求
- CNAME：这意味着 DNS 请求是 CNAME 请求

4.6.5.8 MYSQL 健康检查

当端口检查无法准确判断服务器健康状态时，可能需要对数据库进行健康检查，如果使用的是 MYSQL 类型数据库，可选择 MYSQL 协议类型。



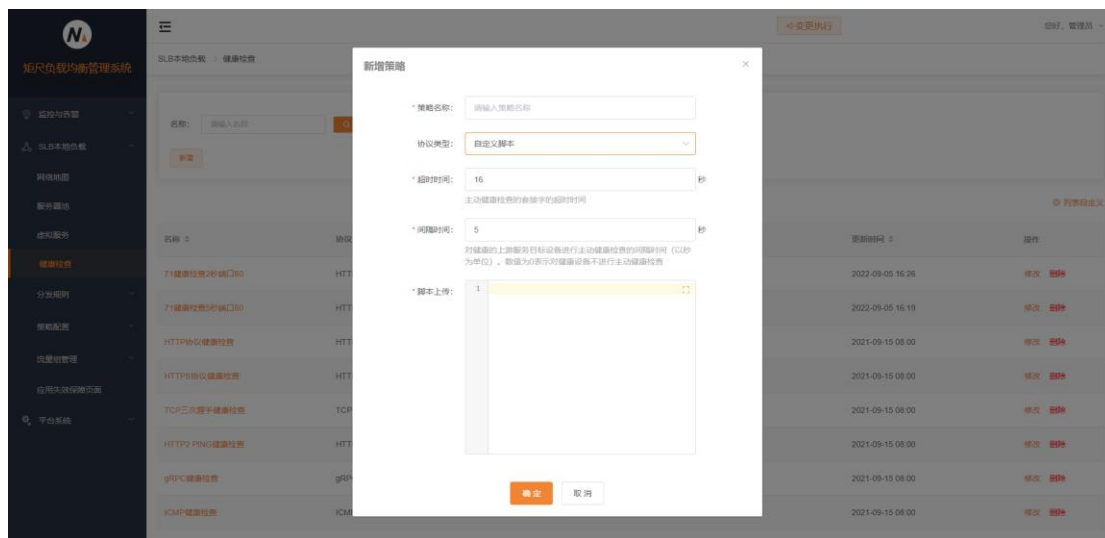
通过发送 MYSQL 请求数据包对服务器进行 MYSQL 协议健康检查，可配置数据库名和用户名密码，检测是否正常连接数据库，配置内容验证，检测是否正确响应请求。各字段含义如下：

- 策略名称：健康检查策略名称
- 超时时间：主动健康检查的套接字的超时时间
- 间隔时间：对健康的上游服务目标设备进行主动健康检查的间隔时间（以秒为单位）
- 数据库名称：需要检查的数据库名称
- 用户名：登录数据库的用户名
- 密码：登录数据库的密码
- 内容验证：是否需要内容验证
- 发送字符串：发送内容（字符串）
- 接收字符串：接收内容（字符串）

4.6.5.9 自定义脚本

当以上健康检查策略不满足业务需求时，还可以灵活定制脚本，通过用户自定义脚本检查每个节点的健康状态（目前仅支持 Python 脚本）。

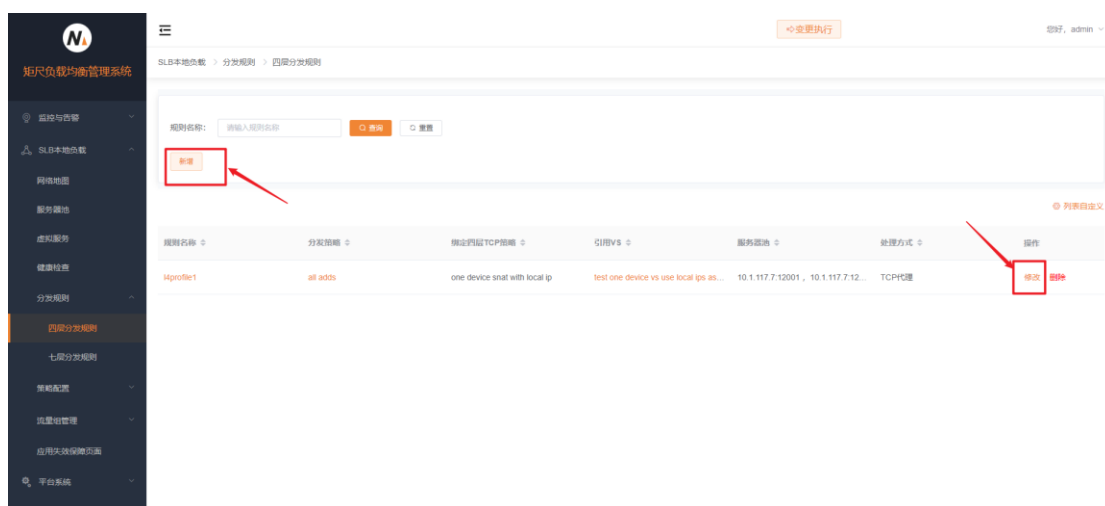
脚本执行时将会接收到 2 个参数，第 1 个参数是服务器节点的 IP，第 2 个参数是目标端口。脚本返回 0 则表示节点是健康的，返回非 0 则表示节点不健康。



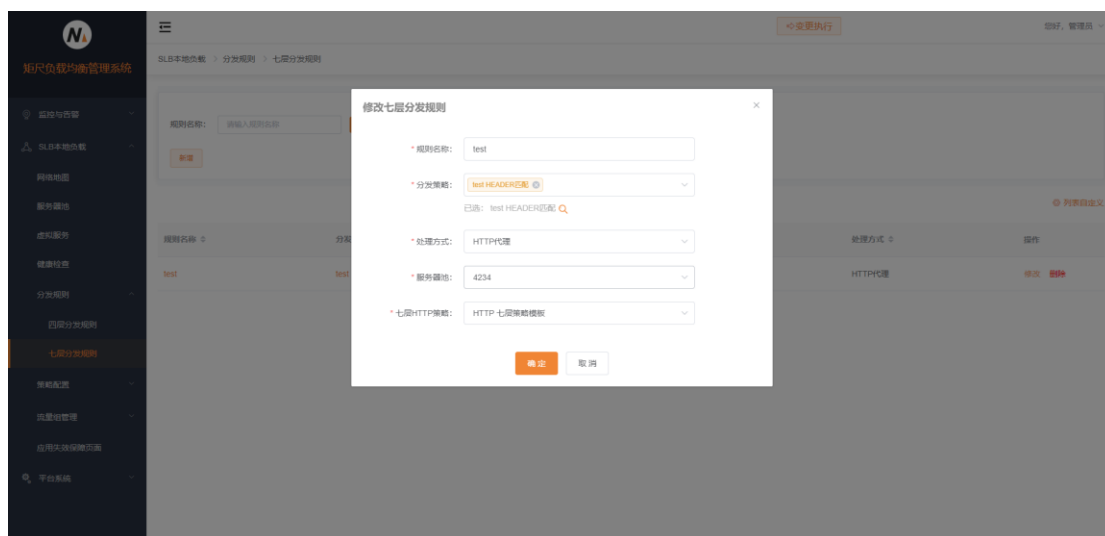
脚本配置详情见附件 [健康检查脚本配置帮助（V1.2.0）.docx](#)

4.6.6 分发规则

进入“SLB 本地负载→分发规则”，支持四层和七层分发规则配置。



点击【新增】按钮或【修改】按钮，打开分发规则编辑对话框：



可配置字段如下：

➤ 四层分发规则：

分发策略：可选多个分发策略。

处理方式：TCP 代理或者 UDP 代理。

服务器池：分发到服务器池。

四层 TCP 策略：选择四层 TCP 策略。

➤ 七层分发规则：

分发策略：可选多个分发策略。

处理方式：可选 HTTP 代理、重定向、指定其他错误码。

服务器池：分发到服务器池。

七层 HTTP 策略：选择七层 HTTP 策略。

4.6.7 策略配置

4.6.7.1 分发策略

进入“SLB 本地负载→策略配置→分发策略”，点击【新增】按钮或【修改】按钮，进入分发策略编辑页面。

支持八种类型匹配：源地址段、URL 匹配、HOST 域名、SNI 域名、HEADER 匹配、Method 匹配、Cookie 匹配、URL 参数匹配。

➤ 源地址段

源地址段为多行文本输入，每行可配置一个 IP 或地址段（支持 IPv6 地址），行之间用换行分割。

示例：10.10.1.2-10.1.2.2

10.10.1.2/32

10.10.1.2/255.255.0.0

最多配置 5 个 IP 地址段。

➤ URL 匹配、HOST 域名、SNI 域名

当选择 URL 匹配、HOST 域名或 SNI 域名类型时，可添加多行输入：

矩尺负载均衡管理系统

SLB本地负载均衡 > 策略配置 > 分发策略 > 分发策略新增

策略名称:

类型:

请输入URL

请输入URL

请输入URL

默认为URL完全匹配，如需前缀匹配请在末尾添加“*”，其中，“*”表示通配符。
例如，“/user/”分发策略能匹配请求/user/login，而/user分发策略则只能匹配/user请求。

确定 取消

➤ Method 匹配

Method 匹配可选默认 8 中方法，可输入自定义方法添加到已选方法中。

矩尺负载均衡管理系统

SLB本地负载均衡 > 策略配置 > 分发策略 > 分发策略新增

策略名称:

类型:

请输入自定义Method

☐ 常用方法

☐ GET

☐ POST

☐ DELETE

☐ PUT

☐ PATCH

☐ OPTIONS

☐ CONNECT

☐ HEAD

☒ 已选方法

确定 取消

➤ HEADER 匹配、Cookie 匹配、URL 参数匹配

当选择 HEADER 匹配、Cookie 匹配或 URL 参数匹配时，可添加多个键值对，每一个键值对可设置匹配类型：

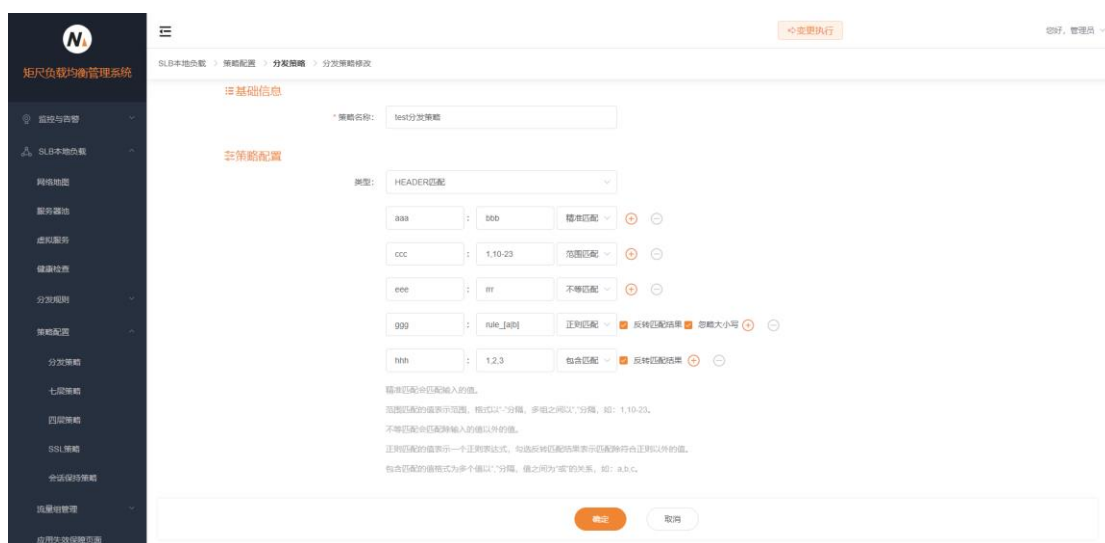
精准匹配：精准匹配会匹配输入的值。

范围匹配：范围匹配的值表示范围，格式以“-”分隔，多组之间以“,”分隔，如：1,10-23。

不等匹配：不等匹配会匹配除输入的值以外的值。

正则匹配：正则匹配的值表示一个正则表达式，勾选反转匹配结果表示匹配除符合正则以外的值。

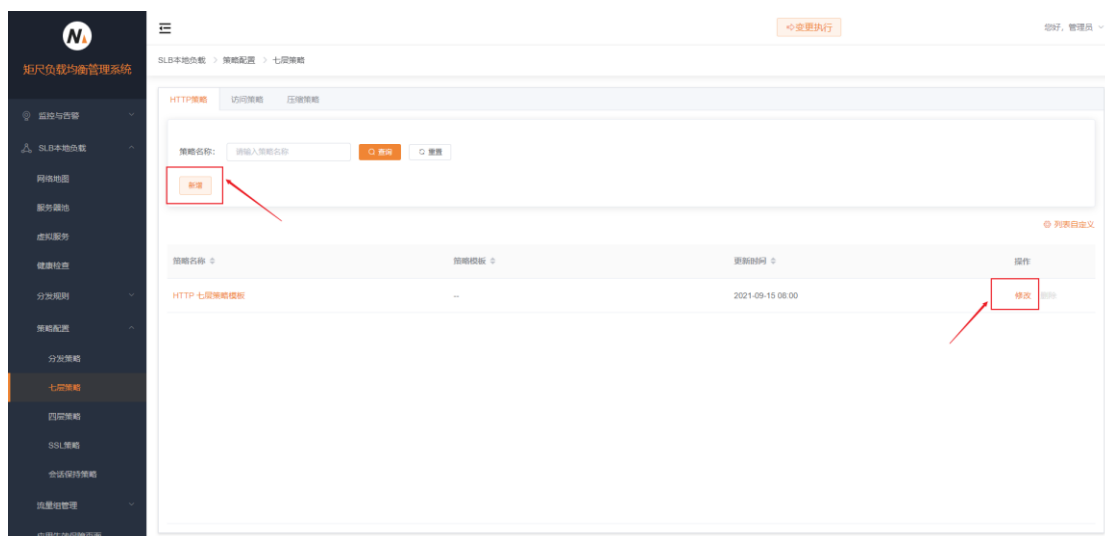
包含匹配：包含匹配的值格式为多个值以“,”分隔，值之间为“或”的关系，如：a,b,c。



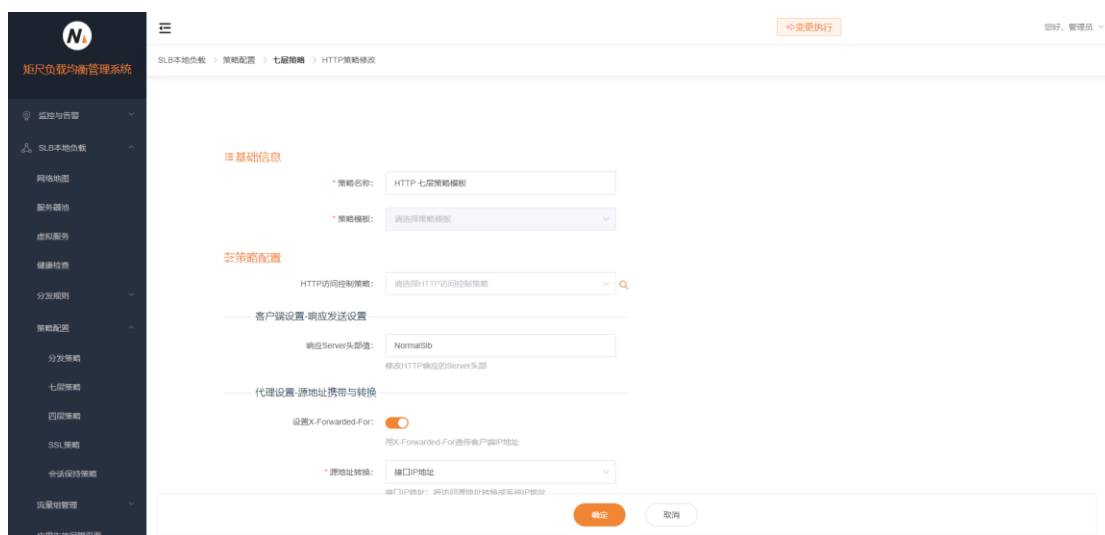
4.6.7.2 七层策略

➤ HTTP 策略

点击“SLB 本地负载→策略配置→七层策略”进入七层策略页面，选择头部页签 HTTP 策略可查看 HTTP 策略列表。



点击【新增】或【修改】按钮可进入 HTTP 策略编辑页面，



各字段含义如下：

- HTTP 访问控制策略：如果需要限制客户端请求的访问，则应选择此策略。
- 是否支持 WebSocket 协议：开启或关闭 WebSocket 协议。
- 响应 Server 头部值：修改 HTTP 响应的 Server 头部。
- 设置 X-Forwarded-For：用 X-Forwarded-For 透传客户端 IP 地址。
- 源地址转换：
 - 接口 IP 地址：将访问源地址转换成系统 IP 地址
 - 指定地址池：将访问源地址转换成指定地址池中的 IP 地址
 - 虚拟服务 IP 地址：将访问源地址转换成虚拟服务 IP 地址

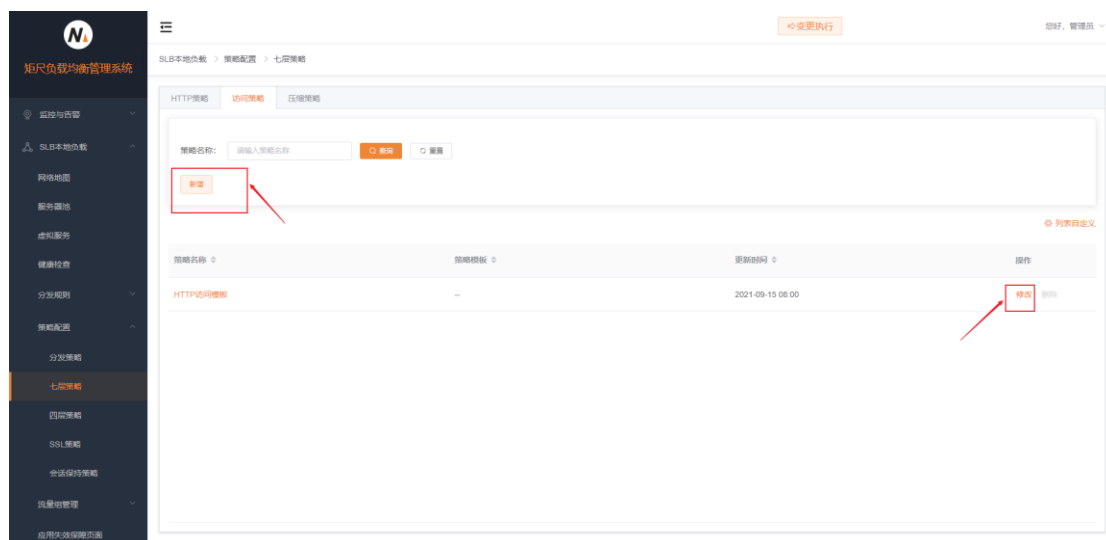
- 会话保持策略：选择会话保持策略。
- Host 头部传递策略：可选择不同的规则修改发往服务器的 HTTP 请求中的 Host 头部。
- 添加或修改请求头部：对于这里设置的 Header，如果名称在 HTTP 请求中不存在，则表示添加头部；如果 Header 名称已存在，则替换 Header 值。
- 删除请求头部：从 HTTP 请求中删除指定名称的 Header。
- HTTP 协议版本：与服务器通讯的 HTTP 版本。
- 修改转发 URL 前缀：为空时表示不修改 URL 前缀。

➤ HTTP 访问策略

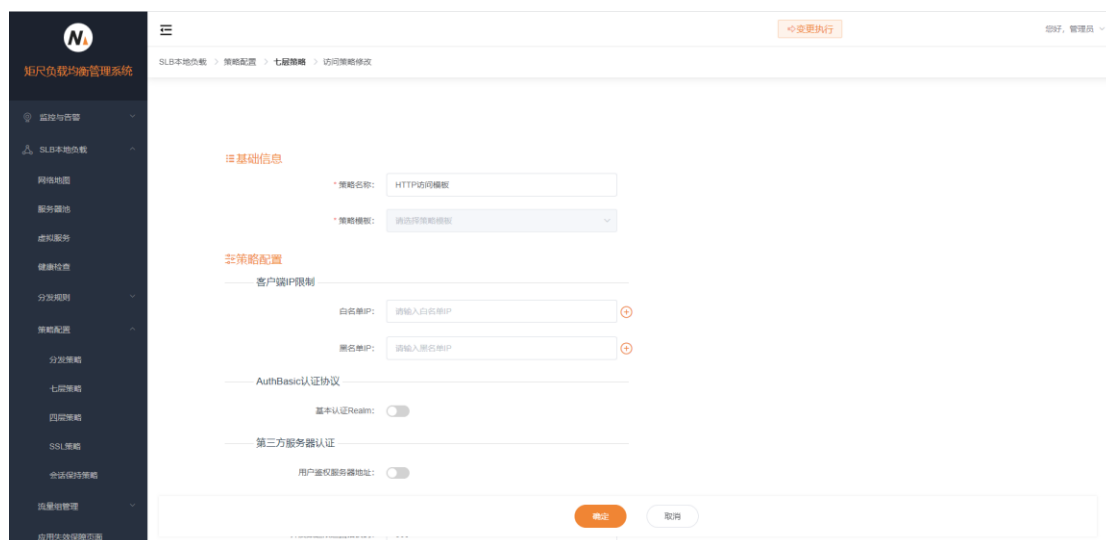
对于七层负载均衡，如果需要在转发至服务器池前，控制客户端请求的 RPS 访问速度、并发连接数、Auth Basic 访问密码、IP 黑白名单等配置，就可以使用 HTTP 访问控制策略。

HTTP 访问控制策略被 HTTP 策略使用。

点击“SLB 本地负载→策略配置→七层策略”进入七层策略页面，选择头部页签“访问策略”可查看访问策略列表。



点击【新增】或【修改】按钮可进入访问策略编辑页面，



矩尺负载均衡系统

SLB本地负载 > 策略配置 > 七层策略 > 访问策略修改

基础信息

- *策略名称: HTTP25同策略
- *策略模板: 请选择策略模板

策略配置

客户端IP限制

- 白名单IP: 请输入白名单IP
- 黑名单IP: 请输入黑名单IP

AuthBasic认证协议

- 基本认证Realm: ☐

第三方服务器认证

- 用户鉴权服务器地址: ☐

确定 取消

各字段含义如下所示：

- 白名单 IP：允许的客户端 IP
- 黑名单 IP：禁止的客户端 IP
- 基本认证 Realm：可以使用 Auth Basic 协议实现简单认证
- 用户鉴权服务器地址：由第三方服务完成请求鉴权后（返回 200 响应码），再代理到服务器池。
- 并发数超限返回错误码：当并发连接超过 limit_conn 时的 HTTP 返回错误码。
- 最大并发请求数：并发处理请求数最大值，可以点击“不限制”复选框，不限制并发处理请求数。
- 最大并发延迟请求数：达到最大并发请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发请求时 reject 新请求。
- 每秒最大处理请求数：每秒处理请求数最大值，可以点击“不限制”复选框，不限制每秒处理请求数。
- 每秒最大处理延迟请求数：达到每秒最大处理请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大处理请求时 reject 新请求。
- 窗口时间内最大并发请求：窗口时间内最大并发请求数最大值，可以点击“不限制”复选框，不限制窗口时间内最大并发请求数。
- 窗口时间内最大并发延迟请求数：达到窗口时间内最大并发请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发请求时 reject 新请求。

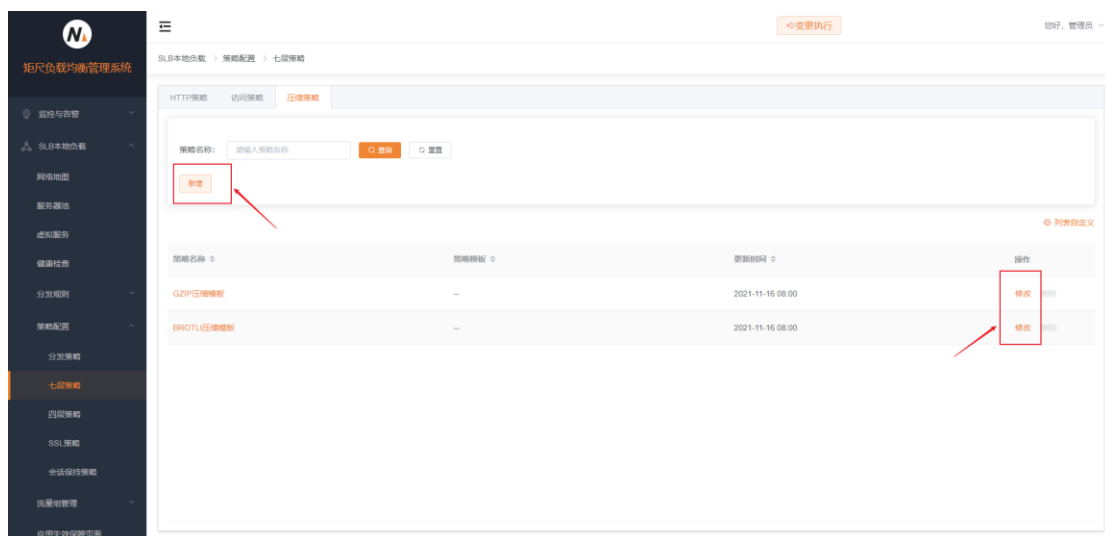
- QPS 超限返回错误码：当某个客户端请求接收速率超过 `limit_req_rate` 后的 HTTP 返回错误码。
- 最大并发请求数：并发处理请求数最大值，可以点击“不限制”复选框，不限制并发处理请求数。
- 最大并发延迟请求数：达到最大并发请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发请求时 `reject` 新请求。
- 每秒最大处理请求数：每秒处理请求数最大值，可以点击“不限制”复选框，不限制每秒处理请求数。
- 每秒最大处理延迟请求数：达到每秒最大处理请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大处理请求时 `reject` 新请求。
- 窗口时间内最大并发请求：窗口时间内最大并发请求数最大值，可以点击“不限制”复选框，不限制窗口时间内最大并发请求数。
- 窗口时间内最大并发延迟请求数：达到窗口时间内最大并发请求数后，在此范围内的请求不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发请求时 `reject` 新请求。

➤ 压缩策略

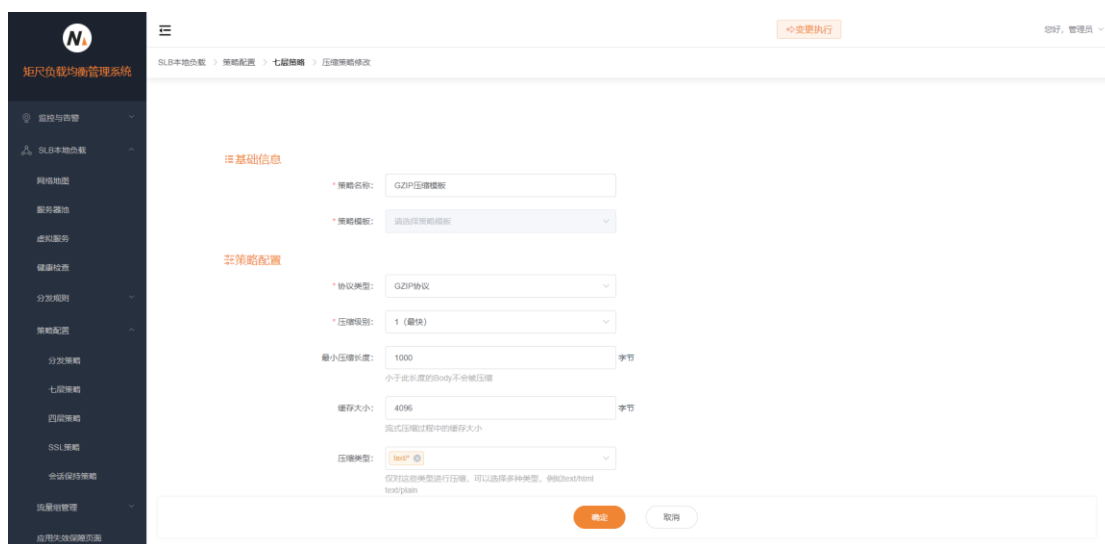
对于七层负载均衡，当需要将文件压缩后再传输给客户端时，就需要使用到压缩策略。目前压缩策略提供 2 种压缩算法：GZIP 和 BROTLI。

压缩策略在虚拟服务的 HTTP/HTTPS 协议下被引用。

点击“SLB 本地负载→策略配置→七层策略”进入七层策略页面，选择头部页签“压缩策略”可查看访问压缩列表。



点击【新增】或【修改】按钮可进入压缩策略编辑页面，

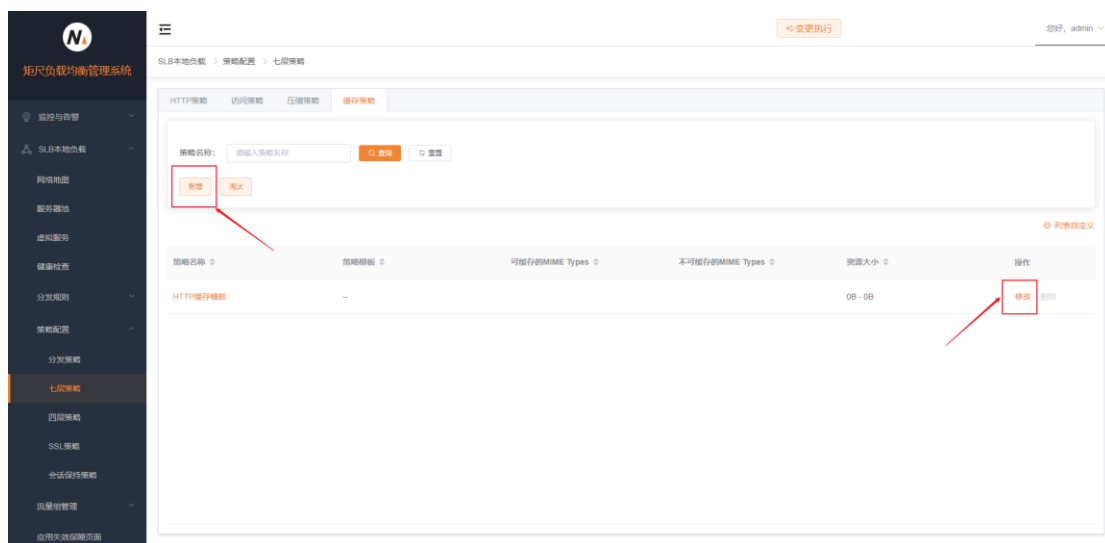


各字段含义如下所示：

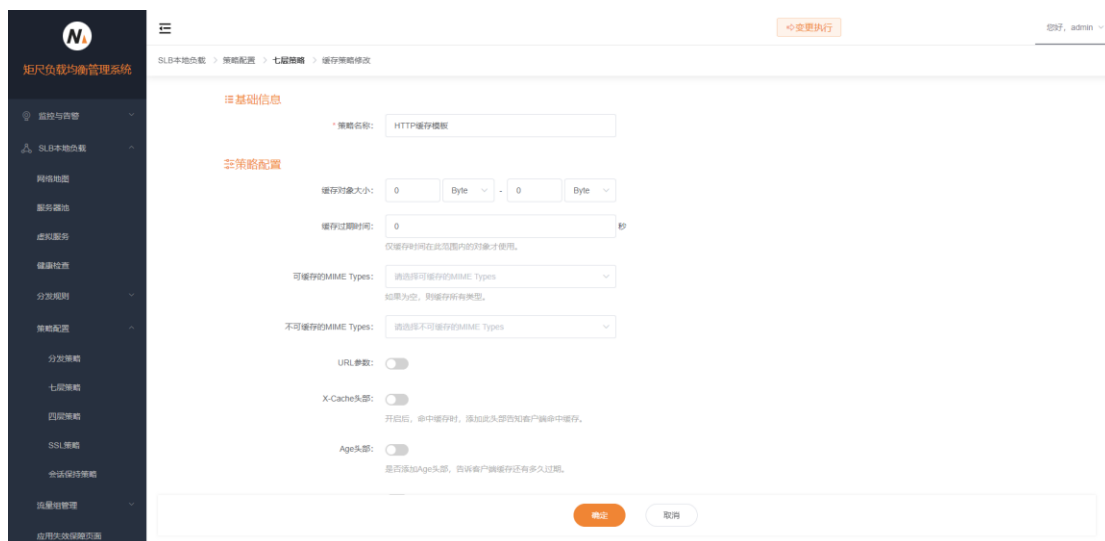
- 协议类型：目前支持 Gzip 算法和 Brotli 算法
- 压缩级别：指定算法的压缩级别
- 最小压缩长度：小于此长度的 Body 不会被压缩
- 缓存大小：流式压缩过程中的缓存大小
- 压缩类型：仅对这些类型进行压缩，可以选择多种类型，例如 text/html text/plain
- 缓冲区大小个数：基于流式压缩响应内容时，配置的内存压缩缓冲区

➤ 缓存策略

点击“SLB 本地负载→策略配置→七层策略”进入七层策略页面，选择头部页签缓存策略可查看缓存策略列表。



点击【新增】或【修改】按钮可进入缓存策略编辑页面，



各字段含义如下：

- X-Cache 头部：开启后，命中缓存时，添加此头部告知客户端命中缓存。
- Age 头部：是否添加 Age 头部，告诉客户端缓存还有多久过期。
- Data 头部：开启后，若服务器返回响应不包含 Date，则自动添加 Date 头部。
- 启发式 Expire 过期时间：不包含 Cache-Control，但包含 If-Modified-Since，使用它缓存。

- 缓存对象大小：限制缓存对象大小范围。
- URL 参数：开启或拒绝 URL 缓存。
 - URI：对应的 URI。
 - 参数：URI 对应的参数。
- 可缓存的 Mime Types：多选允许缓存的 Mime Types，如果为空，则表示缓存所有类型。
- 不可缓存的 Mime Types：多选不可缓存的 Mime Types。
- 缓存过期时间：仅缓存时间在此范围内的对象才使用。

点击淘汰按钮，可查被缓存的内容列表，可根据 URL、域名、转发引擎筛选选项过滤缓存条目：

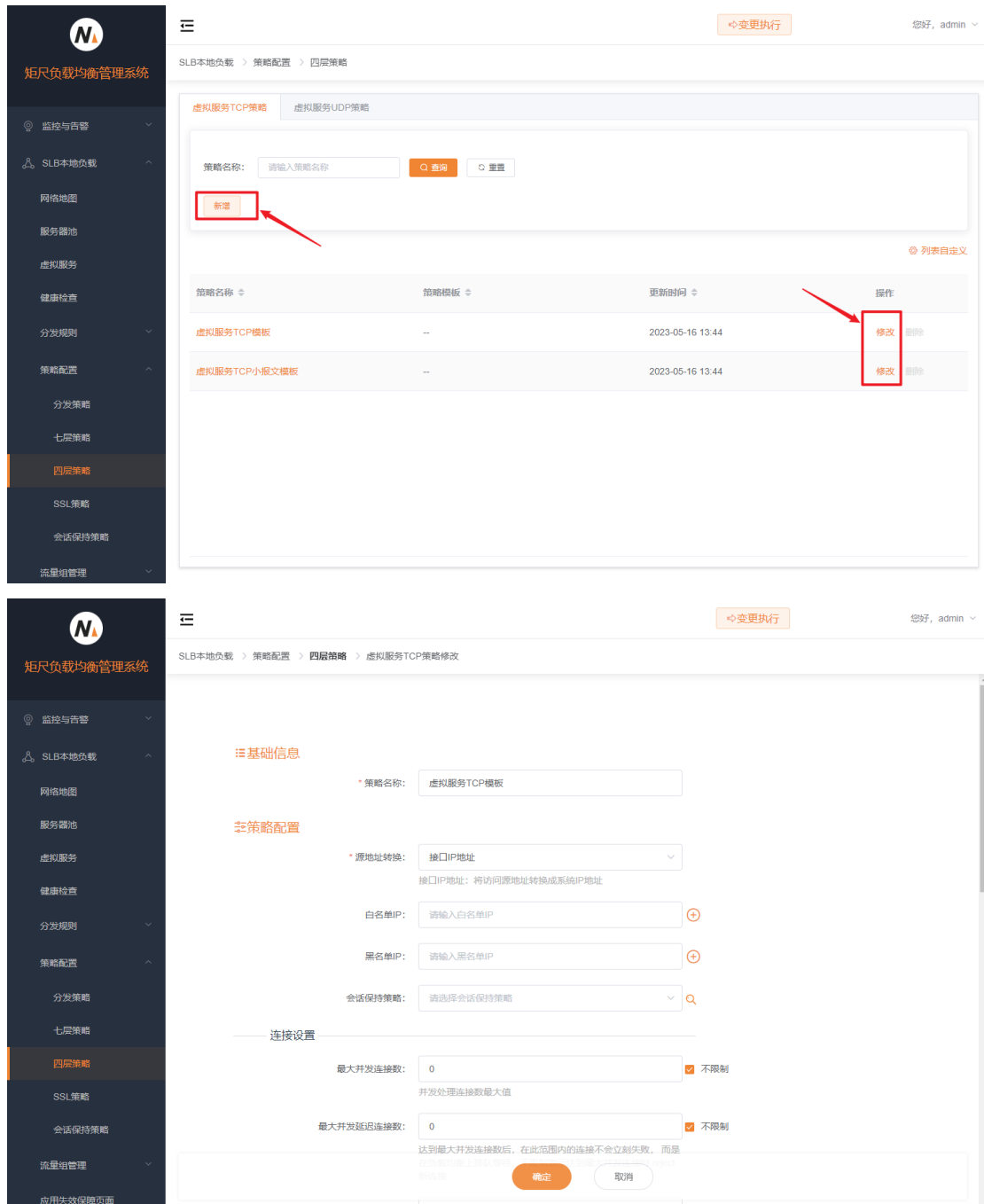
对列表某一项点击淘汰，可淘汰这条缓存。

4.6.7.3 四层策略

➤ 虚拟服务 TCP 策略

四层虚拟服务 TCP 策略会控制 TCP 连接的建链重试次数、读写超时时间、TFO、速度限制、黑白名单、并发连接数限制、源地址转换方式、Nagle 算法等特性。仅当创建客户端协议为 TCP/TLS 或者 TCP 协议的 VS 虚拟服务时，才会用到虚拟服务 TCP 策略。

在【SLB 本地负载→策略配置→四层策略】中选择头部页签虚拟服务 TCP 策略可查看虚拟服务 TCP 策略列表，点击“新增”或者“修改”，增加或变更虚拟服务 TCP 策略。



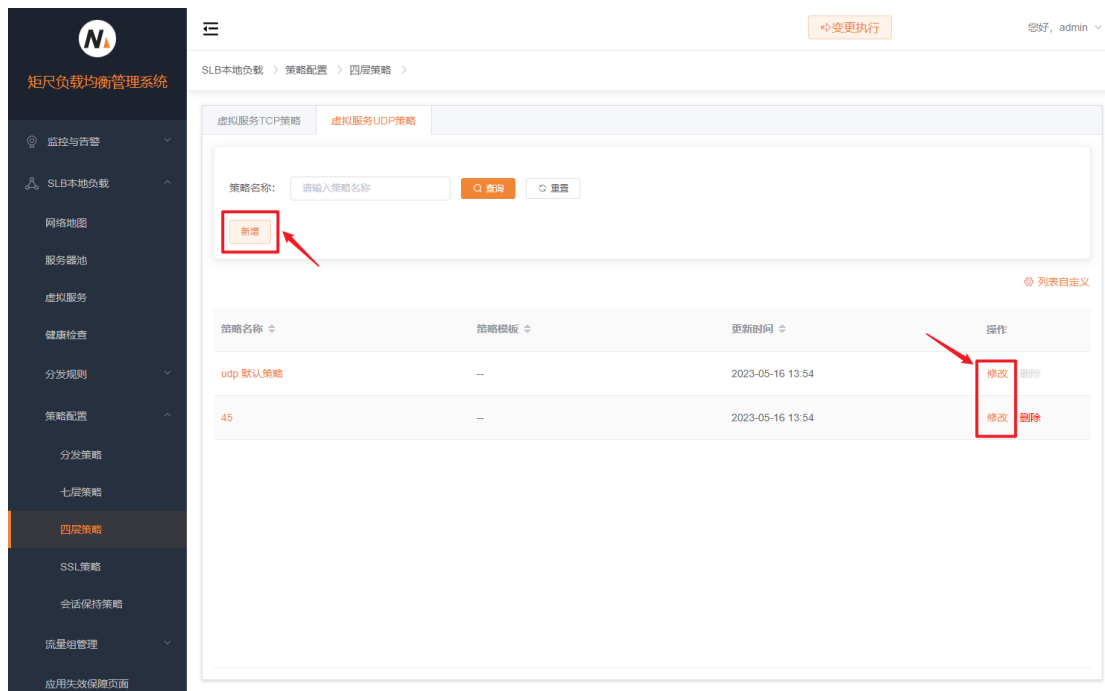
各字段含义如下所示：

- 源地址转换
 - 接口 IP 地址：将访问源地址转换成系统 IP 地址
 - 指定地址池：将访问源地址转换成指定地址池中的 IP 地址
 - 不转换：不进行源地址转换
- 白名单 IP：允许的客户端 IP
- 黑名单 IP：禁止的客户端 IP
- 会话保持策略：选择会话保持策略

- 设备最大并发连接：并发处理连接数最大值，可以点击“不限制”复选框，不限制并发处理连接数。
- 最大并发延迟连接数：达到最大并发连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发连接时 reject 新连接。
- 每秒最大处理连接数：每秒处理连接数最大值，可以点击“不限制”复选框，不限制每秒处理连接数。
- 每秒最大处理延迟连接数：达到每秒最大处理连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大处理连接时 reject 新连接。
- 窗口时间内最大并发连接：窗口时间内最大并发连接数最大值，可以点击“不限制”复选框，不限制窗口时间内最大并发连接数。
- 窗口时间内最大并发延迟连接数：达到窗口时间内最大并发连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发连接时 reject 新连接。
- 客户端最大并发连接数：并发处理连接数最大值，可以点击“不限制”复选框，不限制并发处理连接数。
- 客户端最大并发延迟连接数：达到最大并发连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发连接时 reject 新连接。
- 客户端每秒最大处理连接数：每秒处理连接数最大值，可以点击“不限制”复选框，不限制每秒处理连接数。
- 客户端每秒最大处理延迟连接数：达到每秒最大处理连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发连接时 reject 新连接。
- 客户端窗口时间内最大并发连接：窗口时间内最大并发连接数最大值，可以点击“不限制”复选框，不限制窗口时间内最大并发连接数。
- 客户端窗口时间内最大并发延迟连接数：达到窗口时间内最大并发连接数后，在此范围内的连接不会立刻失败，而是在负载均衡上排队等待，不限制表示达到最大并发连接时 reject 新连接。

➤ 虚拟服务 UDP 策略

在【SLB 本地负载→策略配置→四层策略】中选择头部页签虚拟服务 UDP 策略可查看虚拟服务 UDP 策略列表，点击“新增”或者“修改”，增加或变更虚拟服务 UDP 策略。



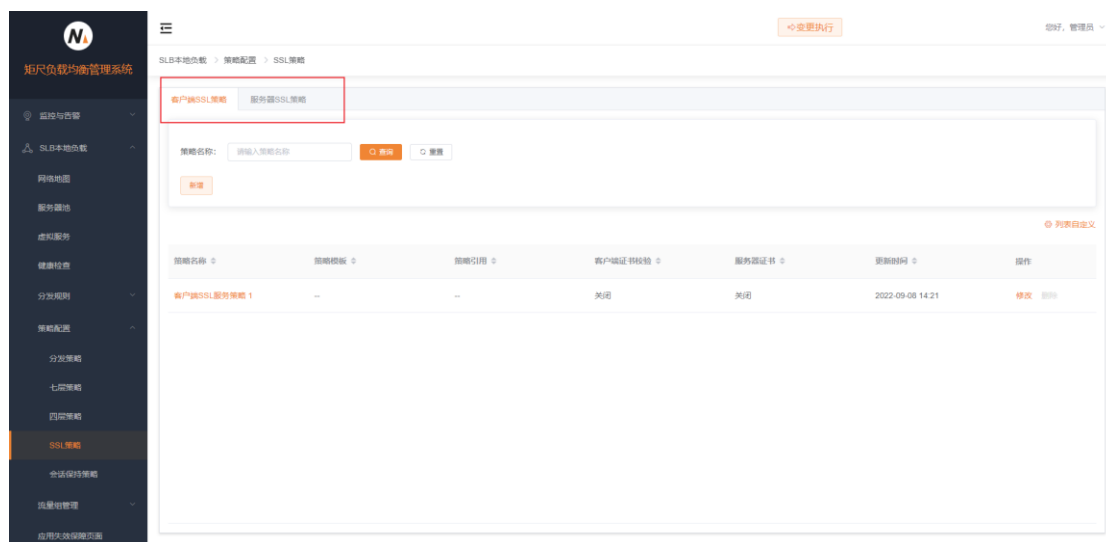
各字段含义如下所示：

- 白名单 IP：允许的客户端 IP
- 黑名单 IP：禁止的客户端 IP
- 会话保持策略：选择会话保持策略

4.6.7.4 SSL 策略

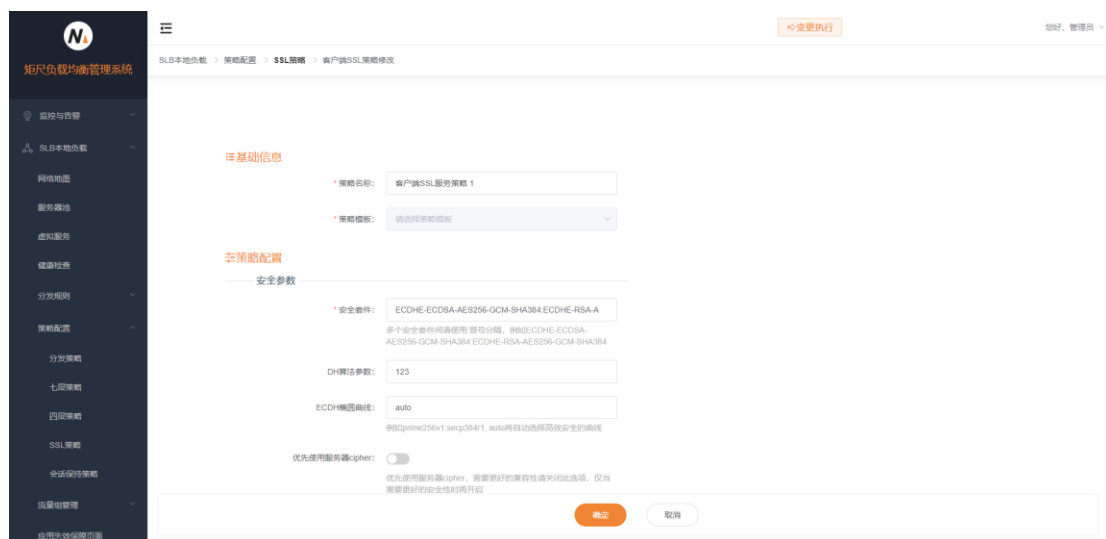
SSL 策略用于控制 SSL 安全套件、Session 缓存、Session Ticket 等参数。仅当创建客户端协议为 TCP/TLS 或者 HTTPS 的 VS 虚拟服务时，才会用到 SSL 策略。

点击“SLB 本地负载→策略配置→SSL 策略”进入到 SSL 策略配置页面，点击头部页签可切换客户端 SSL 策略和服务端 SSL 策略。



➤ 客户端 SSL 策略

在客户端 SSL 策略页签下点击【新增】或【修改】按钮可进入到客户端 SSL 策略编辑页面，如下图：



各字段含义如下所示：

- 安全套件：多个安全套件间请使用冒号分隔，例如 ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384
 - DH 算法参数：DH 协商密钥算法的参数
 - ECDH 椭圆曲线：例如 prime256v1:secp384r1, auto 将自动选择高效安全的曲线
 - 优先使用服务器 cipher：优先使用服务器 cipher，需要更好的兼容性请关闭此选项，仅当需要更好的安全性时再开启
 - 支持的 SSL 协议：支持 TLS1.3
 - Session 缓存：在本机内存中缓存 Session ID，可以减少握手的时间损耗
 - Session ticket：由客户端缓存 ticket，将会随机生成密钥
 - Session 过期时间：可用于防止重放攻击
 - SSL 握手最大超时时间：握手阶段的超时时间
 - SSL 数据缓冲区大小：发送 SSL 数据帧时的缓冲区大小
 - 客户端证书校验：当客户端携带证书时，验证证书颁发机构
 - 服务器证书：发送到客户端的证书、私钥
- 服务器 SSL 策略

在服务器 SSL 策略页签下点击【新增】或【修改】按钮可进入到服务器 SSL 策略编辑页面，如下图：

各字段含义如下所示：

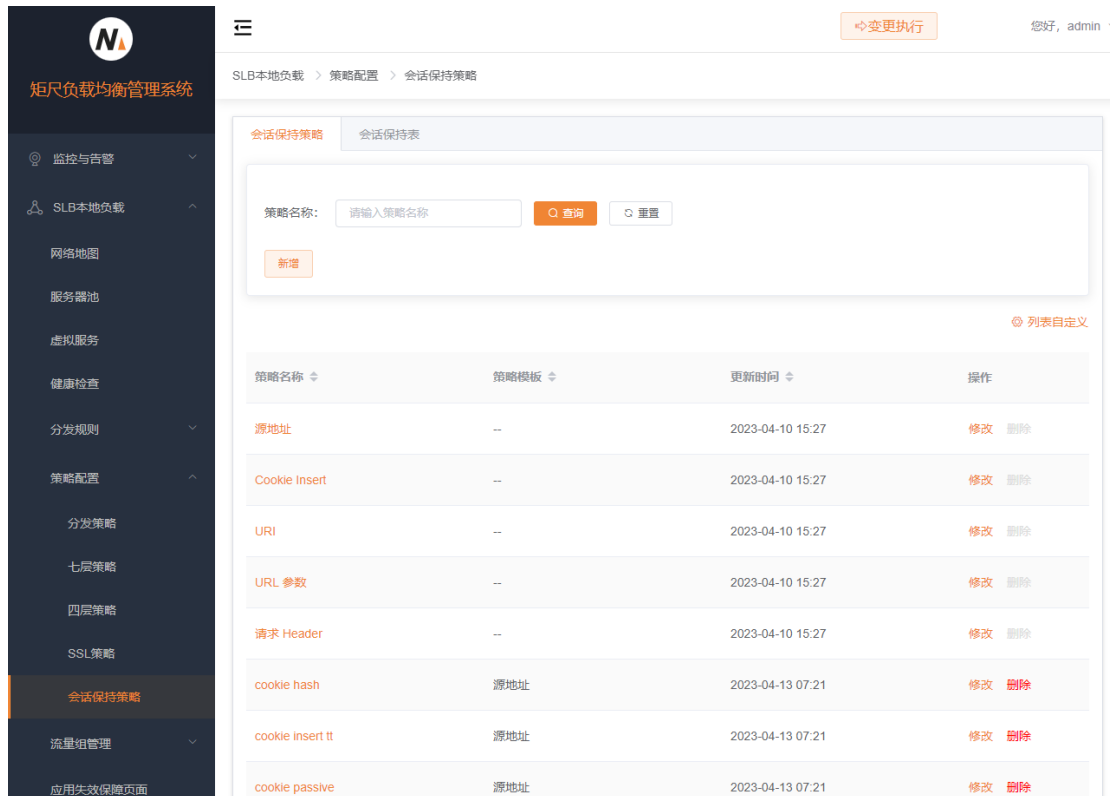
- SNI：TLS 扩展中的 Server Name Indication
- Session 复用：使用设备内存缓存 session 以提升 TLS 握手性能
- 安全套件：多个安全套件间请使用冒号分隔，例如 ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384
- 支持的 SSL 协议：支持 TLS1.3
- 客户端证书：配置证书、密钥并携带证书与服务器握手
- 服务器证书校验：校验服务器返回的证书

- 服务器通用名称：签发服务器证书时所填写的域名

4.6.7.5 会话保持策略

➤ 会话保持策略

点击“SLB 本地负载→策略配置→会话保持策略”进入会话保持策略菜单，选择头部页签“会话保持策略”可查看会话保持策略列表。



The screenshot displays the 'Session Persistence Strategy' (会话保持策略) configuration page within the 'SLB Local Load' (SLB 本地负载) management system. The left sidebar contains navigation options such as 'Monitoring and Alerts' (监控与告警), 'SLB Local Load' (SLB 本地负载), 'Network Map' (网络地图), 'Server Pool' (服务器池), 'Virtual Service' (虚拟服务), 'Health Check' (健康检查), 'Distribution Rules' (分发规则), 'Strategy Configuration' (策略配置), 'Distribution Strategy' (分发策略), 'Seven Layer Strategy' (七层策略), 'Four Layer Strategy' (四层策略), 'SSL Strategy' (SSL策略), 'Session Persistence Strategy' (会话保持策略), 'Flow Group Management' (流量组管理), and 'Application Failure Protection Page' (应用失效保障页面). The main content area shows a table of session persistence strategies. At the top, there is a search bar for strategy names and a 'New' (新增) button. The table lists various strategies like 'Source Address' (源地址), 'Cookie Insert', 'URI', 'URL Parameter', 'Request Header', 'Cookie Hash', 'Cookie Insert II', and 'Cookie Passive', each with its template, update time, and actions (Modify, Delete).

策略名称	策略模板	更新时间	操作
源地址	--	2023-04-10 15:27	修改 删除
Cookie Insert	--	2023-04-10 15:27	修改 删除
URI	--	2023-04-10 15:27	修改 删除
URL 参数	--	2023-04-10 15:27	修改 删除
请求 Header	--	2023-04-10 15:27	修改 删除
cookie hash	源地址	2023-04-13 07:21	修改 删除
cookie insert II	源地址	2023-04-13 07:21	修改 删除
cookie passive	源地址	2023-04-13 07:21	修改 删除

点击【新增】或【修改】按钮可进入 HTTP 策略编辑页面，

SLB本地负载均衡 > 策略配置 > 会话保持策略

会话保持策略 会话保持表

策略名称:

列表自定义

策略名称	策略模板	更新时间	操作
源地址	--	2023-04-10 15:27	<input type="button" value="修改"/> <input type="button" value="删除"/>
Cookie Insert	--	2023-04-10 15:27	<input type="button" value="修改"/> <input type="button" value="删除"/>
URI	--	2023-04-10 15:27	<input type="button" value="修改"/> <input type="button" value="删除"/>
URL 参数	--	2023-04-10 15:27	<input type="button" value="修改"/> <input type="button" value="删除"/>
请求 Header	--	2023-04-10 15:27	<input type="button" value="修改"/> <input type="button" value="删除"/>
cookie hash	源地址	2023-04-13 07:21	<input type="button" value="修改"/> <input type="button" value="删除"/>
cookie insert tt	源地址	2023-04-13 07:21	<input type="button" value="修改"/> <input type="button" value="删除"/>
cookie passive	源地址	2023-04-13 07:21	<input type="button" value="修改"/> <input type="button" value="删除"/>

SLB本地负载均衡 > 策略配置 > 会话保持策略 > 会话保持策略修改

基础信息

* 策略名称:

策略配置

应用类型:

* 会话保持类型:

是否共享: ☐

* COOKIE方法:

* 超时时间: 秒

* COOKIE名称:

各字段含义如下所示：

- 会话保持类型：可选择源地址段、COOKIE、URI、URL 参数、请求 Header 和 SSL Session ID
- 是否共享：对应用了同一个会话保持策略的不同虚拟服务下的相同服务器池共享会话保持规则

- COOKIE 方法：可选择 Cookie Hash、Cookie 插入、Cookie Passive 三种方式
- COOKIE 名称：当选择 Cookie Hash 或者 Cookie Passive 时，必须选择服务器会返回的 Cookie 名称；当选择 Cookie 插入时，表示设备生成的用于会话保持的 Cookie 名称
- HTTPOnly 属性：指定是否限制 Javascript 访问 Cookie
- Secure 属性：指定是否允许未经 HTTPS 加密的页面访问 Cookie
- 密钥：指定插入 Cookie 的加密密钥
- Cookie 过期：指定浏览器的 Cookie 保持时长
- 超时时间：当选择为源地址或者 Cookie Hash、Cookie Passive 时，表示会话保持的时长

➤ 会话保持表

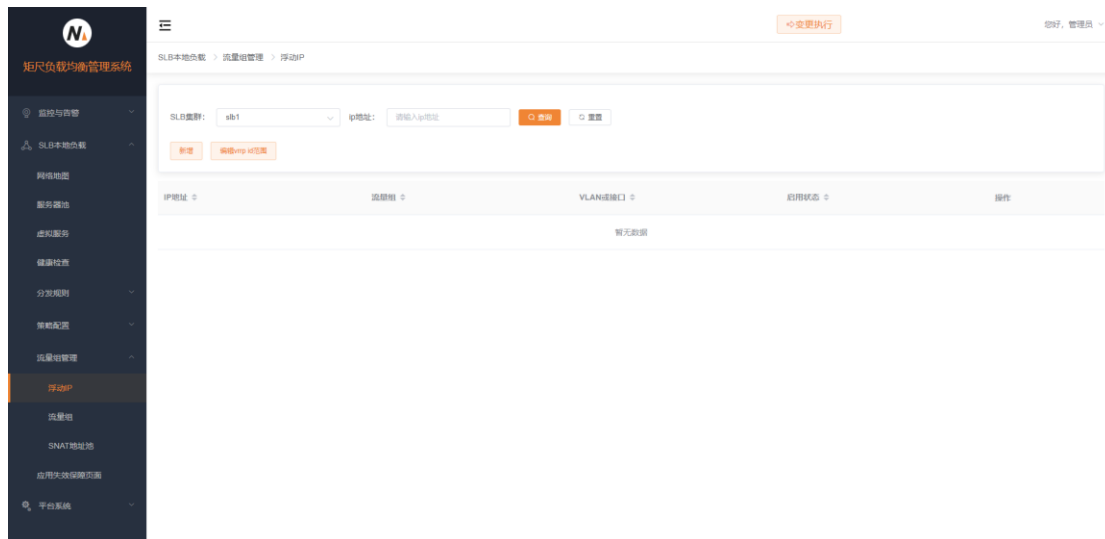
会话保持表展示内容包括会话保持值、类型、虚拟服务、服务器池、服务器节点、剩余保持时间（秒）。

点击“数据统计→会话保持表”菜单，默认展示会话保持记录统计类型，可检索字段：会话保持值、类型（源地址段、COOKIE、URI、URL 参数、请求 Header），可设置自动刷新时间。

4.6.8 流量组管理

4.6.8.1 浮动 IP

点击“SLB 本地负载→流量组管理→浮动 IP”菜单，默认展示当前已选择的 SLB 集群下按照用户创建时间倒序排列的浮动 IP 列表。

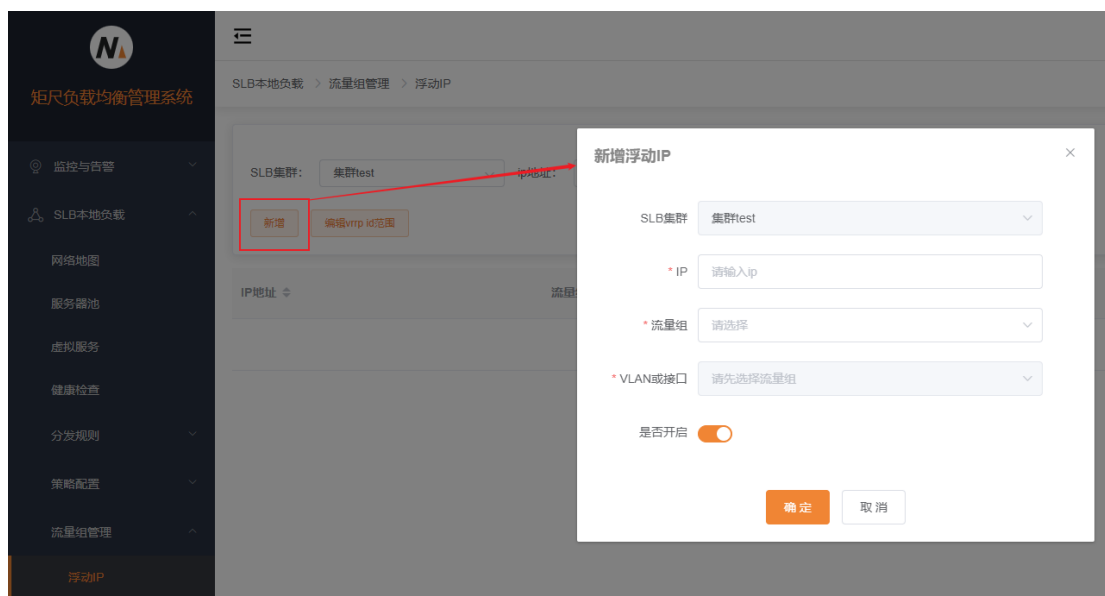


- **查询区域：**

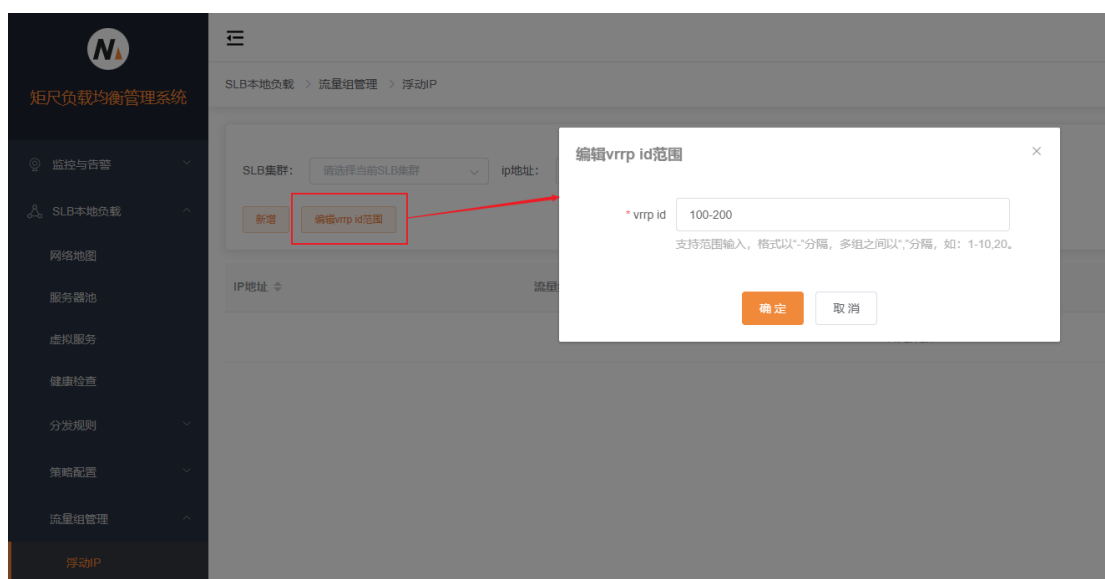
可通过“SLB 集群”、“IP 地址”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

- **数据区域：**

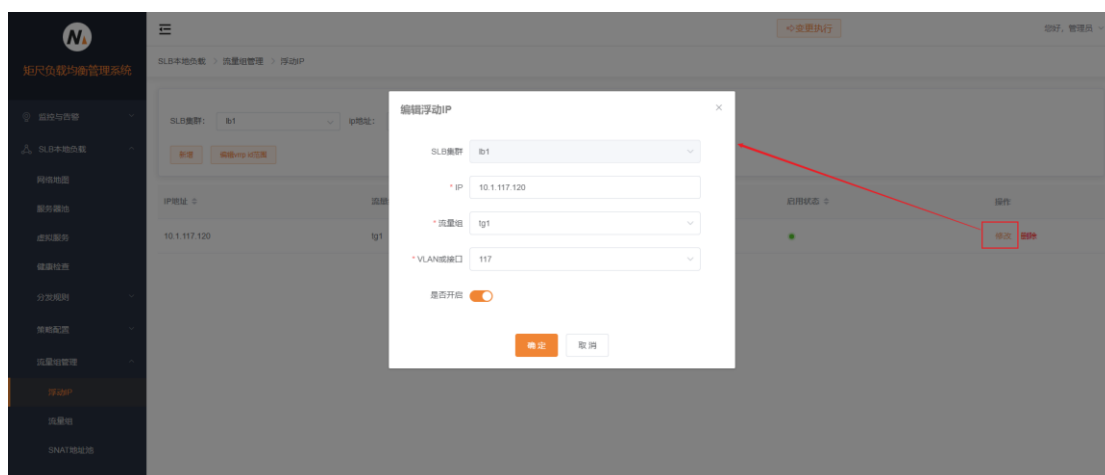
点击列表上方【新增】按钮，打开浮动 IP 地址新增弹框，可添加/配置新的浮动 IP，支持 IPv6 协议，可选配置在 VLAN 或接口上。



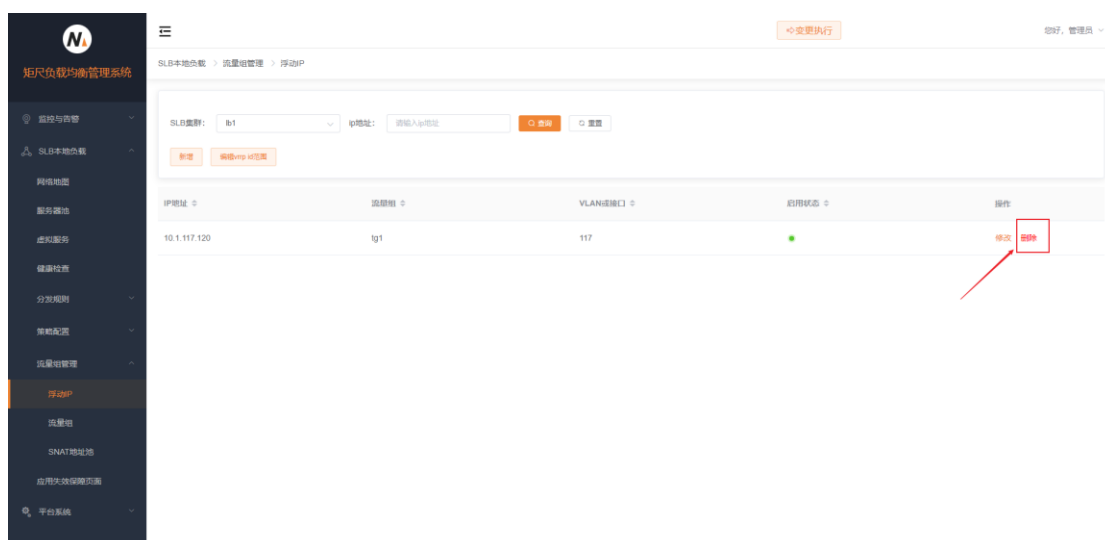
点击列表上方【编辑 vrrp id 范围】按钮，打开编辑 vrrp id 弹框，可编辑 vrrp id 范围。



选择需要修改的浮动 IP，点击此用户所在行操作栏的【修改】按钮，弹框打开浮动 IP 修改页面，可启用或关闭该浮动 ip。



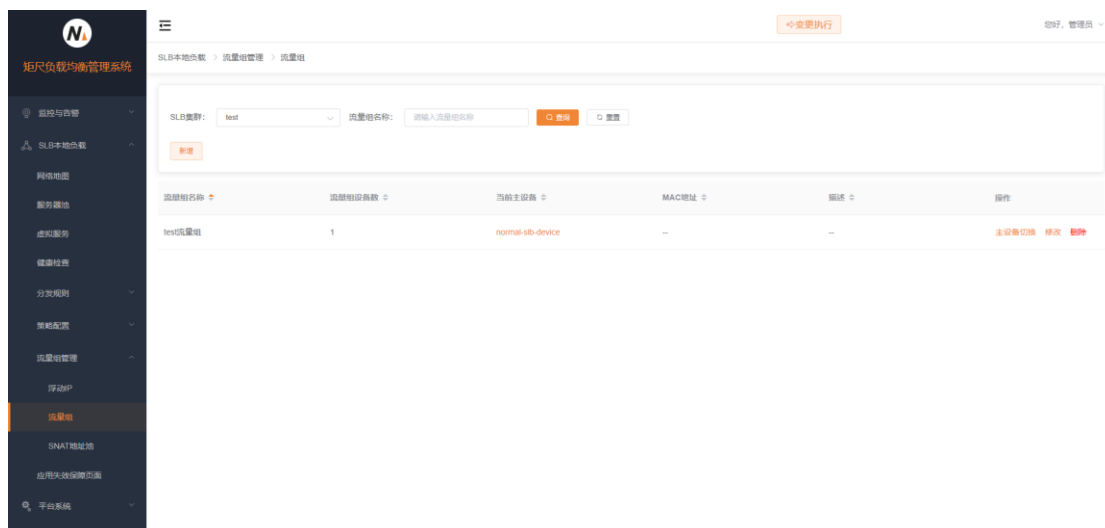
选择需要删除的浮动 IP 信息，然后操作栏的【删除】按钮，可对浮动 IP 进行删除操作。



4.6.8.2 流量组

流量组配置主要实现，将一个集群中的多个设备划分为一个或多个流量组。配置了的流量组在创建虚拟服务、接口地址时进行调用。

点击“SLB 本地负载→流量组管理→流量组”菜单，默认展示当前已选择的 SLB 集群下按照用户创建时间倒序排列的流量组信息列表。



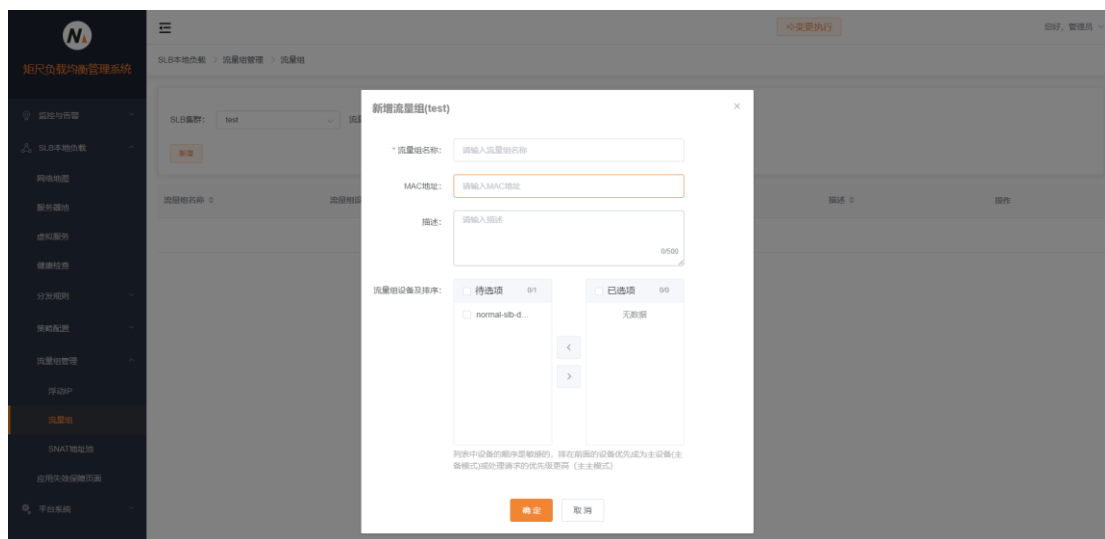
● 查询区域：

可通过“SLB 集群”、“流量组名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

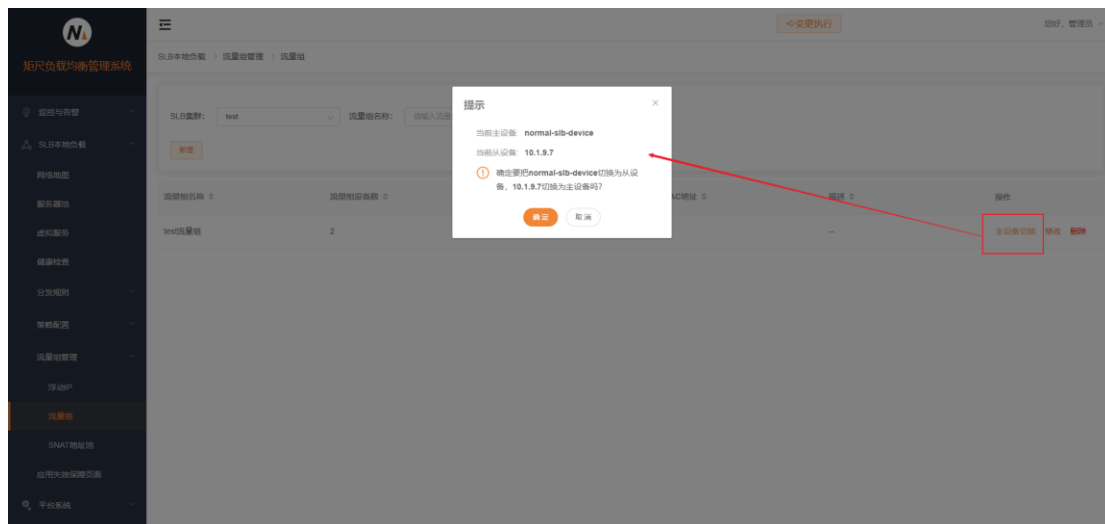
● 数据区域：

点击列表上方【新增】按钮，弹框打开流量组新增页面，可添加/配置新的流量组信息。

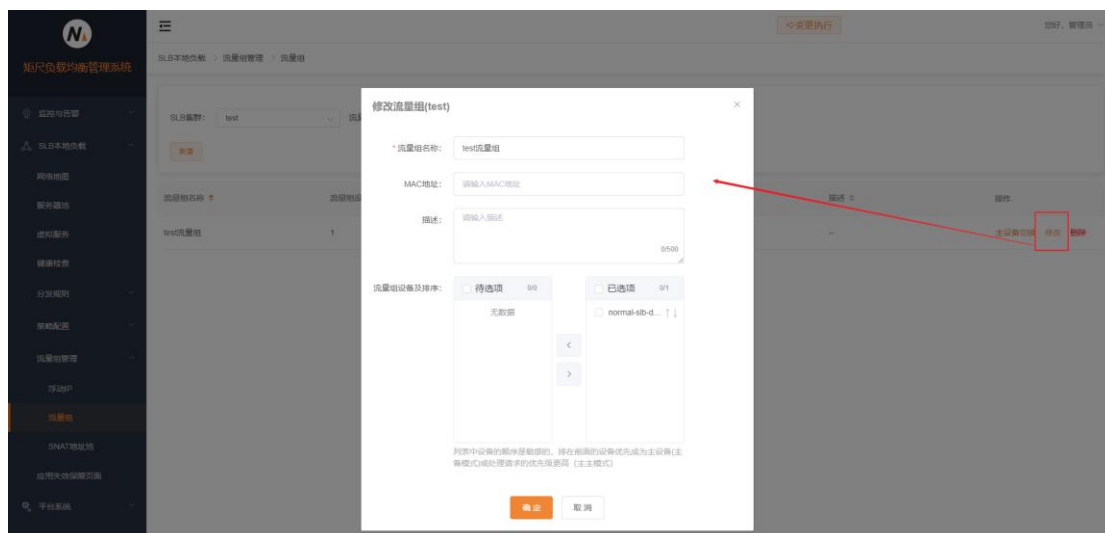
新增流量组时排在第一的设备默认为主设备。



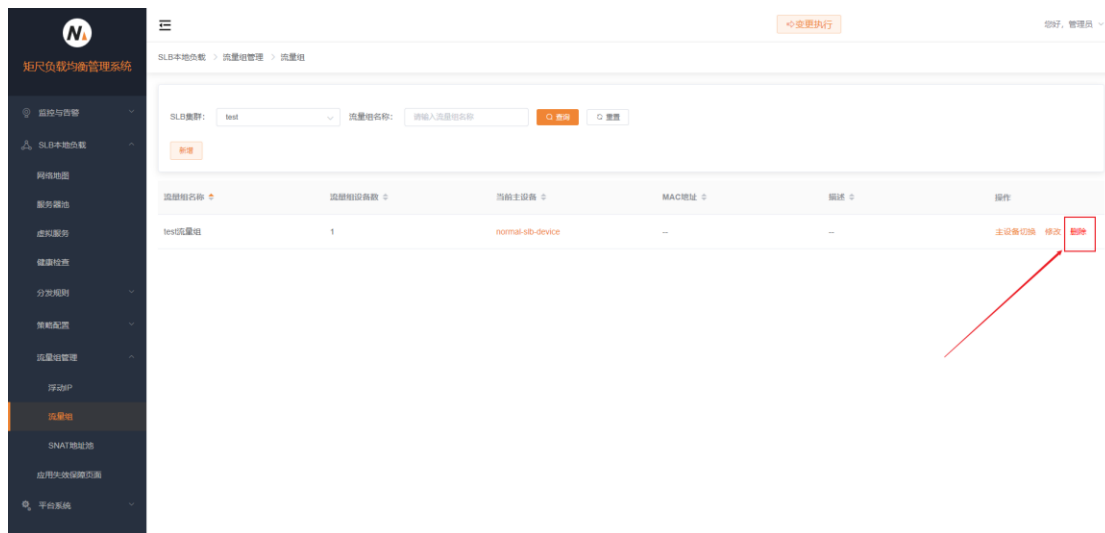
点击【主设备切换按钮】，可将流量组内的主从设备互换。



修改流量组：选择需要修改的流量组信息，点击此用户所在行操作栏的【修改】按钮，弹框打开流量组信息修改页面。



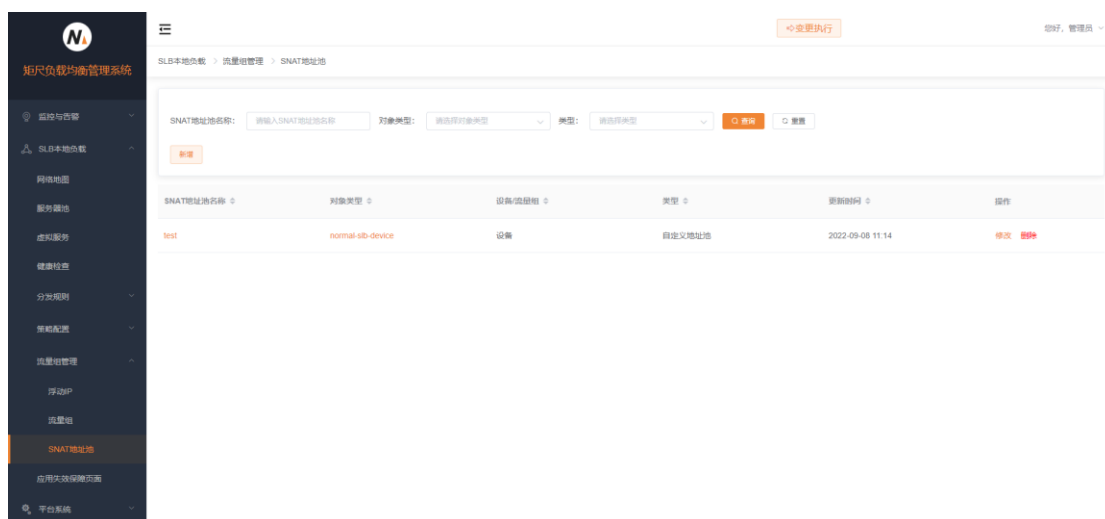
选择需要删除的流量组信息，然后操作栏的【删除】按钮，可对流量组信息进行删除操作。



注：如果用户要删除流量组信息已被接口地址或虚拟服务进行关联，则无法删除成功。

4.6.8.3 SNAT 地址池

点击“SLB 本地负载→流量组管理→SNAT 地址池”菜单，将展示所有的SNAT 地址池：



● 查询地址池：

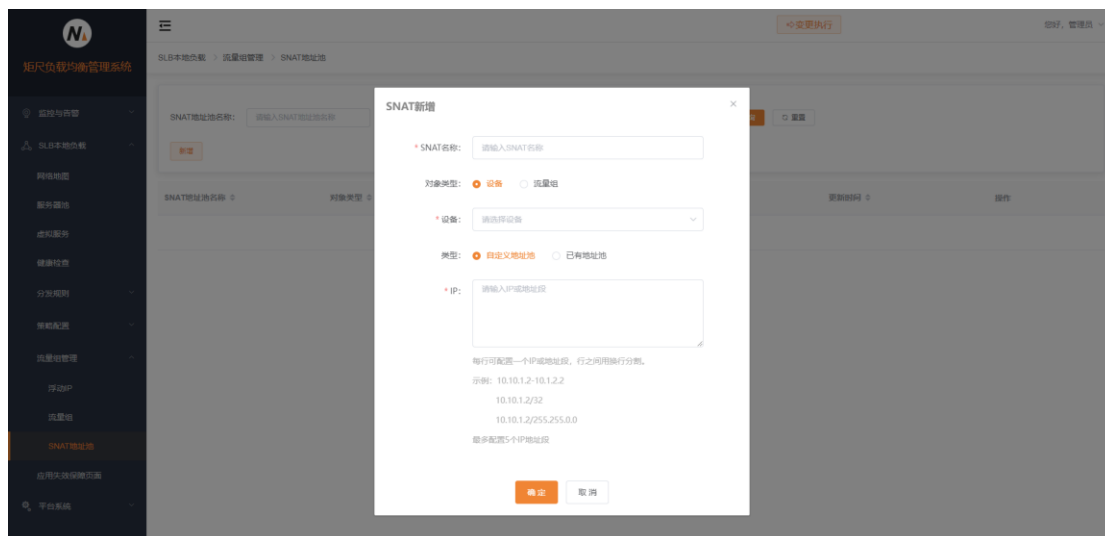
可通过“SNAT 名称”进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空。

SNAT 地址池的对象类型分为“流量组”或者“设备”2 种，前者应用于对象类型同为“流量组”的虚拟服务，后者应用于对象类型同为“设备”的虚拟服务，您可以通过“对象类型”选项进行切换；

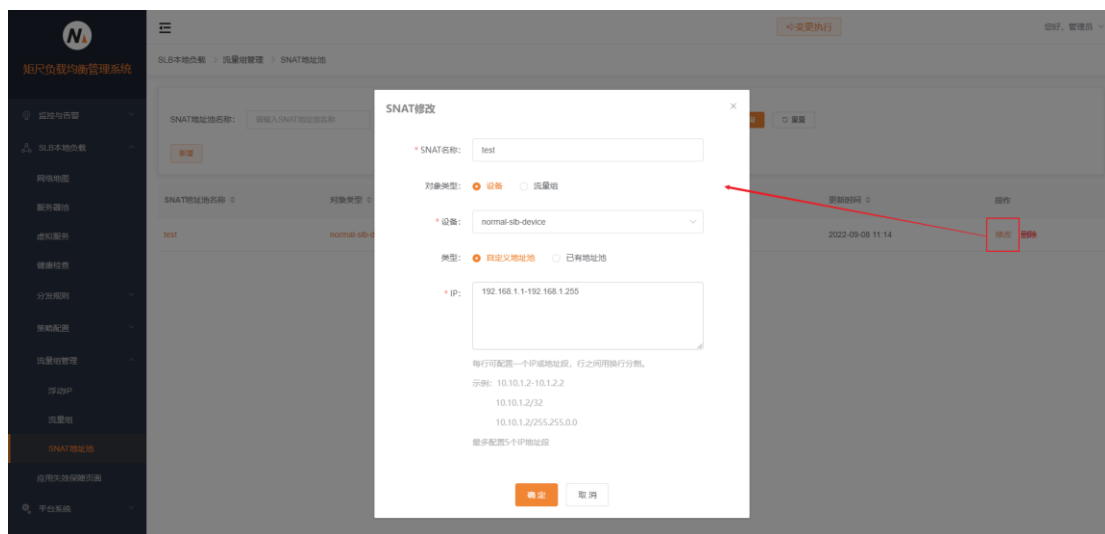
SNAT 地址池可以使用已经存在的本地 IP 地址或者浮动 IP 地址，也可以创建新的自定义 IP 地址（支持 IPv6），您可以通过“类型”选项进行切换；

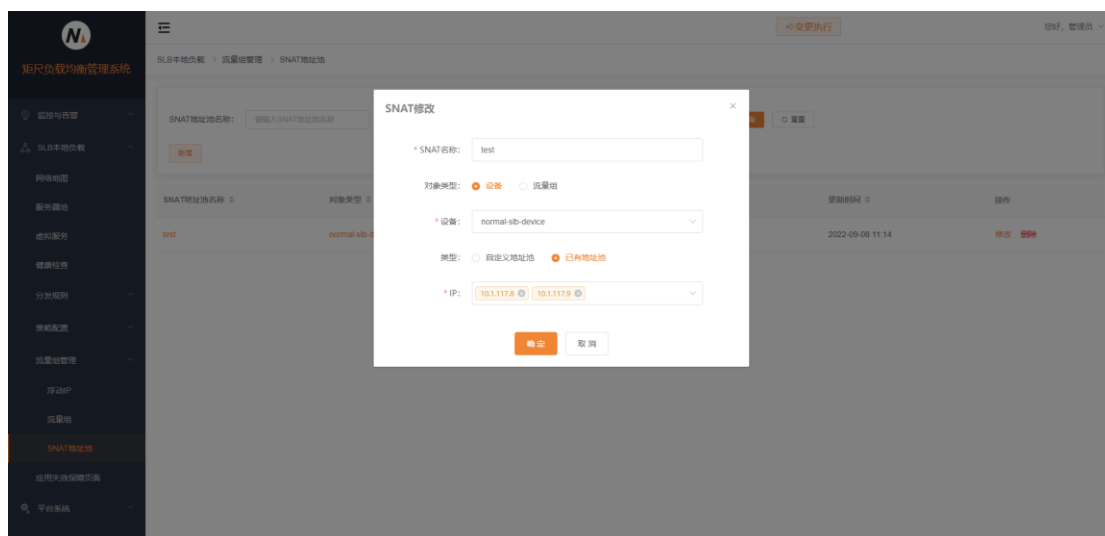
● 数据区域：

新增 SNAT 地址池：点击列表上方【新增】按钮，弹框打开 SNAT 地址池新增页面，可添加/配置新的 SNAT 地址池：



选择需要修改的 SNAT 地址池信息，点击此用户所在行操作栏的【修改】按钮，弹框打开 SNAT 地址池信息修改页面。





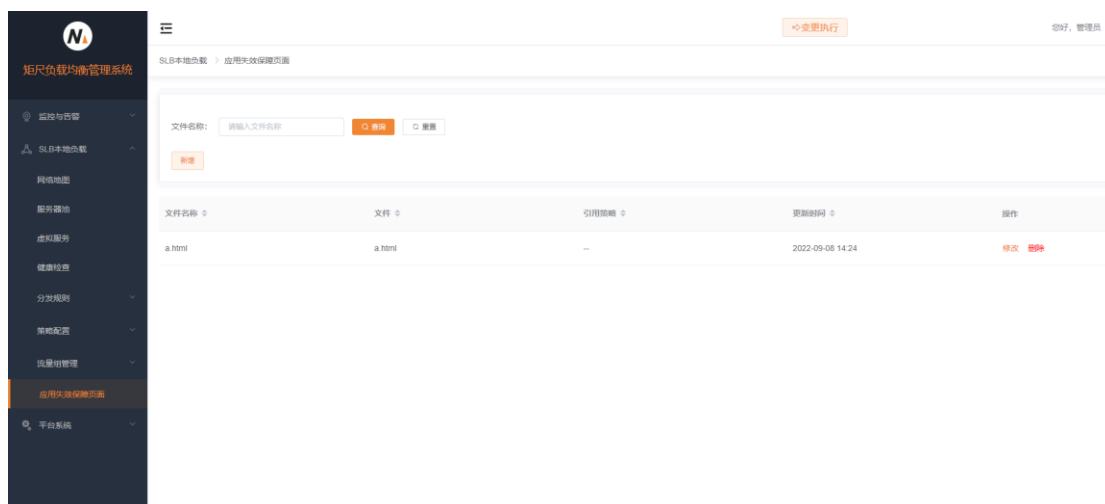
选择需要删除的 SNAT 地址池信息，然后操作栏的【删除】按钮，可对 SNAT 信息进行删除操作。

注：如果用户需要删除的 SNAT 地址池已被虚拟服务进行关联，则无法删除成功。

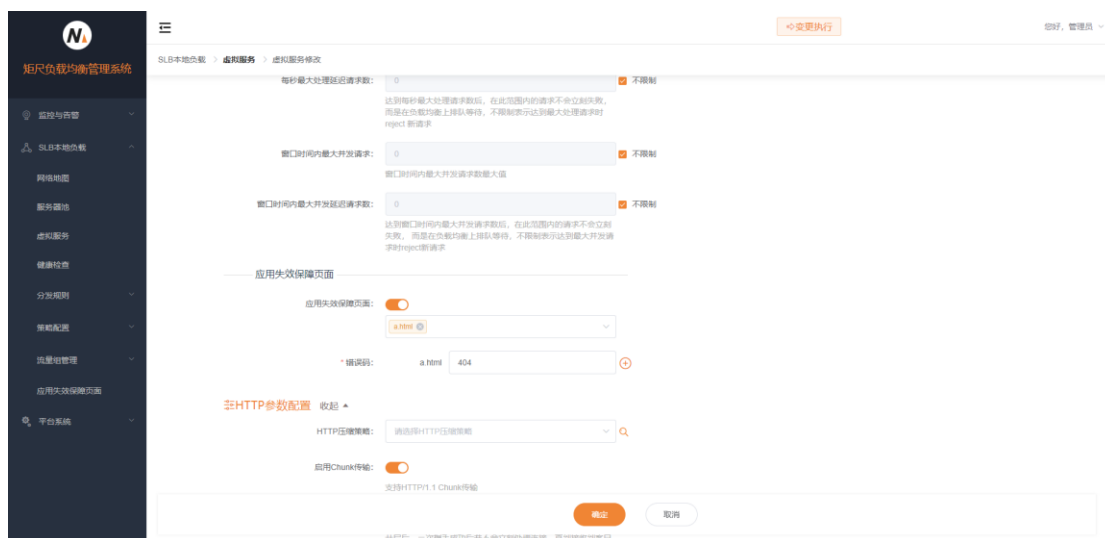
4.6.9 应用失效保障页面

当七层虚拟服务中服务器返回特定的 HTTP 错误码时，可以改为向用户返回特定的页面。

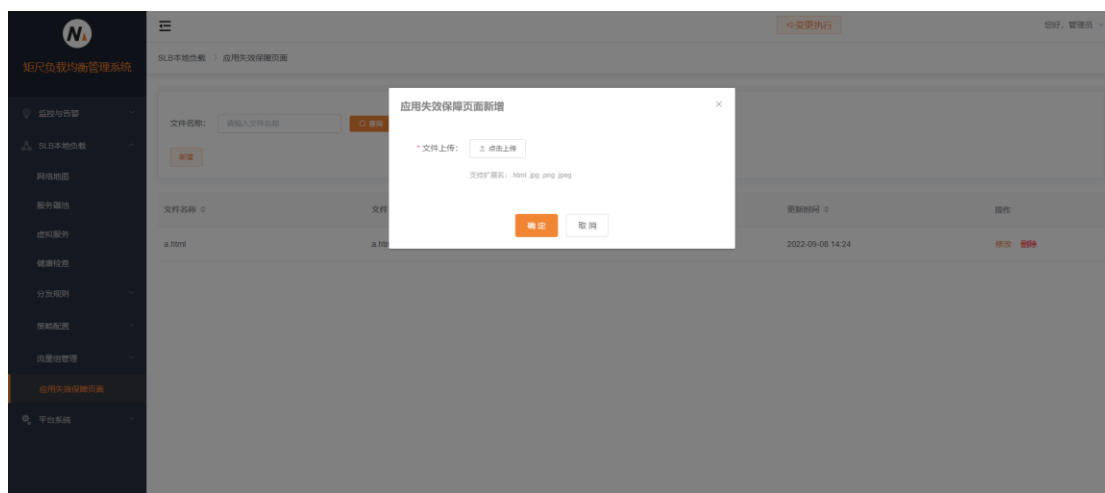
点击“SLB 本地负载→应用失效保障页面”菜单，可以看到已经准备好的页面文件。



这些页面将在“虚拟服务”HTTP/HTTPS 协议下被引用：



可以点击列表上方的“上传”按钮，上传新的应用失效保障页面：

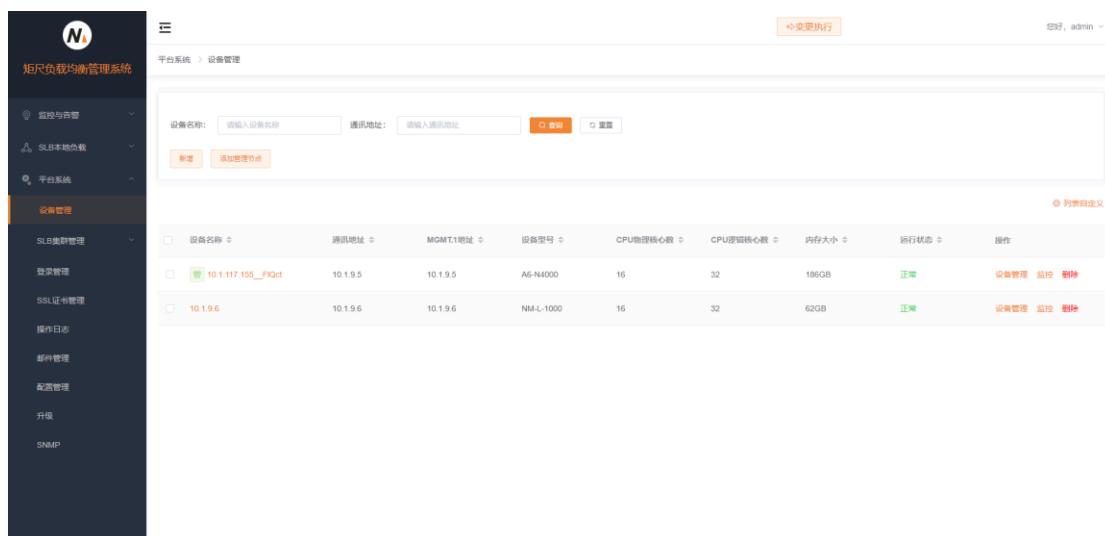


4.7 平台系统

4.7.1 设备管理

设备管理实现在用户收到设备后，此时需要初始化系统，录入设备的相关信息，在 SLB 集群中进行设备关联。同时在设备关联页面，可查询到设备当前的运行状态。

点击“平台系统→设备管理”菜单，默认按照设备创建时间倒序展示设备信息列表。



● 查询区域：

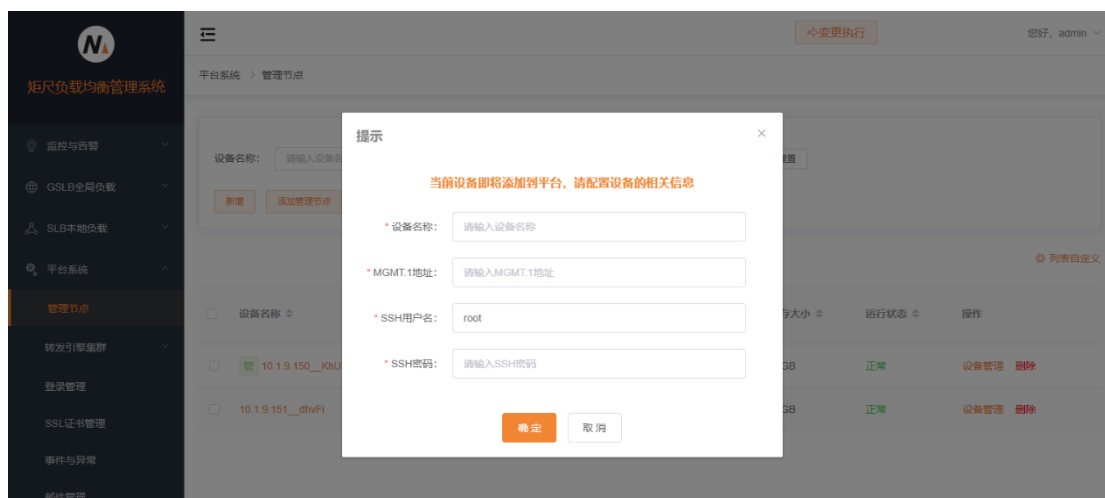
可通过“设备名称”、“通讯地址”属性，进行条件模糊查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空。

● 数据区域：

➤ 新增设备

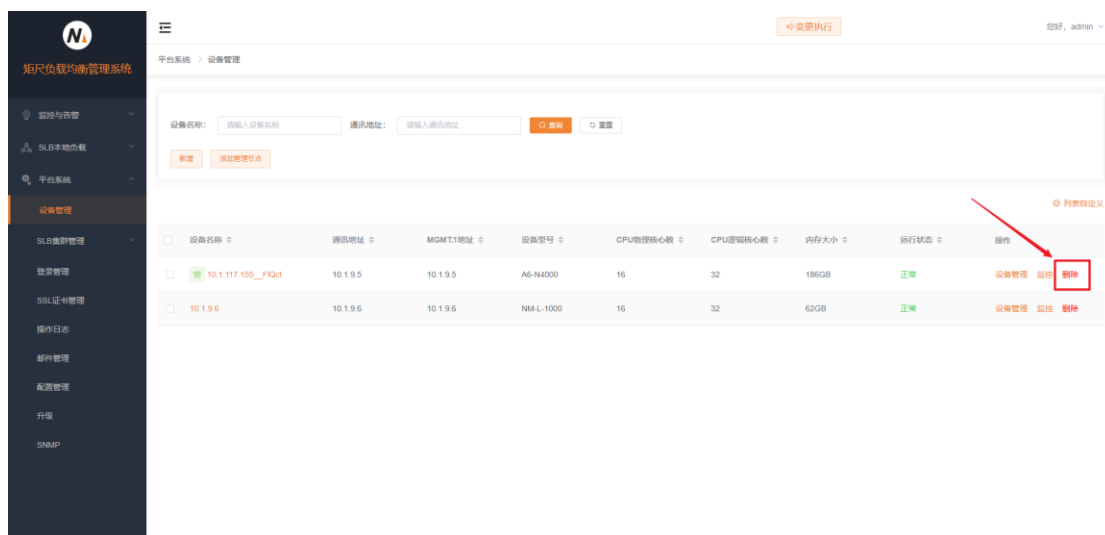
点击列表上方【新增】按钮，弹框打开设备新增页面，可添加/配置新设备信息。

‘通讯地址’为可输入的单选下拉框，默认提示文字“请输入通讯地址”；失去焦点后，检验地址是否有效，有效的地址下拉框后显示“√”，同时显示此地址对应的型号，可下拉选择接口返回的其他 IP 地址；无效的地址下拉框后显示“X”，地址无效无法保存成功。默认用户名为 root，密码为 n6_normae



➤ 删除设备

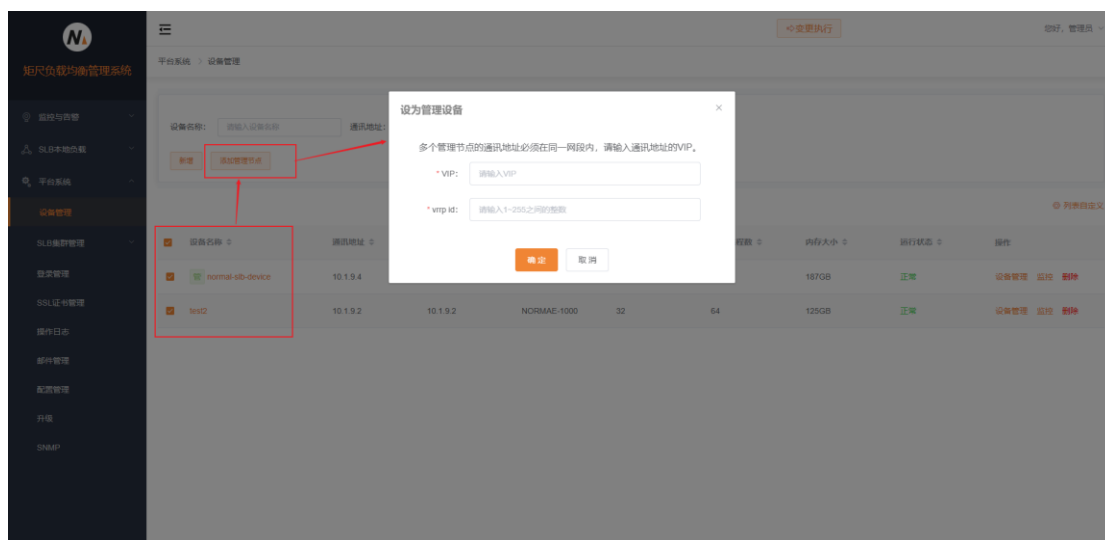
选择需要删除的设备信息，然后操作栏的【删除】按钮，可对设备信息进行删除操作。



注：如果要删除的设备已被 SLB 集群关联，则无法删除成功。

➤ 添加管理设备

选择需要设置成管理设备的设备，并点击【添加管理设备】按钮，实现多管理设备的配置。



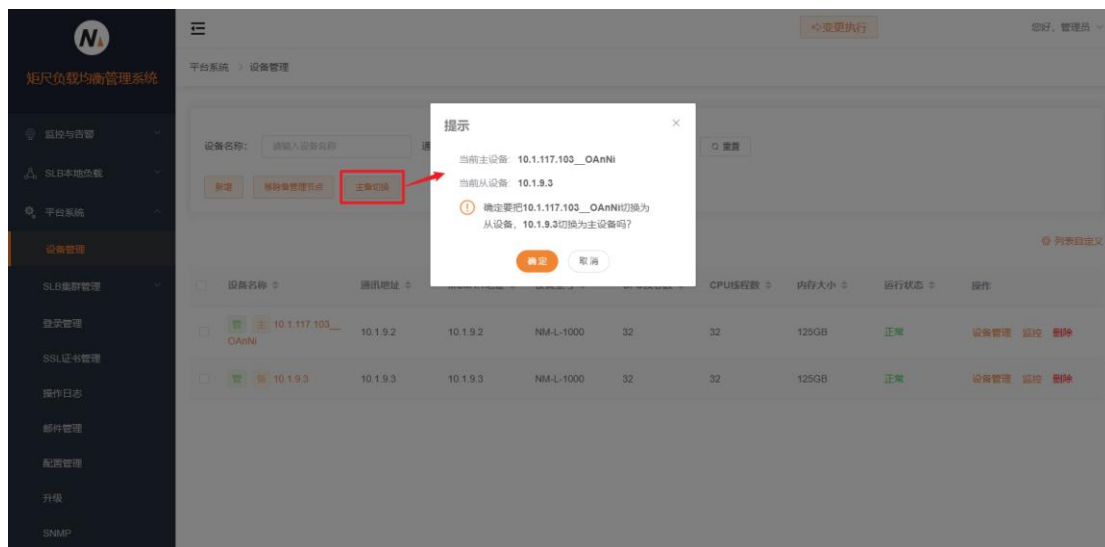
注：默认第一个加入平台的设备为管理设备，其他设置皆为非管理设备，可以同时设置两个设备组成高可用集群：

- (1) 选择需要设置为管理设备的设备状态必须是正常的；

- (2) 同时选择多个设备作为管理设备时，需要输入 VIP 和 vrrp id；
- (3) 同时选择两个设备作为管理设备时，默认之前那台管理设备为主设备，另一台为管理设备。

➤ 主备切换

当两台设备都为管理设备时，其中一台为主设备，搜索栏会出现【主备切换】按钮，点击主备切换按钮可将这两台设备进行主备切换。



➤ 设备信息修改

在设备列表中点击【设备管理】按钮，可进入这台设备管理页面，详见“[4.8.1 设备管理](#)”。

4.7.2 SLB 集群管理

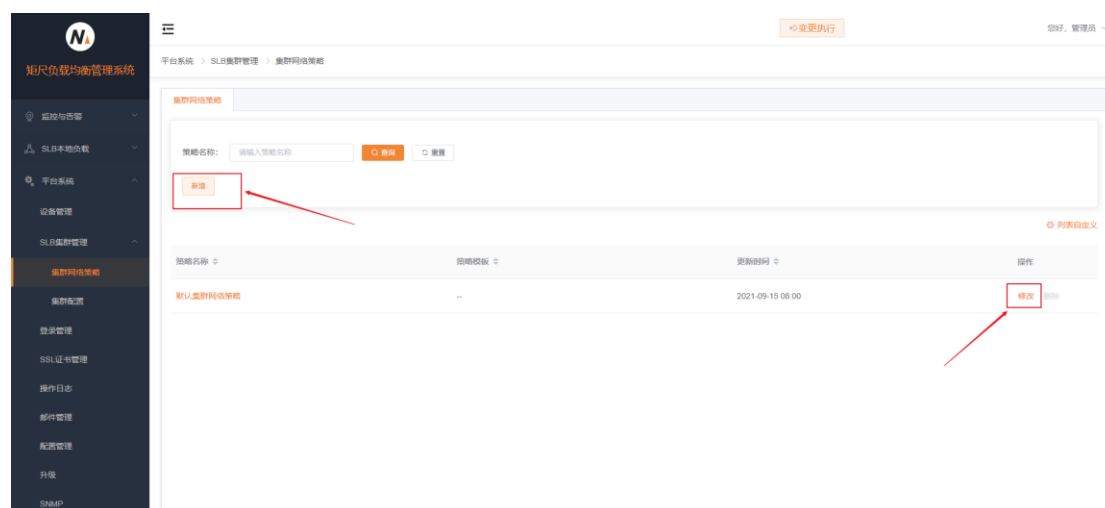
SLB 集群实现将一组设备进行组合起来接收和处理流量，通过选择并应用“平台系统→SLB 集群管理→集群网络策略”中创建的集群网络策略。可查看 SLB 集群中设备的运行状况。

4.7.2.1 集群网络策略

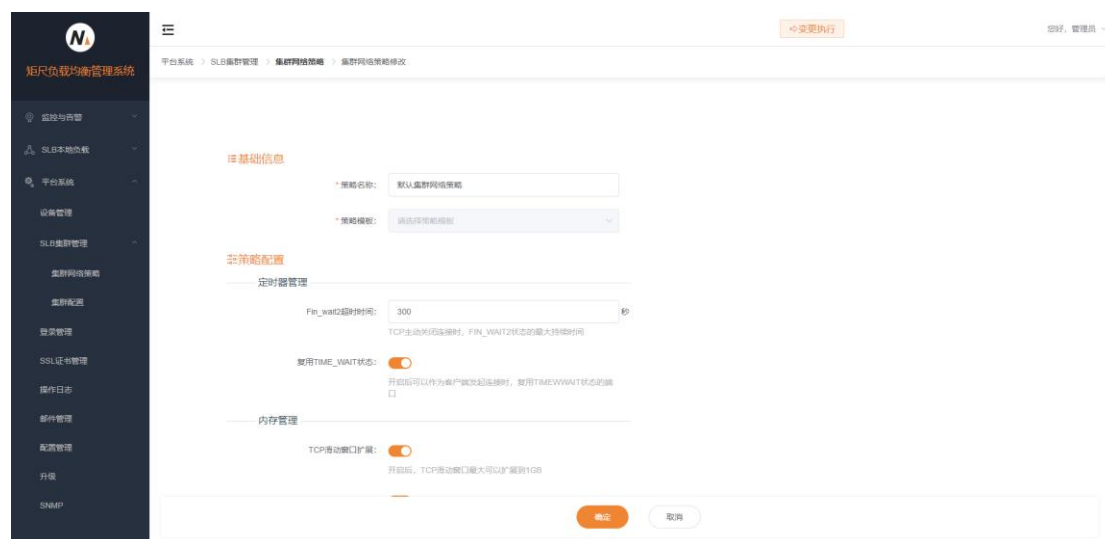
您需要对每个 SLB 集群配置“集群网络策略”，以改变集群中各设备的网络参数，包括拥塞控制算法、TCP 握手重试次数等。通常，您可以使用设备出

厂提供的“默认集群网络策略”，您可以修改“默认集群网络策略”中的参数，也可以基于“默认集群网络策略”创建新的集群网络策略。您可以在多个 SLB 集群中复用同一个“集群网络策略”

在【平台系统→SLB 集群管理→集群网络策略】中点击“新增”或者“修改”，变更集群网络策略。



根据网络要求修改集群网络策略中的参数：



各字段含义如下所示：

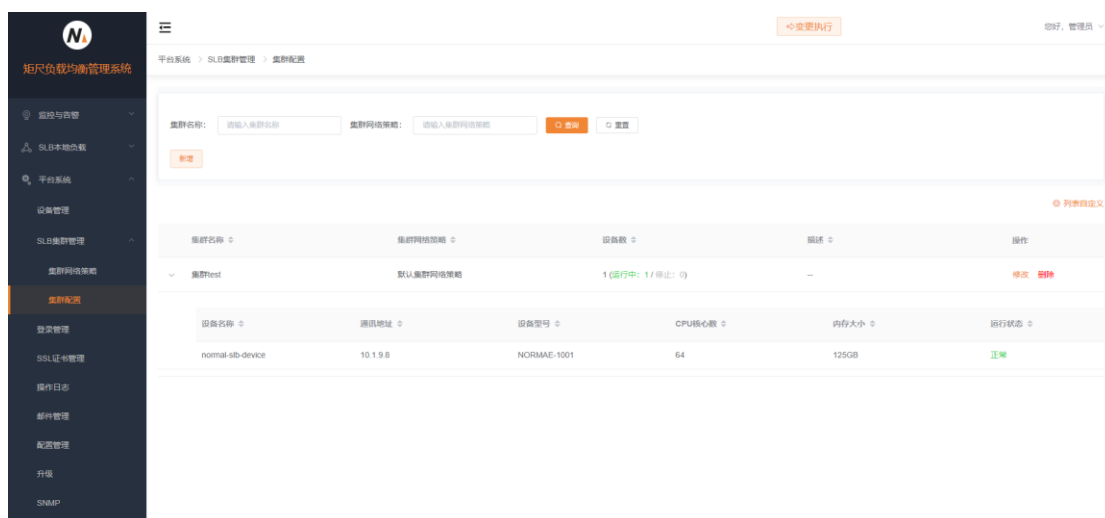
- **Fin_wait2 超时时间：**TCP 主动关闭连接时，FIN_WAIT2 状态的最大持续时间
- **复用 TIME_WAIT 状态：**开启后可以作为客户端发起连接时，复用 TIMEWAIT 状态的端口
- **TCP 滑动窗口扩展：**开启后，TCP 滑动窗口最大可以扩展到 1GB

- TCP 缓冲区自动调整：开启后，在高并发状态下会降低单连接缓冲区，在低并发下会提升连接的收发速度
- TCP 发送缓冲区最小值：TCP 缓冲区自动调整开启后，设置发送缓冲区的最小值
- TCP 发送缓冲区初始值：TCP 缓冲区自动调整开启后，设置发送缓冲区的初始值
- TCP 发送缓冲区最大值：TCP 缓冲区自动调整开启后，设置发送缓冲区的最大值
- TCP 接收缓冲区最小值：TCP 缓冲区自动调整开启后，设置接收缓冲区的最小值
- TCP 接收缓冲区初始值：TCP 缓冲区自动调整开启后，设置接收缓冲区的初始值
- TCP 接收缓冲区最大值：TCP 缓冲区自动调整开启后，设置接收缓冲区的最大值
- RST on overflow：开启后，在 SYN 过载后直接向客户端发送 RST 报文；关闭后，则直接丢弃 SYN 报文，这样客户端握手的超时重发机制仍然有效
- MSS：MSS 大小，应与交换机设置保持一致
- IPv4 TTL：IPv4 报文中 Time To Live 字段的默认大小
- IPv6 TTL：IPv6 报文中 Time To Live 字段的默认大小
- 拥塞控制算法：目前支持 CUBIC 和 RENO 算法
- Explicite Congestion Notification 显式拥塞通知：定义于 RFC 3168，开启后允许拥塞控制端对端通知，从而可以避免丢包
- 初始拥塞窗口：对于 CDN 等高速网络，可以提升该窗口大小
- 慢启动：开启慢启动可以避免网络拥塞
- SACK：开启后可以精确重传丢失报文，避免 TCP 递增序列号的描述能力不足
- DSACK：参见 RFC2883，开启后可以提升 SACK 的效率
- FACK：对于 SACK 重传阶段进行拥塞流控
- Tcp_recovery：开启丢包恢复功能，参见 RFC6675
- SYN 最大重发次数：SYN 丢失后的最大重发次数
- SYN_ACK 帧最大重发次数：作为服务器建立三次握手时，SYN_ACK 帧丢失后的最大重发次数
- FIN 帧最大重发次数：关闭连接时，FIN 帧丢失后的最大重发次数

Early retrans 早期重传：开启后可以改进快速重传的效率

4.7.2.2 集群配置

点击“平台系统→SLB 集群管理→集群配置”菜单，默认按照用户创建时间倒序展示 SLB 集群信息列表。

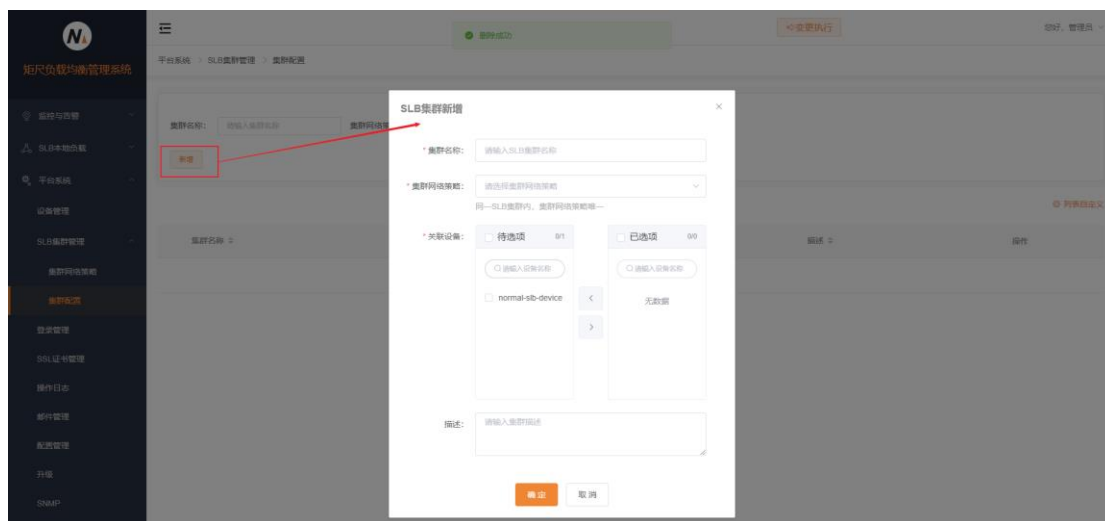


● 查询区域：

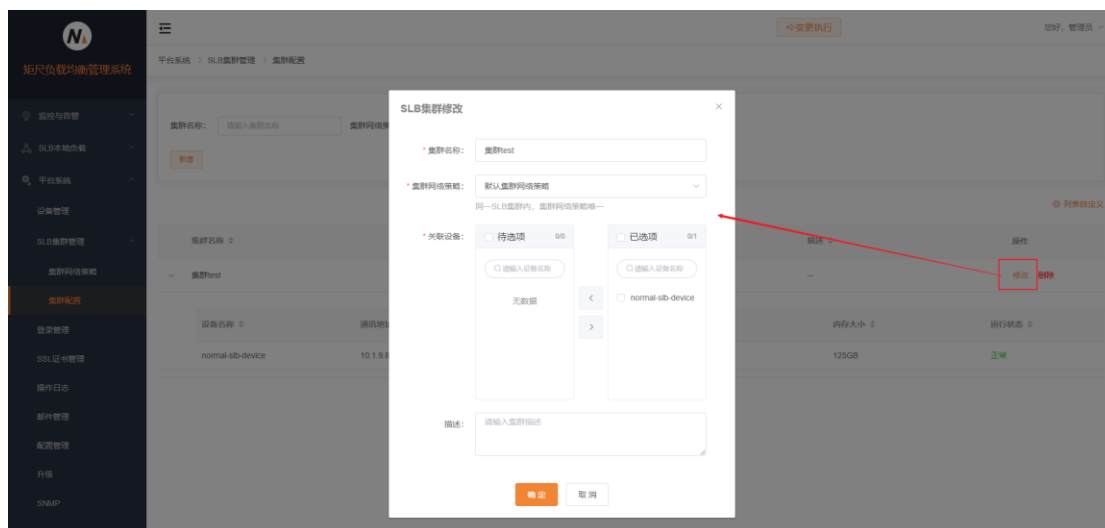
可通过“集群名称”、“集群网络策略”属性，进行条件模糊查询操作。
点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域：

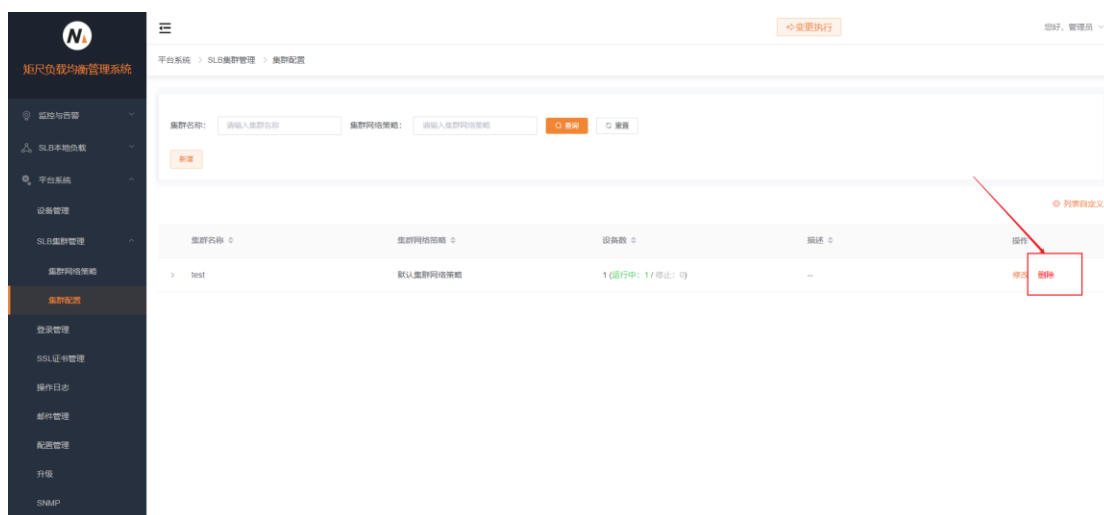
点击列表上方【新增】按钮，弹框打开 SLB 集群新增页面，可添加/配置新的 SLB 集群信息：注：SLB 集群和集群网络策略是一一对应关系；一个 SLB 集群可以选择两台设备。



选择需要修改的 SLB 集群信息，点击此用户所在行操作栏的【修改】按钮，弹框打开 SLB 集群信息修改页面。



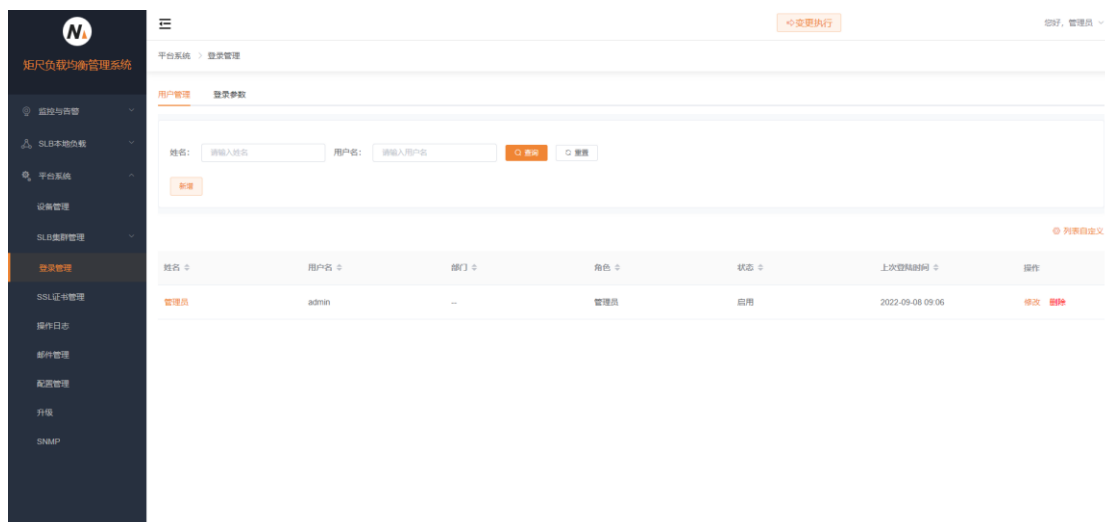
选择需要删除的 SLB 集群信息，然后操作栏的【删除】按钮，可对 SLB 集群信息进行删除操作。注：如果要删除的 SLB 集群下有服务器池、虚拟服务、路由、接口地址、网口聚合、VLAN、流量组信息，则无法删除成功。



4.7.3 登陆管理

系统中的新增的用户只能通过管理员在后台添加账号的方式，用户使用管理员预设的用户名、密码登录系统。

点击“平台系统→登陆管理”菜单，默认按照用户创建时间倒序展示用户信息列表。



点击【新增】可以新增用户。



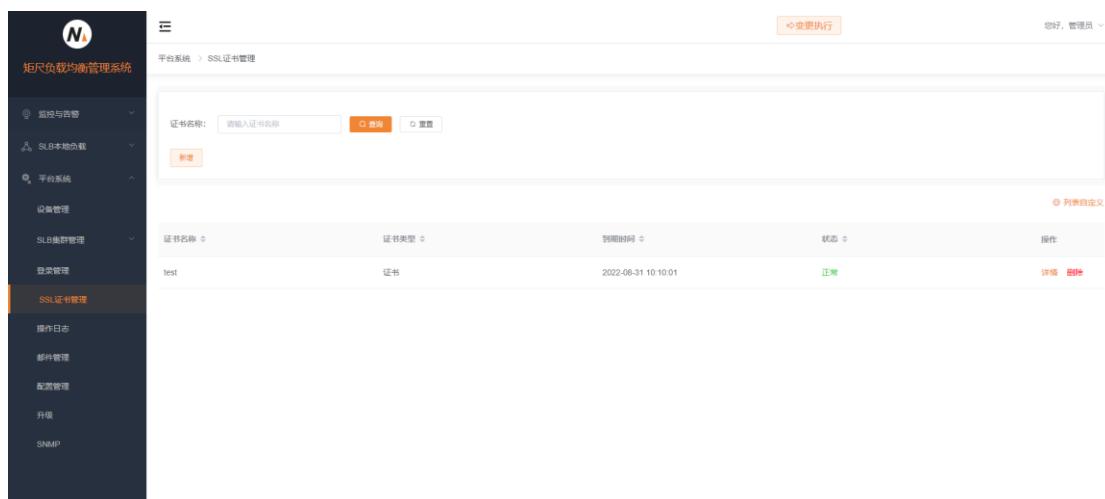
登录参数：在登录管理菜单中切换标签到“登录参数”，可配置登录会话超时时间。默认的登录会话超时时间为 24 小时，超过该时间没有发起请求将会退出登录，你也可以修改登录会话超时时间。



4.7.4 SSL 证书管理

SSL 证书管理实现对服务器证书的维护，在创建 TCP/SSL、HTTPS 协议的虚拟服务应用到此处维护的证书。

点击“平台系统→SSL 证书管理”菜单，默认按照证书创建时间倒序排列展示所有 SSL 证书信息列表。



● 查询区域：

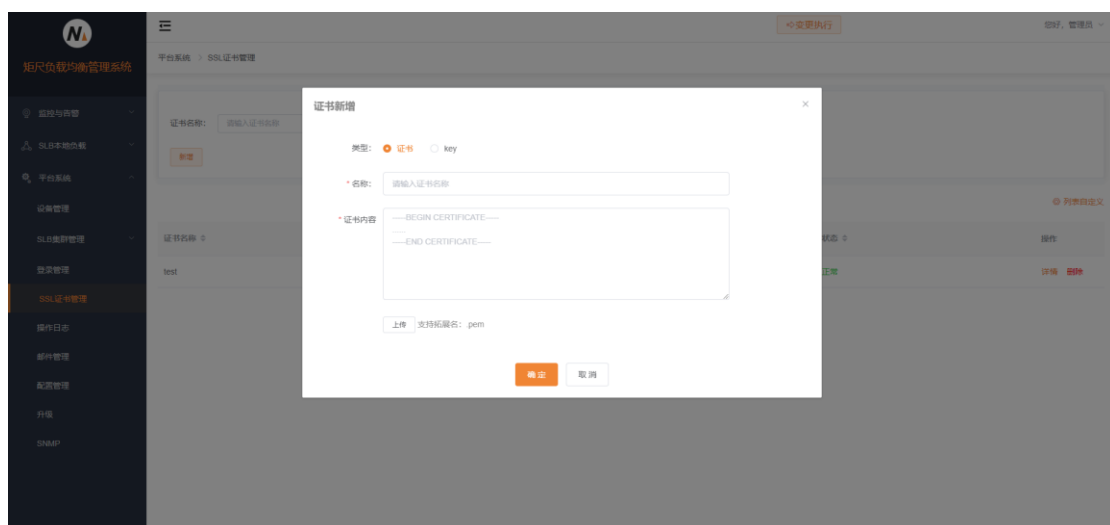
可通过“证书名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

在证书列表中，临近过期的证书会在到期时间前显示感叹号标记，黄色代表 30 天内过期，橙色代表 7 天内过期，红色代表已过期，将鼠标移到感叹号上面会显示具体过期时间。



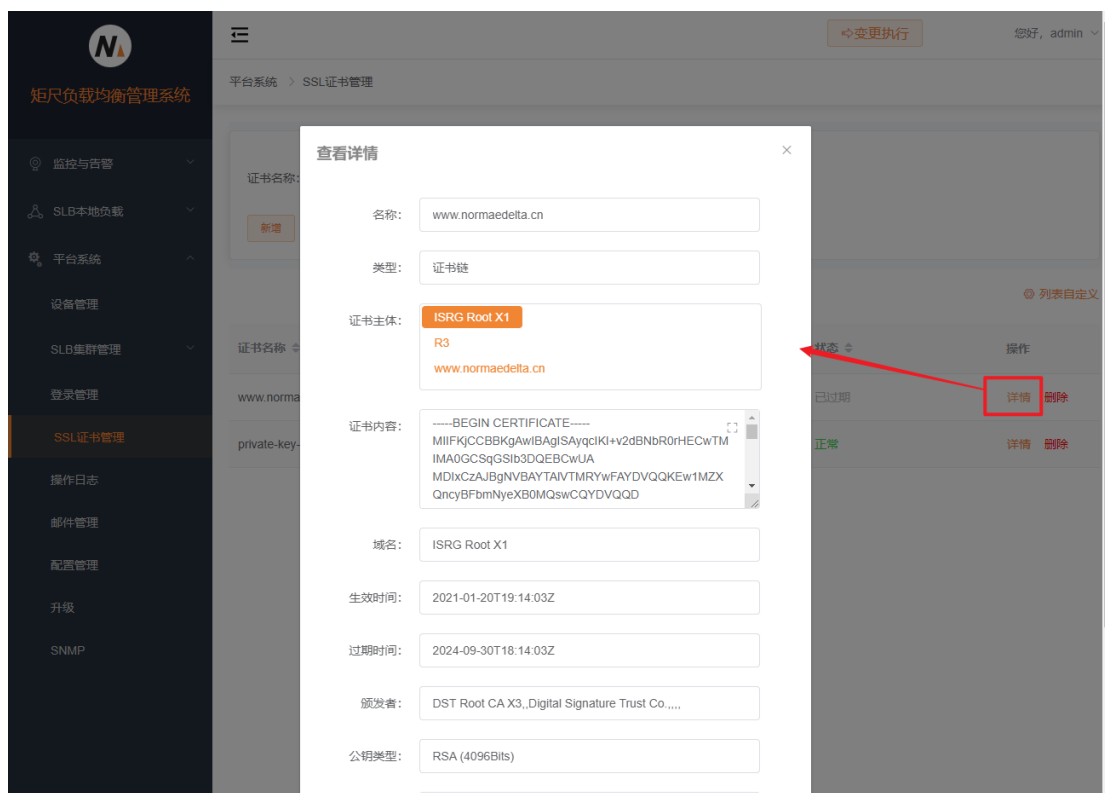
● 数据区域：

点击列表上方【新增】按钮，弹框打开 SSL 证书新增页面，可添加/配置新的证书/私钥信息。



注：证书名称、私钥支持手输（粘贴）、附件上传，域名、生效时间、到期时间、颁发者、签名算法等信息为证书上传成功后自动识别的。

点击列表中【详情】按钮，弹框打开证书/私钥详情页面。



选择需要删除的 SSL 证书信息，然后操作栏的【删除】按钮，可对 SSL 证书信息进行删除操作。

注：如果用户需要删除的策略已被虚拟服务进行关联，则无法删除成功

4.7.5 事件日志

事件日志记录了系统事件日志以及操作事件日志，可根据事件类型和时间范围查询事件日志，便于管理员进行查询、追责。

点击“平台系统→事件日志”菜单，默认按照操作时间倒序默认展示近三天的事件日志列表，如下所示：

平台系统 > 事件日志

事件日志: 所有事件 操作时间: 2023-06-26 11:23:17 至 2023-06-29 11:23:17 查询 重置

列表自定义

时间	资源类型	资源名称	事件类型	描述	详情
2023-06-29 11:05:55	虚拟服务	aaaa	修改	虚拟服务aaaa修改"HTTP压缩策略"	✓
2023-06-29 11:05:40	虚拟服务	aaaa	新增	虚拟服务aaaa新增	✓
2023-06-29 11:05:06	设备	normal-slb-device	修改	设备normal-slb-device修改"设备名称"	✓
2023-06-29 11:05:02	设备	normal-slb-device1	修改	设备normal-slb-device1修改"设备名称"	✓
2023-06-29 11:05:00	服务器池	dperf_http_pool	修改	服务器池dperf_http_pool修改	✓
2023-06-29 10:54:07	服务器池	dperf_http_pool	修改	服务器池dperf_http_pool修改"超时时间"	✓
2023-06-29 10:11:44	服务器池	dperf_spool	修改	服务器池dperf_spool修改"组中至少健康节点数量"、"优先级..."	✓
2023-06-29 09:37:23	服务器池	dperf_spool	修改	服务器池dperf_spool修改"优先级分组"、"组中至少健康节点..."	✓
2023-06-29 09:36:47	服务器池	dperf_spool	修改	服务器池dperf_spool修改"组中至少健康节点数量"、"优先级..."	✓
2023-06-29 09:36:06	服务器节点	10.1.9.4:18883	上线	服务器节点10.1.9.4:18883上线	●

共 9083 条 10条/页 < 1 2 3 4 5 6 ... 909 > 前往 1 页

可通过“事件日志”、“操作时间”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空。

系统事件：系统自动生成的事件，如：设备上下线，虚拟服务上下线，SSL证书过期等。

操作事件：由管理员操作行为产生的事件，如：新增虚拟服务，删除服务器池、修改配置、上传升级包等。

4.7.6 邮件管理

邮件服务器的配置主要实现当系统产生告警信息后，可通过邮件及时通知相关人员以及时处理。

点击“平台系统→邮件管理”菜单。在邮件服务器-未配置页面，点击【去配置】按钮，进入邮件服务器配置页面，邮件服务器配置所示。正确输入页面所有字段信息并点击【保存并验证】按钮，验证成功后返回邮件服务器配置查询页面。

平台系统 > 邮件管理

邮件服务器 邮件接收人

* 邮件服务器: smtp.163.com
仅支持smtp服务器

SSL: ☒
注: 非ssl端口默认25, ssl端口默认465

* 邮箱账号: 18539043730@163.com

* 邮箱密码: *****

* 端口: 465

修改

邮件接收人：

邮件管理菜单页切换标签到邮件接收人列表，点击下拉框可选择设备列表，点击新增按钮可添加邮件接收人。可配置项：接收人名称、接收邮件地址、接收事件类型。

新增邮件接收人

名称: 请输入名称

* 邮件地址: 请输入邮件地址

事件组: 请选择事件组

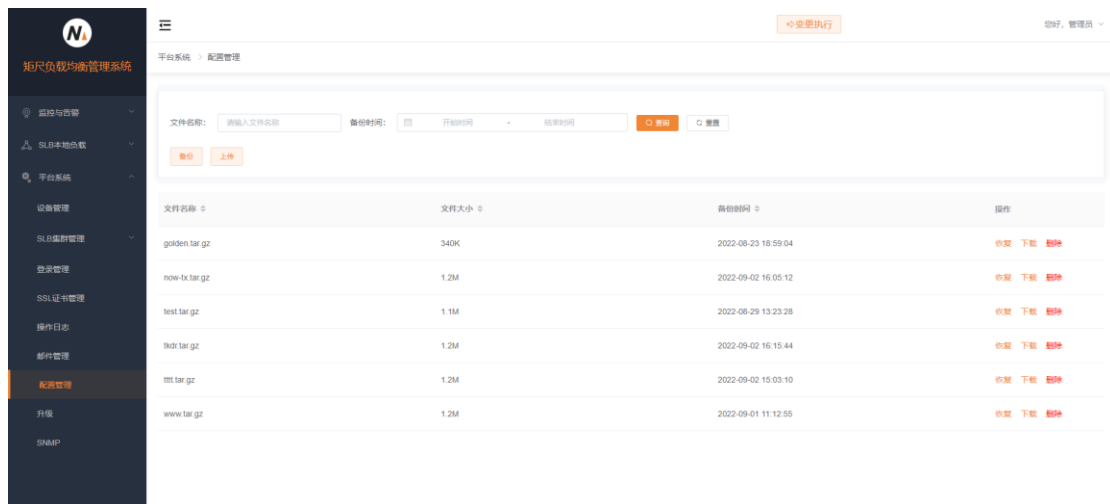
确定 取消

在操作一栏，修改和删除按钮可对该联系人进行修改和删除。点测试按钮会发送一封测试邮件到该联系人邮箱。

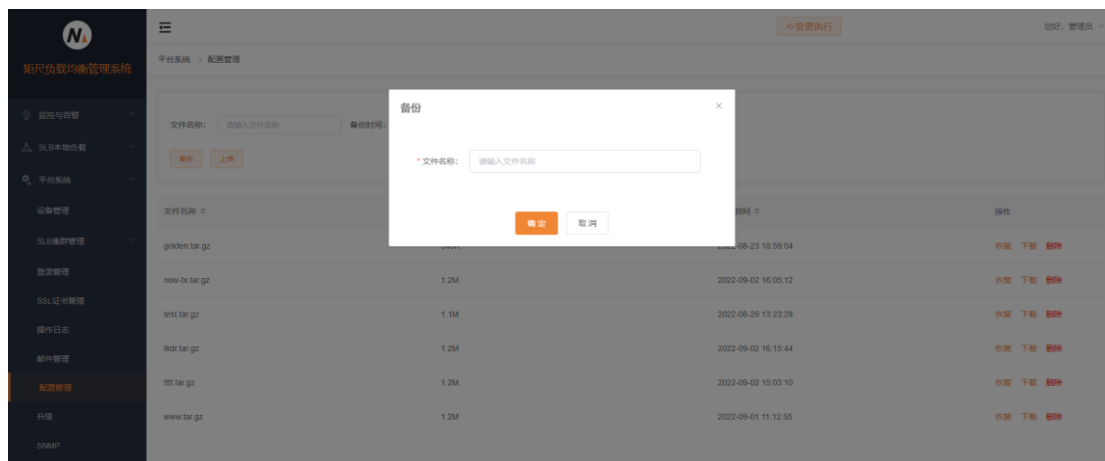


4.7.7 配置管理

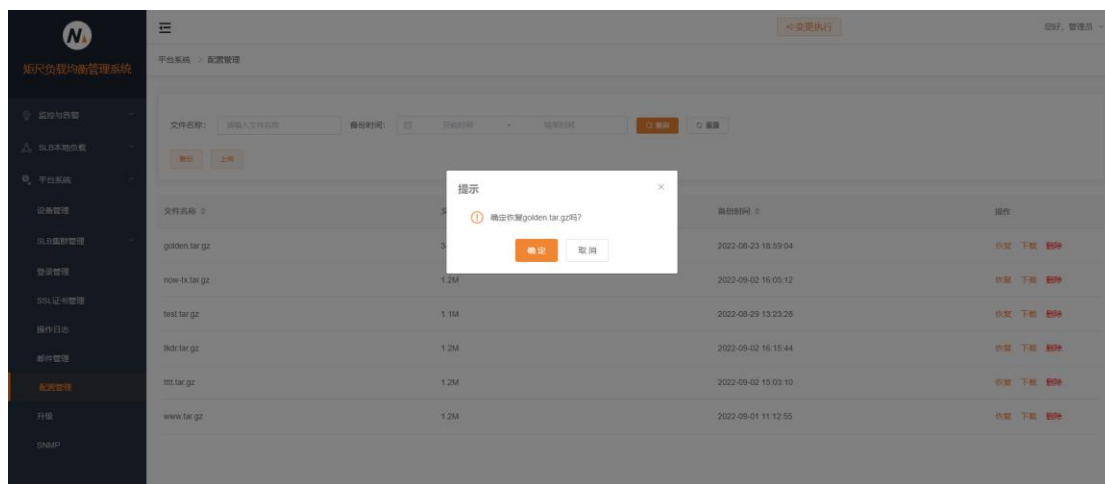
点击“平台系统→配置管理”菜单，列表显示当前平台中所有已备份的配置文件。



备份配置：点击列表上方的“备份”按钮，输入配置的备份文件名，即可备份配置（目前暂不包括网络配置）。备份配置完成后，可以在下方的列表中查看、下载或者删除。

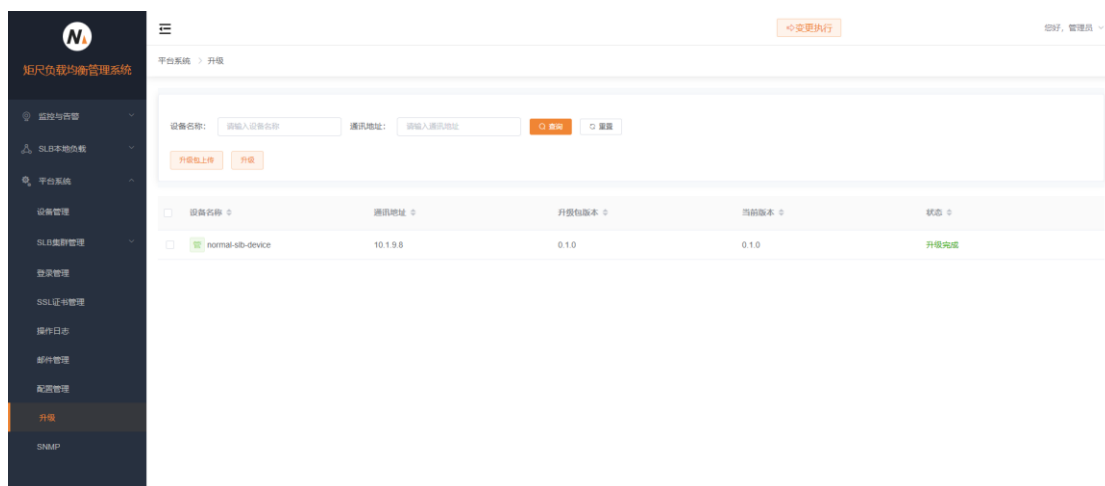


恢复配置：点击列表配置的“恢复”按钮，可以将当前系统的配置恢复为配置文件中的配置。



4.7.8 升级

点击“平台系统→升级”菜单，列表显示当前平台中所有设备当前版本和状态信息。



● 查询区域：

可通过“设备名称”、“管理地址”属性，进行条件模糊查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域：

点击列表上方【升级包上传】按钮，弹框打开升级包上传页面，支持上传格式为 .tar.gz 的附件。



升级包上传的过程中，所有设备的状态为：升级包传输中(此状态下需要在状态后显示传输进度条，到 100%后进度条消失同时状态变为：升级包就绪)；

升级包上传完成，所有设备的状态变为：升级包就绪；

点击【升级】按钮之前需勾选需要升级的设备，所选设备的状态变为：升级中，一个接一个升级，升级成功的设备状态变为：升级完成同时当前版本更新；升级失败的设备状态后显示【升级】按钮，点击后状态变为：升级中。

4.7.9 SNMP 配置

点击“平台系统→SNMP”菜单，顶部页签可切换 Agent 和 Traps。

● Agent:

(1) 配置信息：可配置 Contact Information（必填）、Machine Location（必填）、客户端白名单（必填）。如下图：

The screenshot shows the 'Agent' configuration page. The left sidebar contains the navigation menu with 'SNMP' selected. The main content area has tabs for 'Agent' and 'Traps'. Under the 'Agent' tab, there are three sections: '配置信息' (Configuration Information), 'Access(v1, v2c)', and 'Access(v3)'. The '配置信息' section contains three required fields: 'Contact Information' (with a dropdown menu), 'Machine Location' (with a text input), and '客户端白名单' (Client Whitelist) (with a range input). A '保存' (Save) button is at the bottom right of the form.

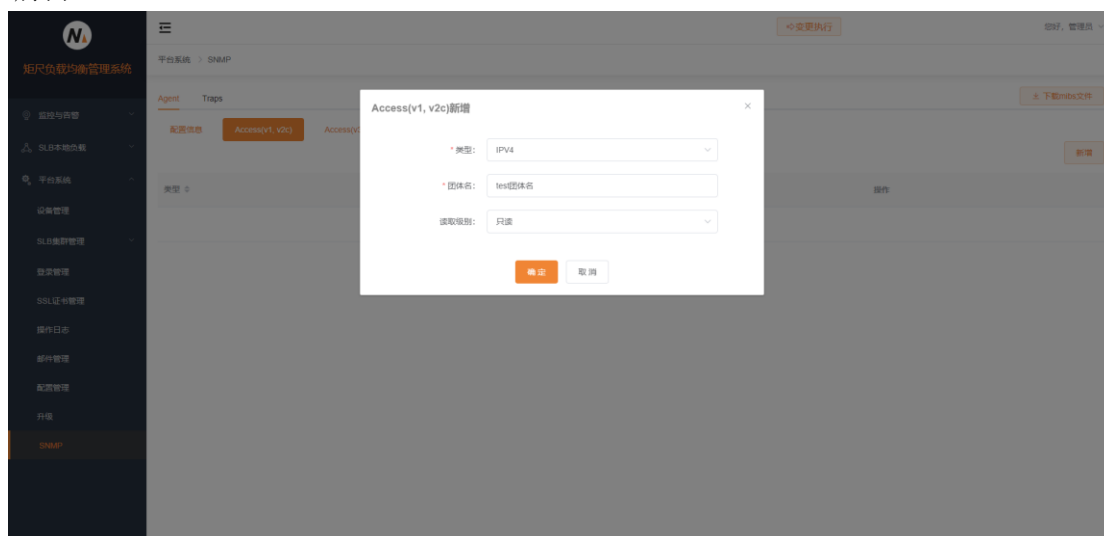
(2) Access (v1, v2c)：表格展示类型、团体名、读取级别。如下图：

The screenshot shows the 'Access(v1, v2c)' configuration page. The left sidebar is the same as the previous screenshot. The main content area has tabs for 'Agent' and 'Traps'. Under the 'Traps' tab, there are two sections: '配置信息' (Configuration Information) and 'Access(v3)'. The '配置信息' section contains a table with the following data:

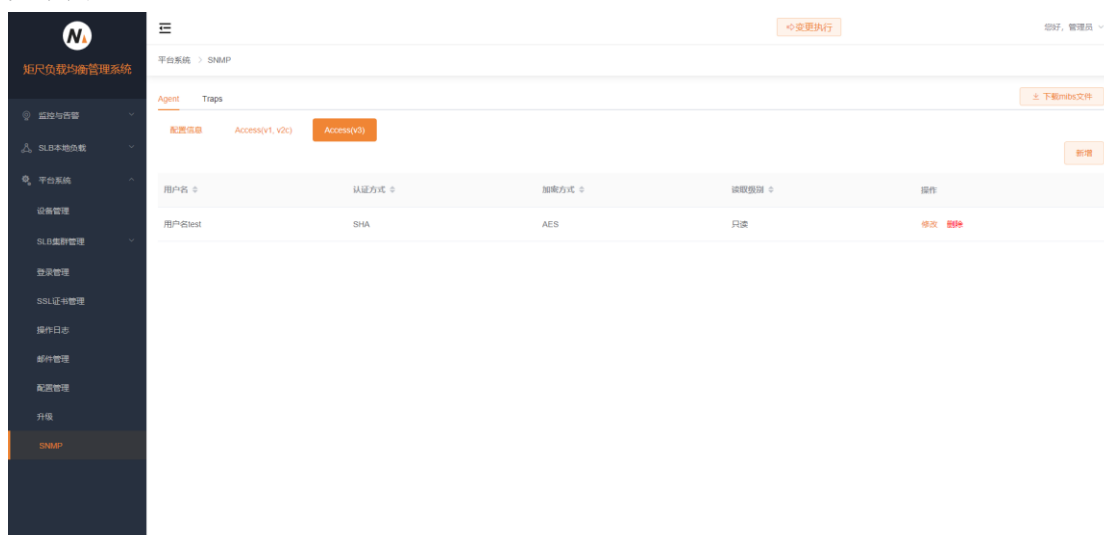
类型	团体名	读取级别	操作
IPv4	test团体名	只读	修改 删除

A '新增' (Add) button is located at the bottom right of the table.

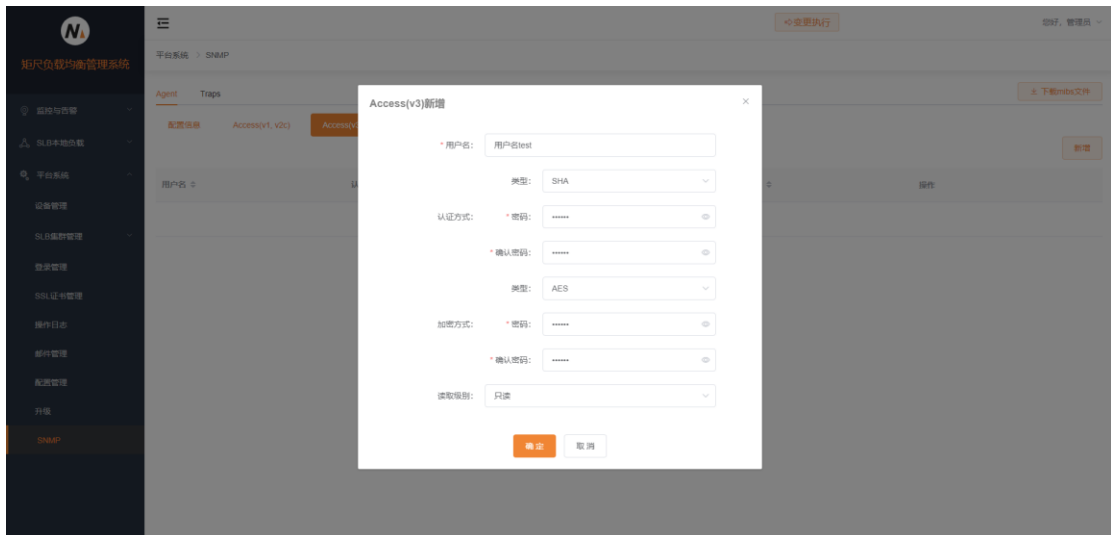
可点击按钮【新增】或【修改】，打开对话框可进行 Access（v1，v2c）编辑：



（3）Access（V3）：表格展示用户名、认证方式、加密方式、读取级别。如下图：

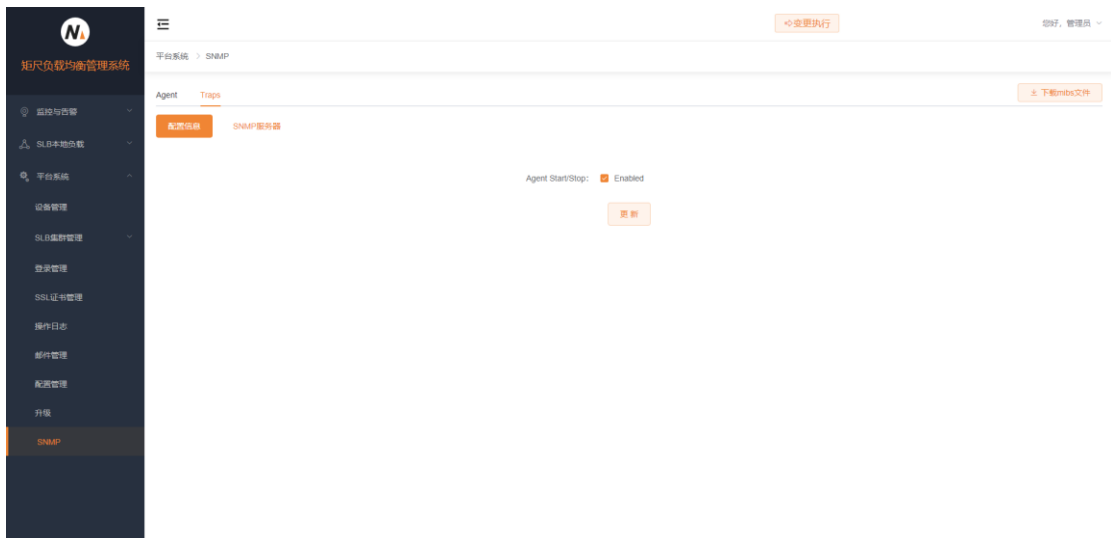


可点击按钮【新增】或【修改】，打开对话框可进行 Access（v3）编辑：

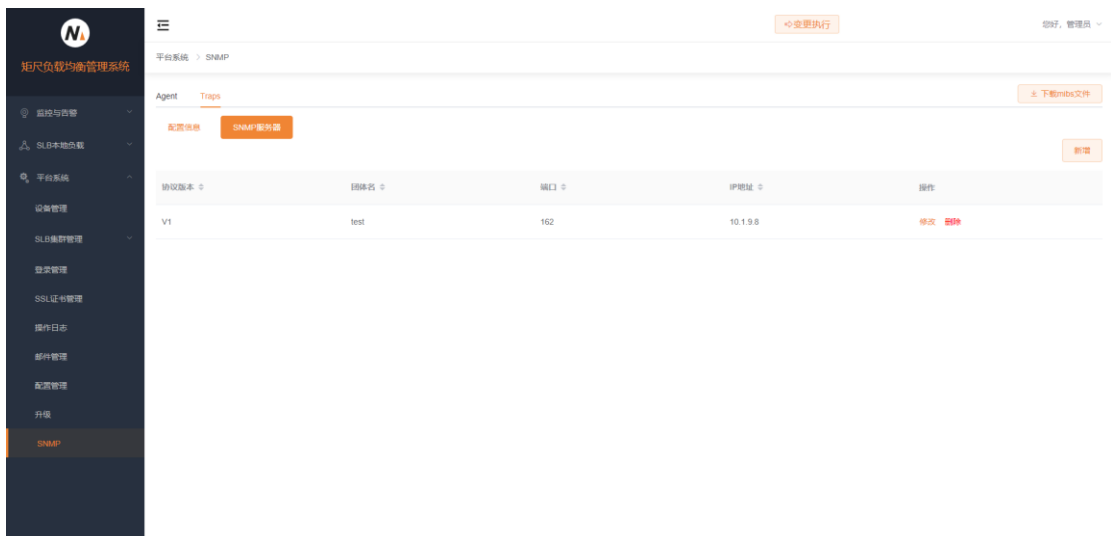


● Traps:

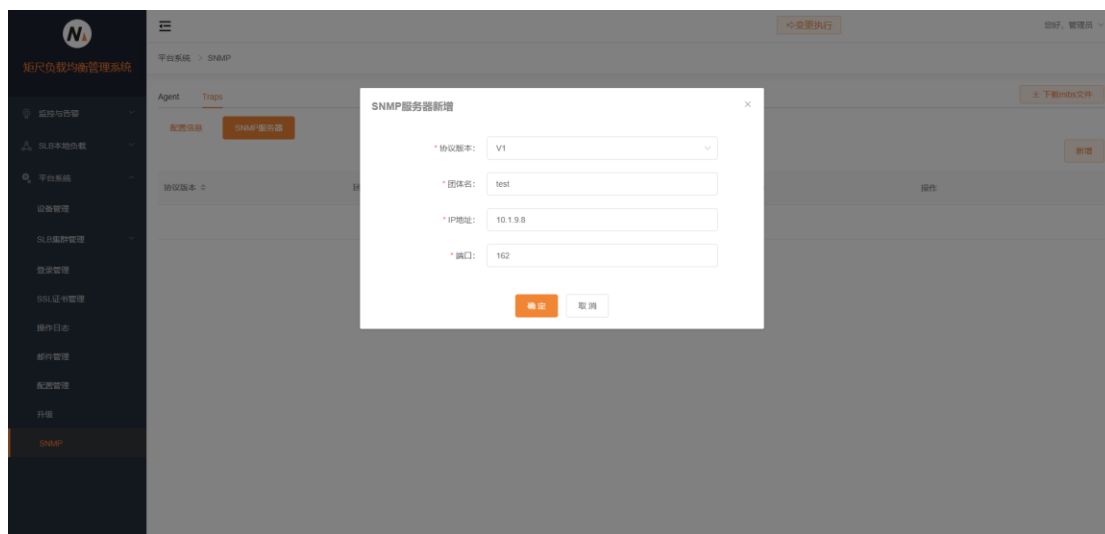
(1) 配置信息：可配置开关 Agent Start/Stop。如下图：



(2) SNMP 服务器：表格展示用户名、认证方式、加密方式、读取级别。如下图：

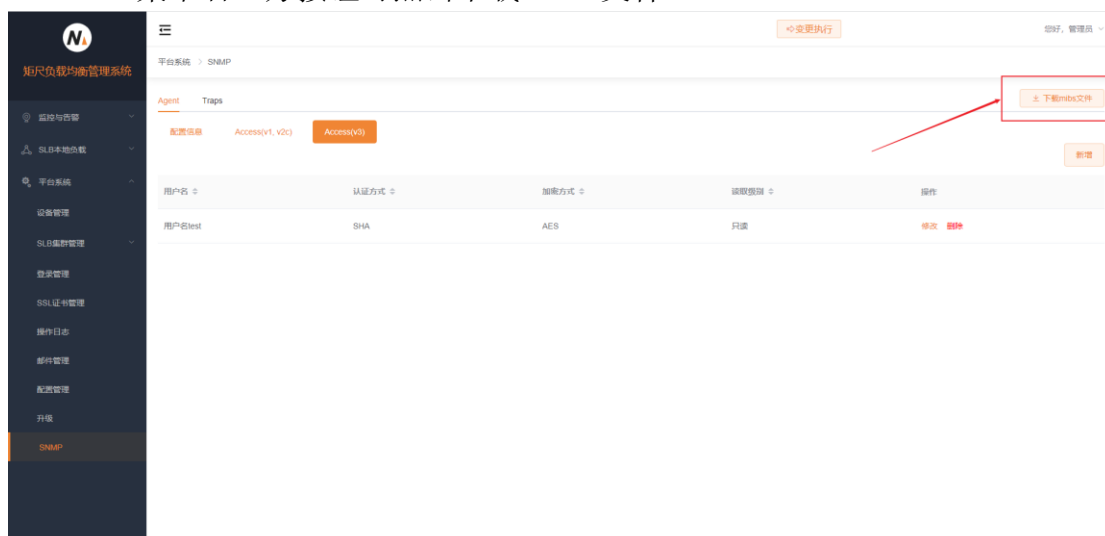


可点击按钮【新增】或【修改】，打开对话框可进行 SNMP 服务器编辑：



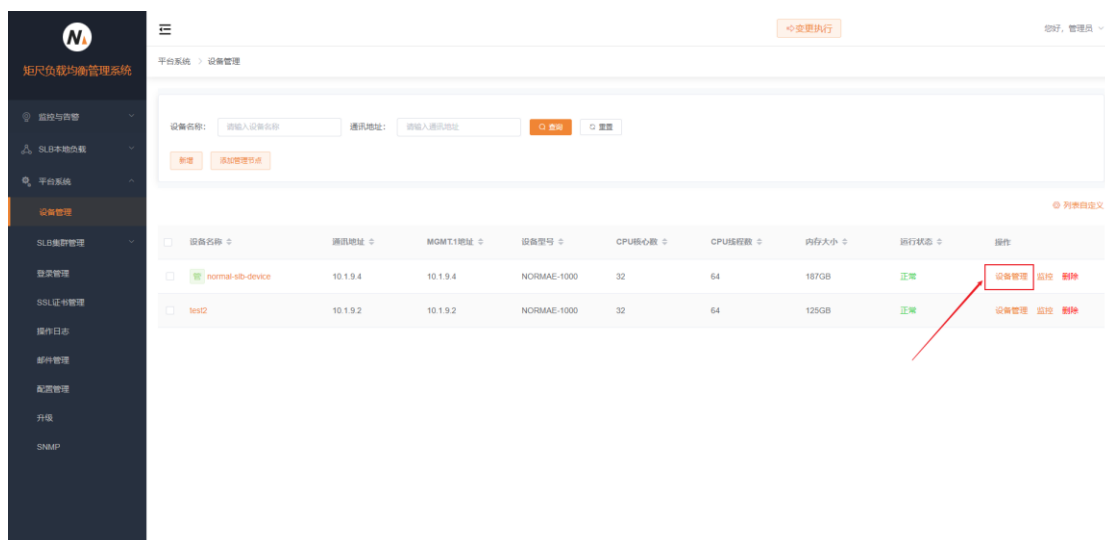
● 下载 mibs 文件

SNMP 菜单右上方按钮可点击下载 mibs 文件。



4.8 单台设备页面

在“平台设备→设备管理”菜单，设备列表中点击【设备管理】按钮，可进入这台设备管理页面。



4.8.1 设备管理

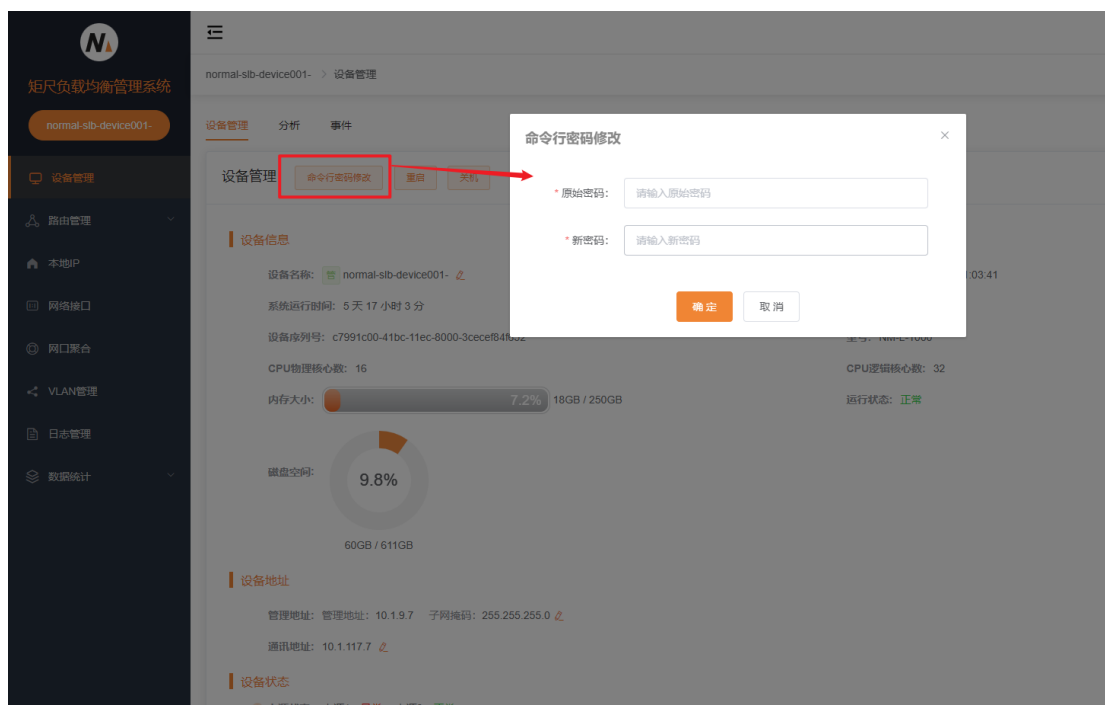
设备管理菜单分 3 个模块：设备管理、分析、事件。

➤ 设备管理

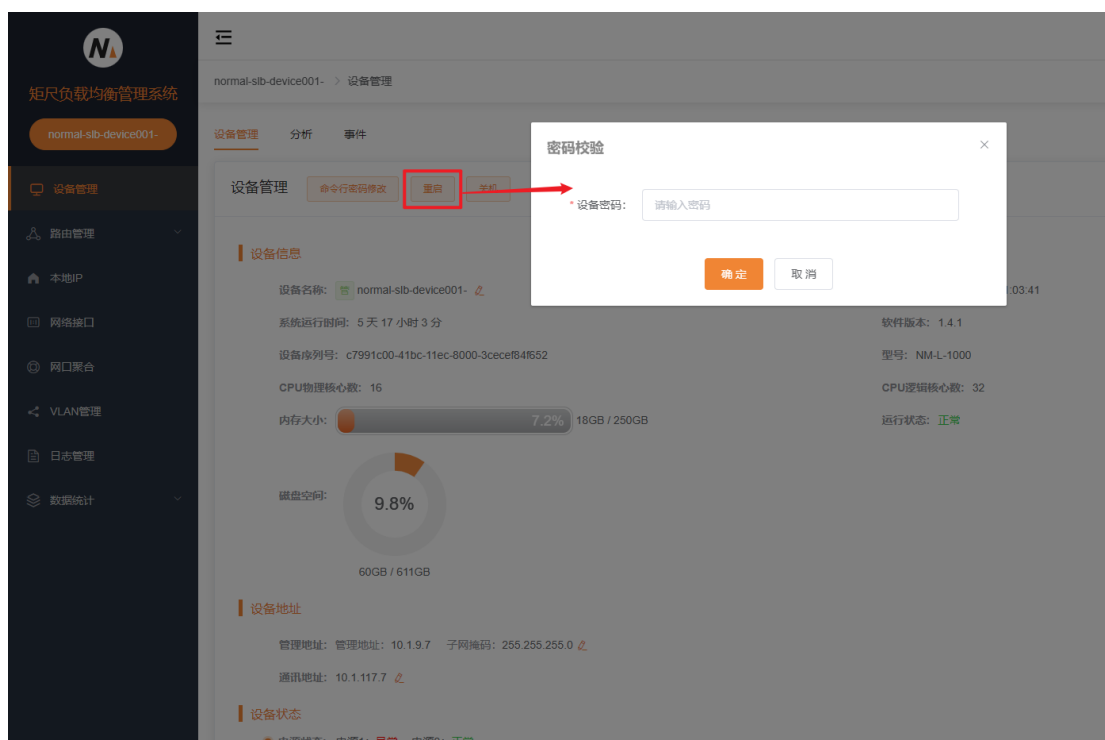
设备管理标签下内容分为：设备信息、设备地址、设备状态。可查看设备信息和设备状态，并可做一些修改操作。

设备管理头部按钮：

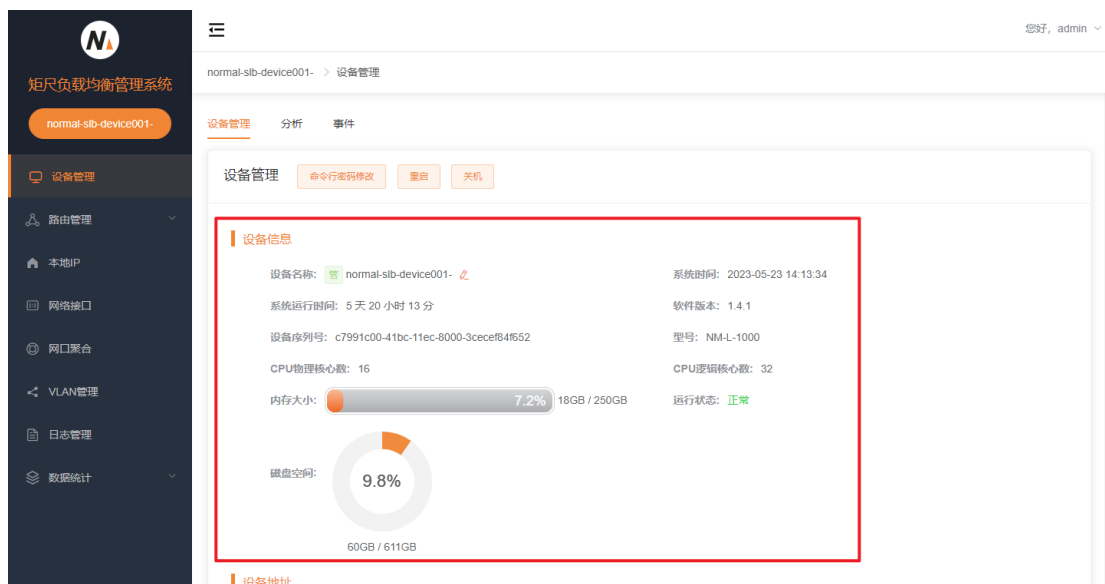
修改命令行密码：



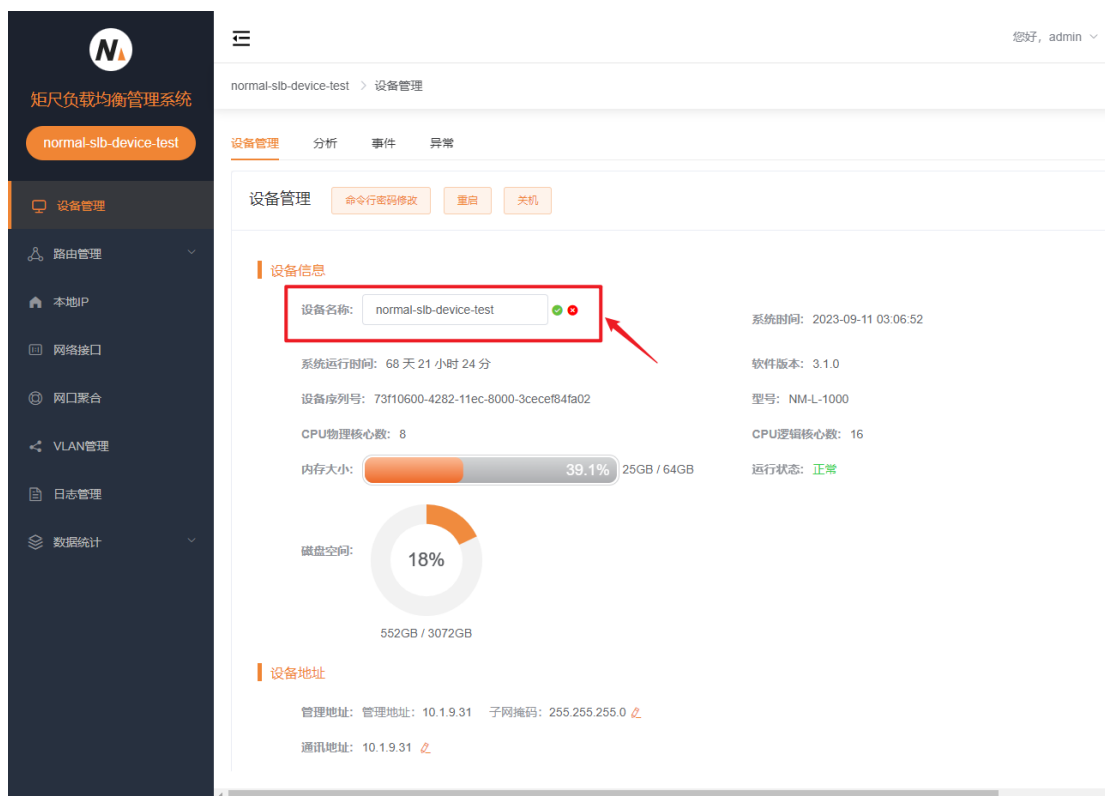
重启/关机：需校验设备密码后才能执行。



设备信息：包括设备名称、系统时间、系统运行时间、软件版本、设备序列号、型号、CPU 物理核心数、CPU 逻辑核心数、内存大小、运行状态、磁盘空间。

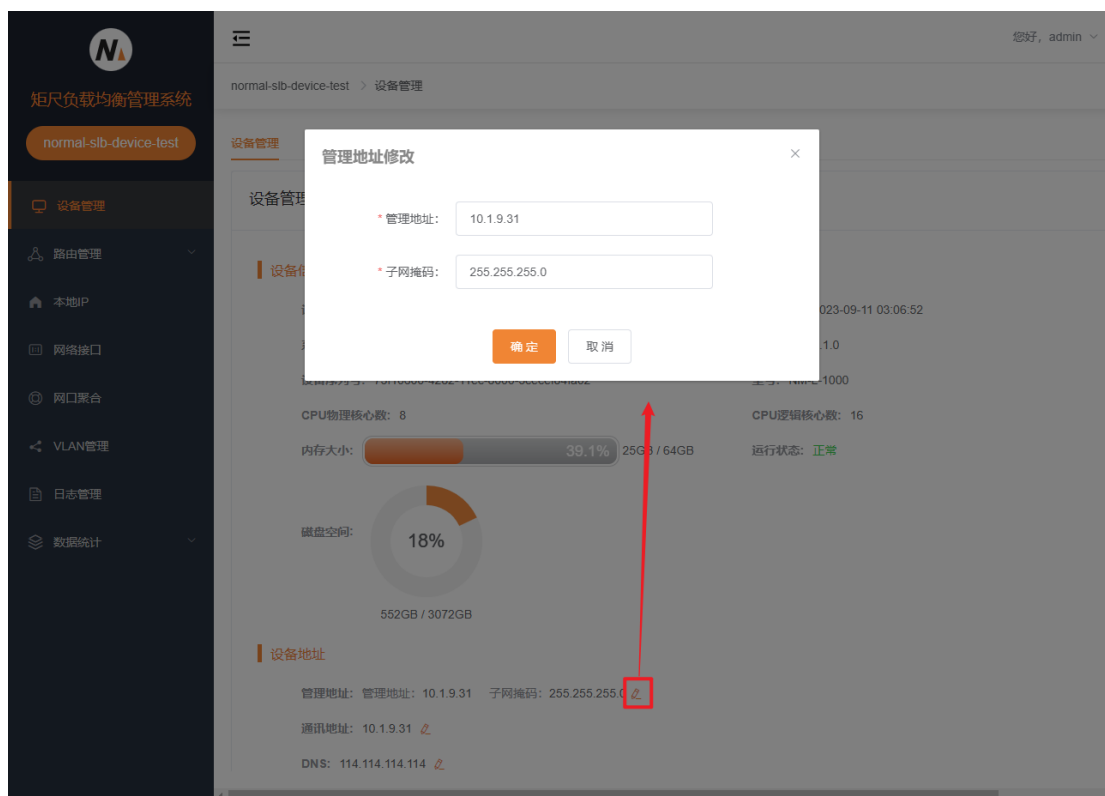


修改设备名称：



➤ 设备地址

修改管理地址:



修改通讯地址：

normal-slb-device-test > 设备管理

设备管理 分析 事件 异常

设备管理 命令行密码修改 重启 关机

设备信息

设备名称: normal-slb-device-test 系统时间: 2023-09-11 03:06:52

系统运行时间: 68 天 21 小时 24 分 软件版本: 3.1.0

设备序列号: 73f10600-4282-11ec-8000-3cecef84fa02 型号: NM-L-1000

CPU物理核心数: 8 CPU逻辑核心数: 16

内存大小: 39.1% 25GB / 64GB 运行状态: 正常

设备地址

管理地址: 10.1.9.31 子网掩码: 255.255.255.0

通讯地址: 10.1.9.31

DNS: 114.114.114.114

修改设备 DNS：

normal-slb-device-test > 设备管理

设备管理 分析 事件 异常

系统运行时间: 68 天 21 小时 24 分 软件版本: 3.1.0

设备序列号: 73f10600-4282-11ec-8000-3cecef84fa02 型号: NM-L-1000

CPU物理核心数: 8 CPU逻辑核心数: 16

内存大小: 39.1% 25GB / 64GB 运行状态: 正常

设备地址

管理地址: 10.1.9.31 子网掩码: 255.255.255.0

通讯地址: 10.1.9.31

DNS: 114.114.114.114

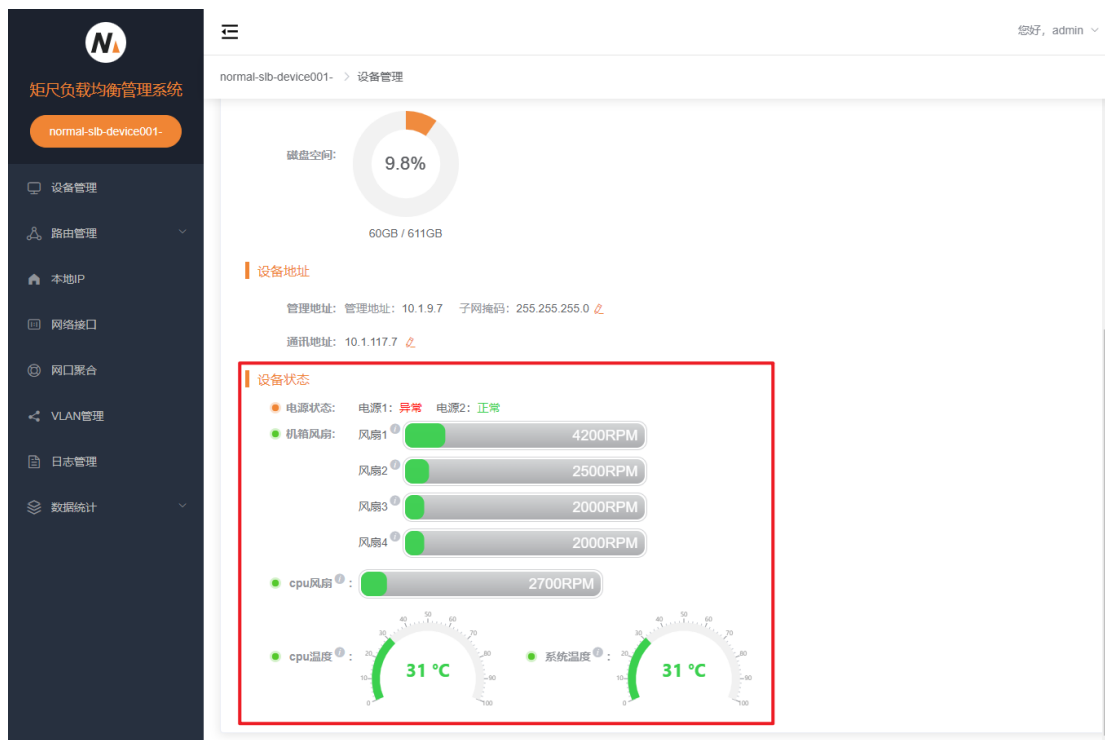
设备状态

电源状态: 电源1: 正常 电源2: 异常

机箱风扇: 风扇1: 4100RPM 风扇2: 2500RPM

设备状态（全部正常为绿色，部分正常为橙色，全部异常为红色）：

1. 电源状态（正常和异常两种）；
2. 机箱风扇状态（进度条绿色表示正常 200-20000PRM、红色表示风扇转速过高>20000PRM、蓝色表示转速过低<200PRM）；
3. cpu 风扇状态（同机箱风扇）；
4. cpu 温度（绿色表示正常<96℃、红色表示温度过高>96℃）；
5. 系统温度（绿色表示正常<85℃、红色表示温度过高>85℃）。



➤ 分析



交互功能参见“4.5 监控与告警”章节。

B 区展示该设备对应时间段内“吞吐量”（客户端）、“CPU 利用率”、“接口吞吐量”、“虚拟服务吞吐量”（客户端和服务端总和）。

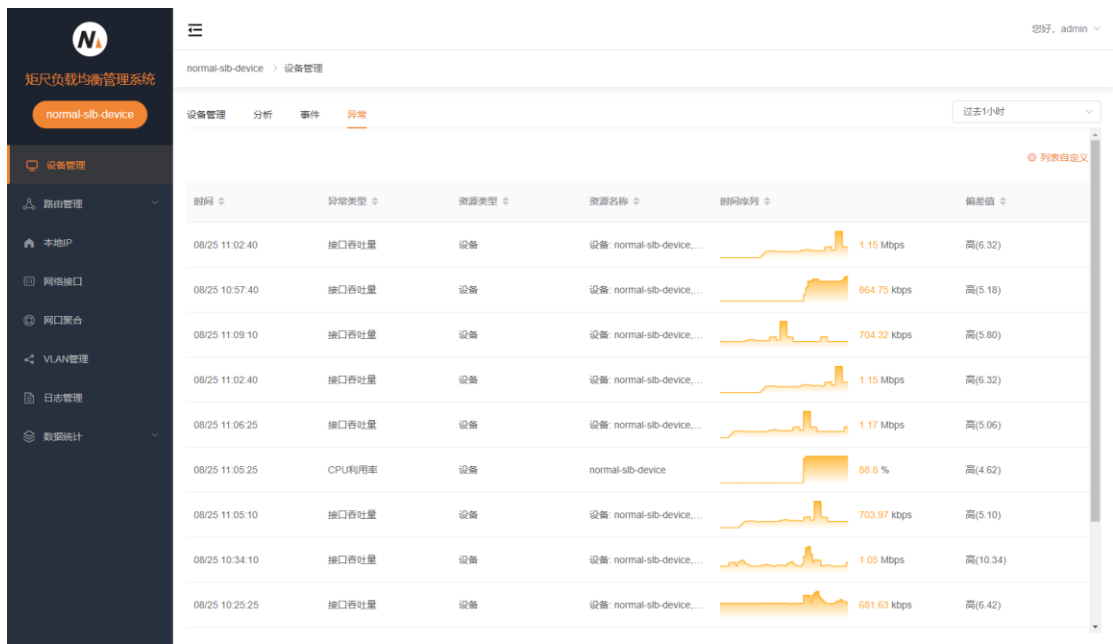
➤ 事件

详见“4.5 监控与告警”章节的“事件”介绍。



➤ 异常

详见“4.5 监控与告警”章节的“异常”介绍。



4.8.2 路由管理

路由管理菜单可查看路由表、静态路由和 OSPF。

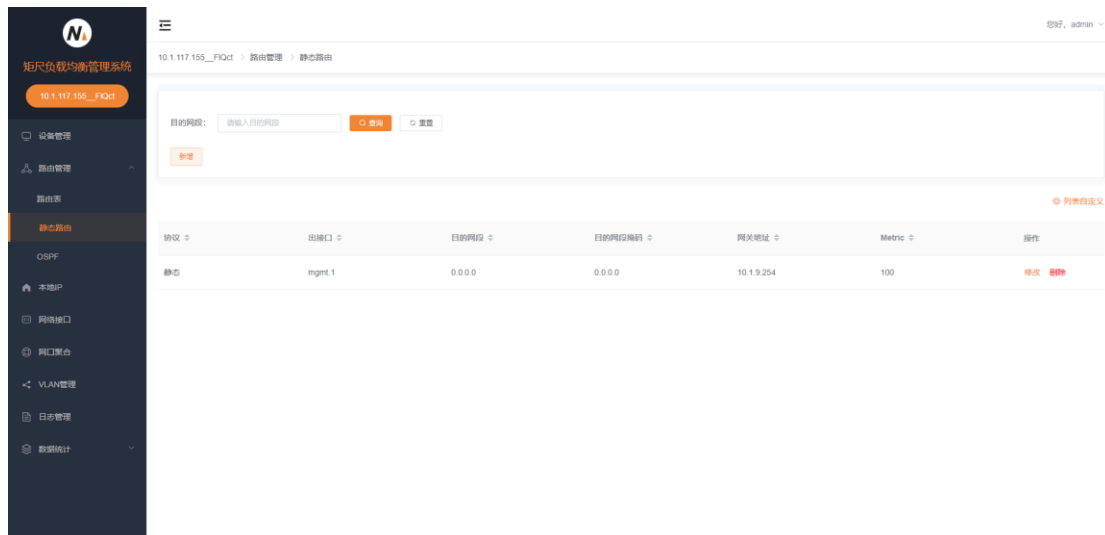
4.8.2.1 路由表

展开“路由管理”菜单，点击“路由表”子菜单，默认展示当前设备下按照用户创建时间倒序排列的路由信息列表。

协议	出接口	目的网段	目的网段掩码	网关地址	Metric
静态	mgmt.1	0.0.0.0	0.0.0.0	10.1.9.254	100
直连	mgmt.1	10.1.9.0	255.255.255.0	0.0.0.0	100
直连	117	10.1.117.0	255.255.255.0	0.0.0.0	100
直连	117	10.1.117.0	255.255.255.0	0.0.0.0	100
直连	117	000:	000:	::	256
静态	mgmt.1	0.0.0.0	0.0.0.0	10.1.9.254	100

4.8.2.2 静态路由

展开“路由管理”菜单，点击“静态路由”二级菜单即可查看自己创建过的静态路由。

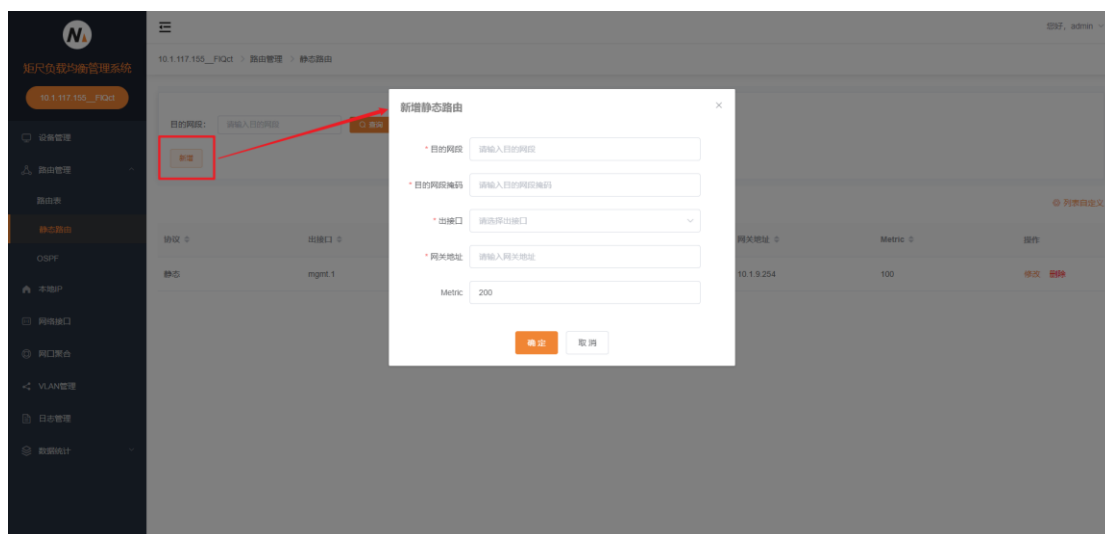


- 查询区域：

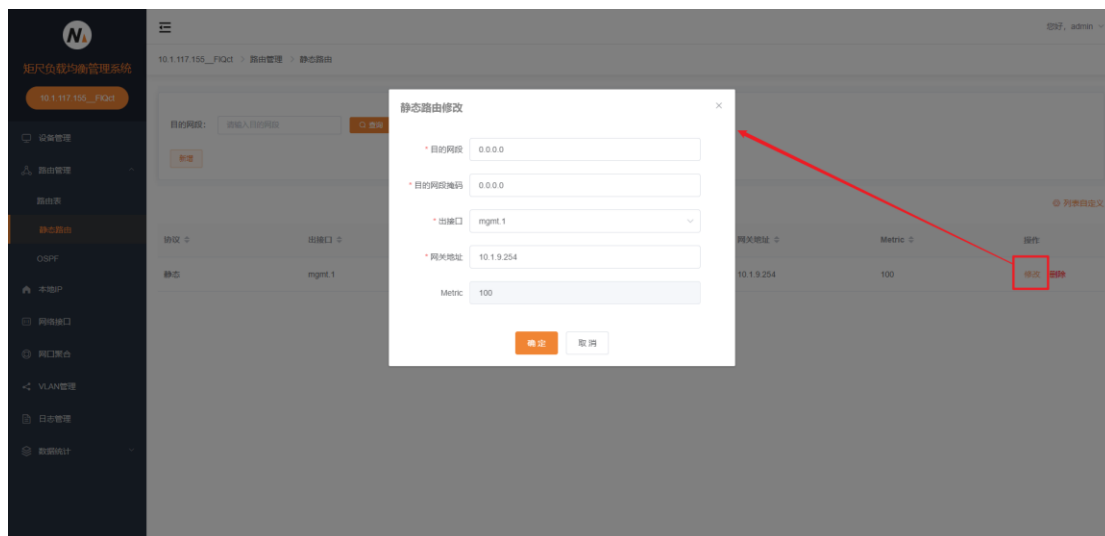
可通过“目的网段”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

- 数据区域：

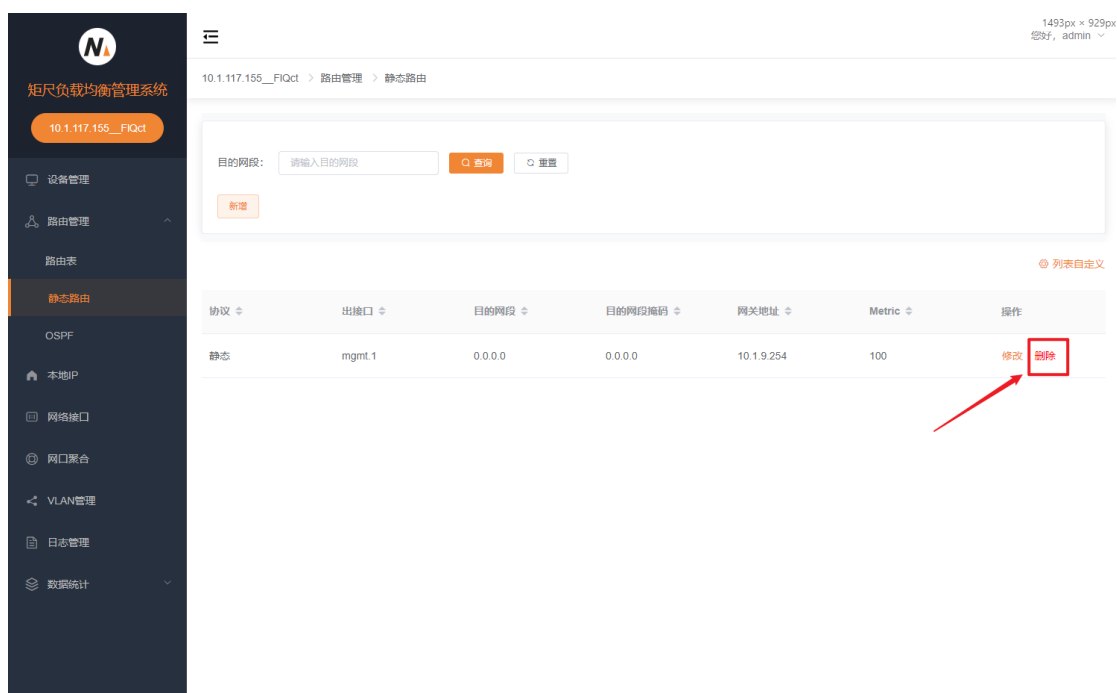
点击列表上方【新增】按钮，弹框打开路由新增对话框，可添加/配置新的路由信息。



选择需要修改的路由信息，点击此用户所在行操作栏的【修改】按钮，弹框打开路由信息修改对话框。



选择需要删除的路由信息，然后操作栏的【删除】按钮，可对路由信息进行删除操作。



4.8.2.3 OSPF

展开“路由管理”菜单，点击“OSPF”二级菜单，可进入动态路由配置界面。

进入动态路由菜单后，头部可切换“全局配置”和“接口配置”。

矩尺负载均衡管理系统

10.1.117.155_FIQct

设备管理

路由管理

路由表

静态路由

OSPF

本地IP

网络接口

网口聚合

VLAN管理

日志管理

数据统计

您好, 管理员

10.1.117.155_FIQct > 路由管理 > OSPF

全局配置 接口配置

启用状态: ☒

* 路由ID:

* 区域ID:

* 运行网段:

10.1.117.0/24

每行可配置一个IP或地址段，行之间用换行分割。
示例: 10.10.1.2/32

分发默认路由: ☐

分发静态路由: ☐

提交

矩尺负载均衡管理系统

10.1.117.155_FIQct

设备管理

路由管理

路由表

静态路由

OSPF

本地IP

网络接口

网口聚合

VLAN管理

日志管理

数据统计

您好, 管理员

10.1.117.155_FIQct > 路由管理 > OSPF

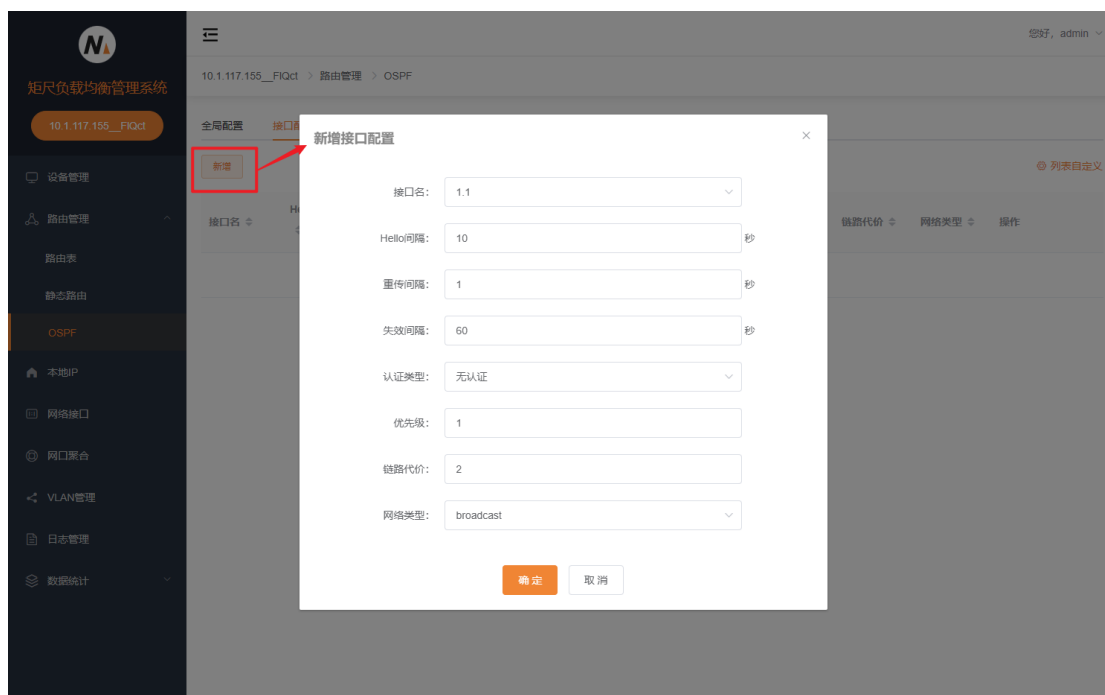
全局配置 接口配置

新增

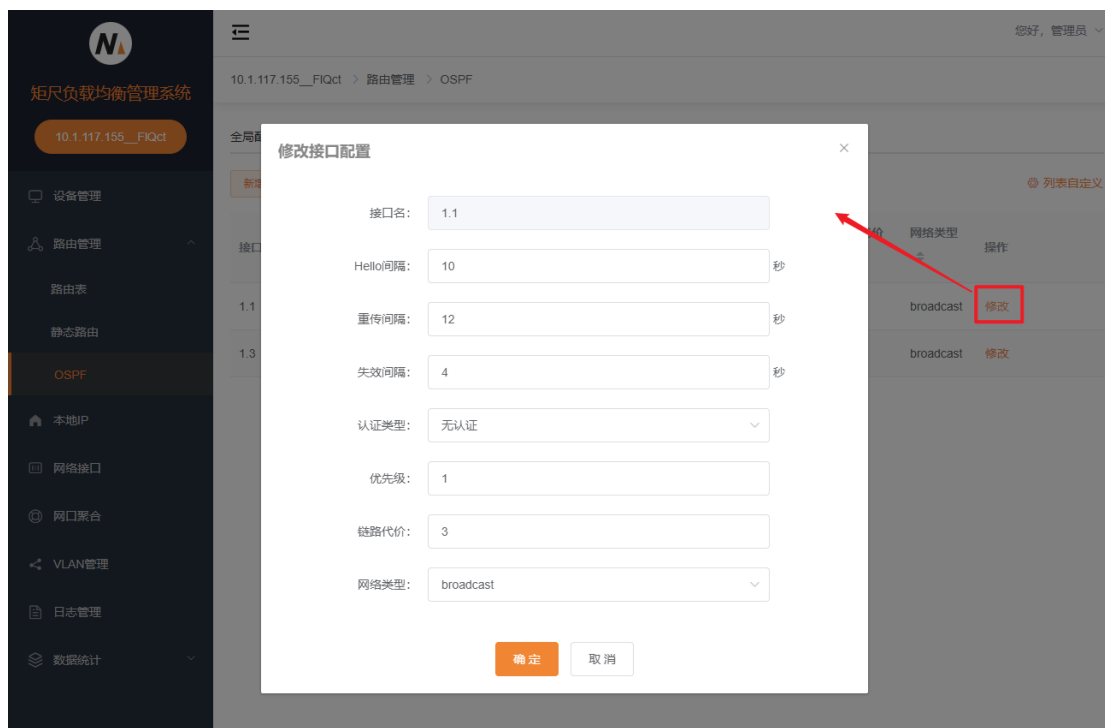
列表自定义

接口名	Hello间隔	重传间隔	失效间隔	认证类型	认证key	认证字符	优先级	链路代价	网络类型	操作
1.1	10秒	12秒	4秒	无认证	--	--	1	3	broadcast	修改
1.3	5秒	4秒	3秒	MD5 认证	123	dasd	1	2	broadcast	修改

新增接口配置：

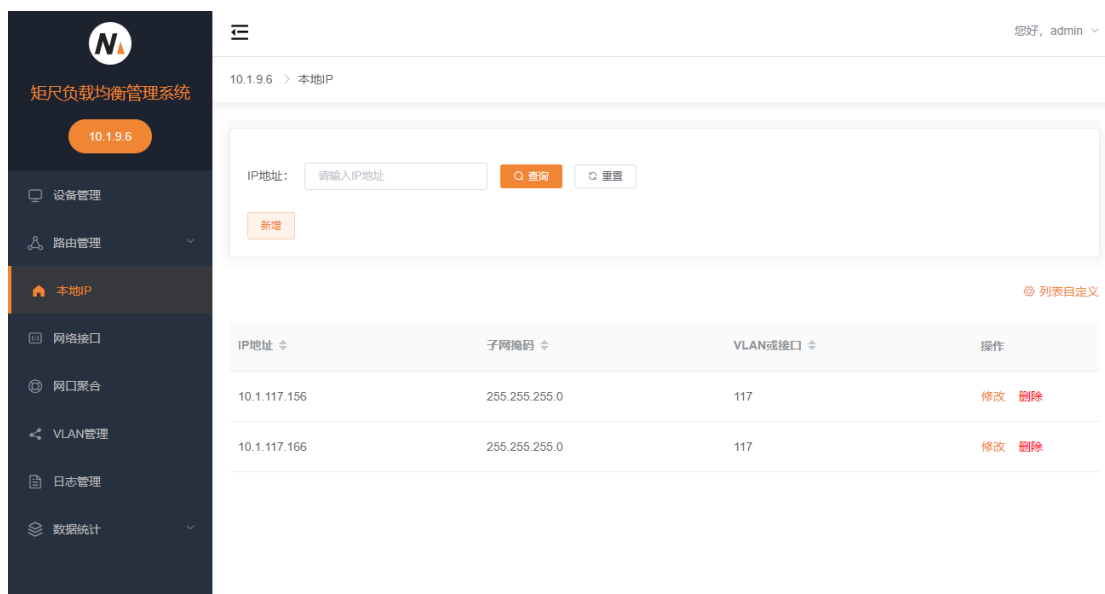


修改接口配置：



4.8.3 本地 IP

点击“本地 IP”菜单，默认展示当前设备下按照用户创建时间倒序排列的本地 IP 地址信息列表。

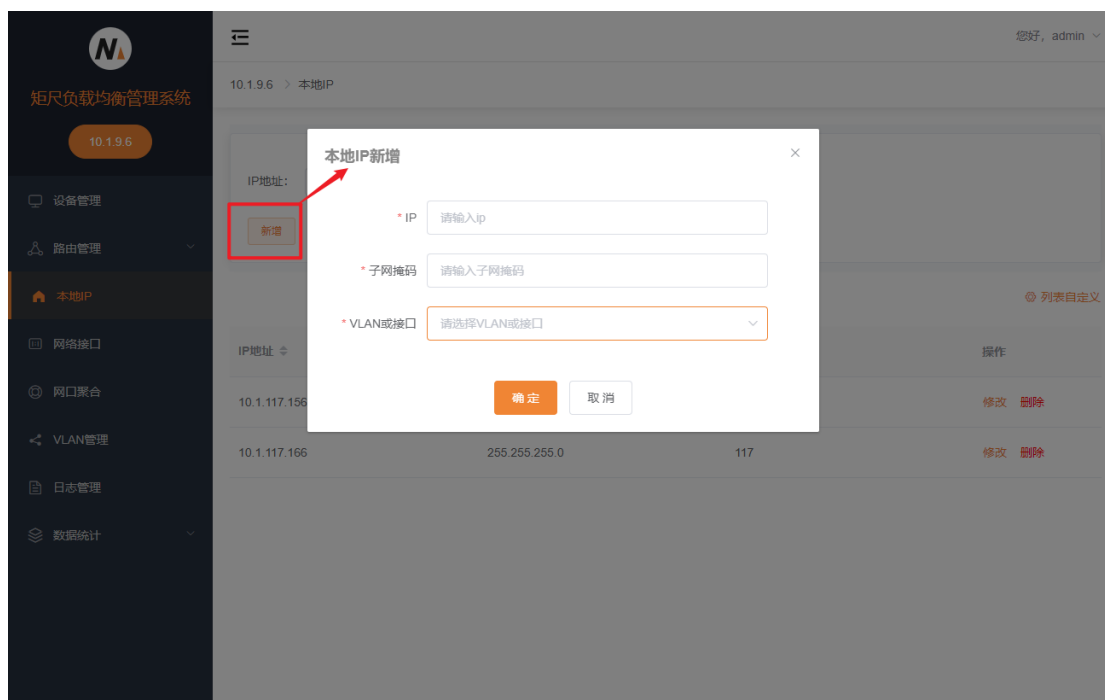


● 查询区域:

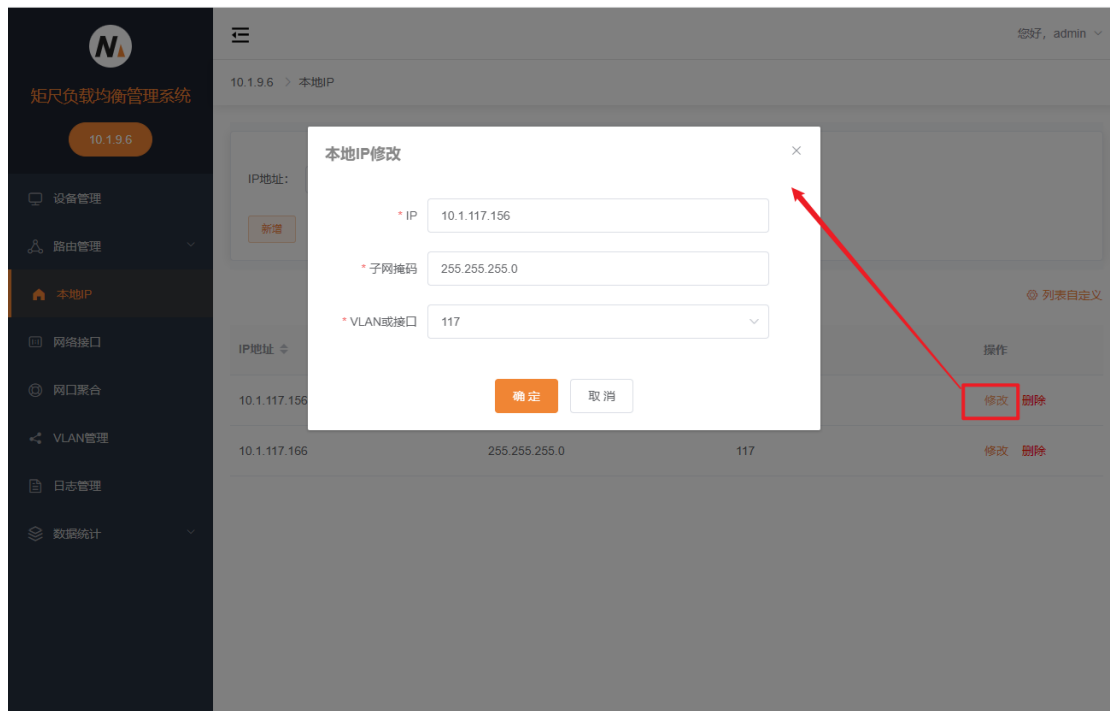
可通过“IP 地址”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域:

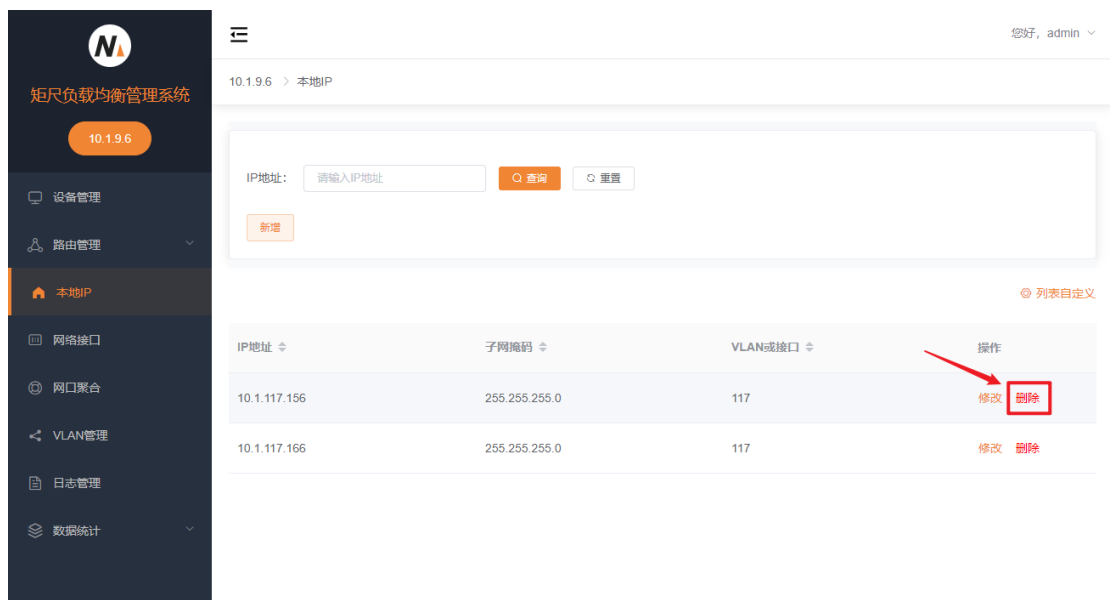
点击列表上方【新增】按钮，弹框打开本地 IP 地址新增页面，可添加/配置新的接口地址信息。IP 地址支持 IPv6 协议，可选配置在 VLAN 或接口上。



选择需要修改的接口地址信息，点击此用户所在行操作栏的【修改】按钮，弹框打开接口地址信息修改页面。



选择需要删除的接口地址信息，然后操作栏的【删除】按钮，可对接口地址信息进行删除操作。



4.8.4 网络接口

网络接口展示当前已配置的接口列表，列表展示内容包括接口名称、MAC地址、协商网速、网口类型、划分 VLAN 数量、网口聚合名称、MTU、状态。

点击“网络接口”菜单，默认打开接口信息标签，展示系统当前已配置的网络接口基础信息列表。可点击标签切换显示【接口基础信息】和【接口统计信息】。

矩尺负载均衡管理系统 10.1.9.6

设备管理 路由管理 本地IP 网络接口 网口聚合 VLAN管理 日志管理 数据统计

10.1.9.6 > 网络接口

您好, admin

接口名称: 查询 重置

接口基础信息 接口统计信息

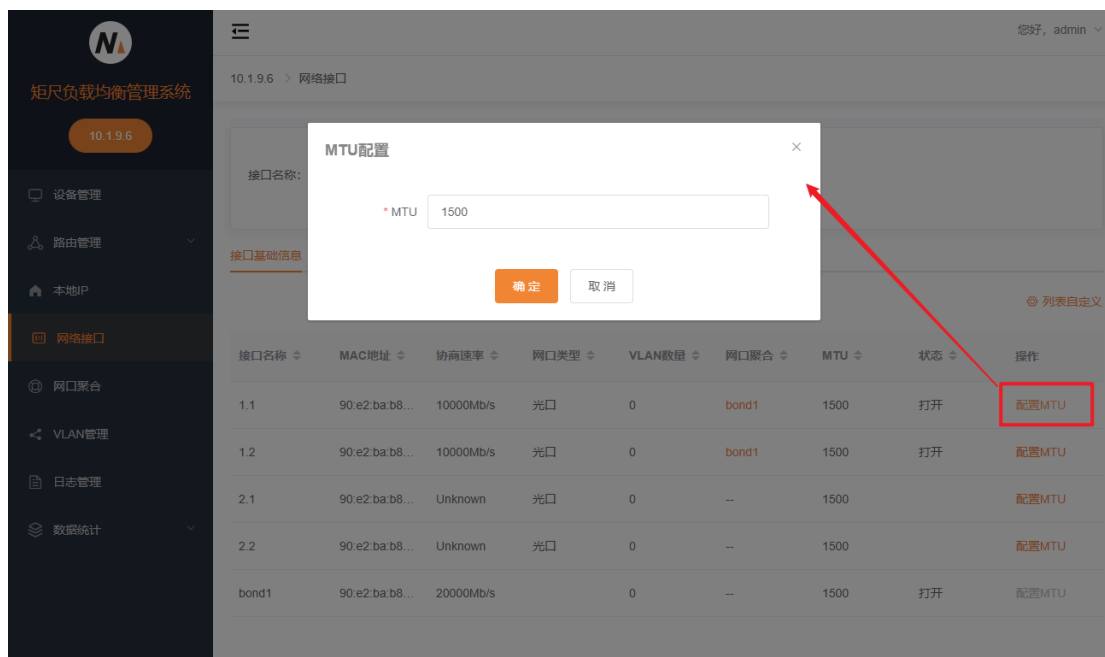
列表自定义

接口名称	MAC地址	协商速率	网口类型	VLAN数量	网口聚合	MTU	状态	操作
1.1	90:e2:ba:b8...	10000Mb/s	光口	0	bond1	1500	打开	配置MTU
1.2	90:e2:ba:b8...	10000Mb/s	光口	0	bond1	1500	打开	配置MTU
2.1	90:e2:ba:b8...	Unknown	光口	0	--	1500		配置MTU
2.2	90:e2:ba:b8...	Unknown	光口	0	--	1500		配置MTU
bond1	90:e2:ba:b8...	20000Mb/s		0	--	1500	打开	配置MTU

查询区域:

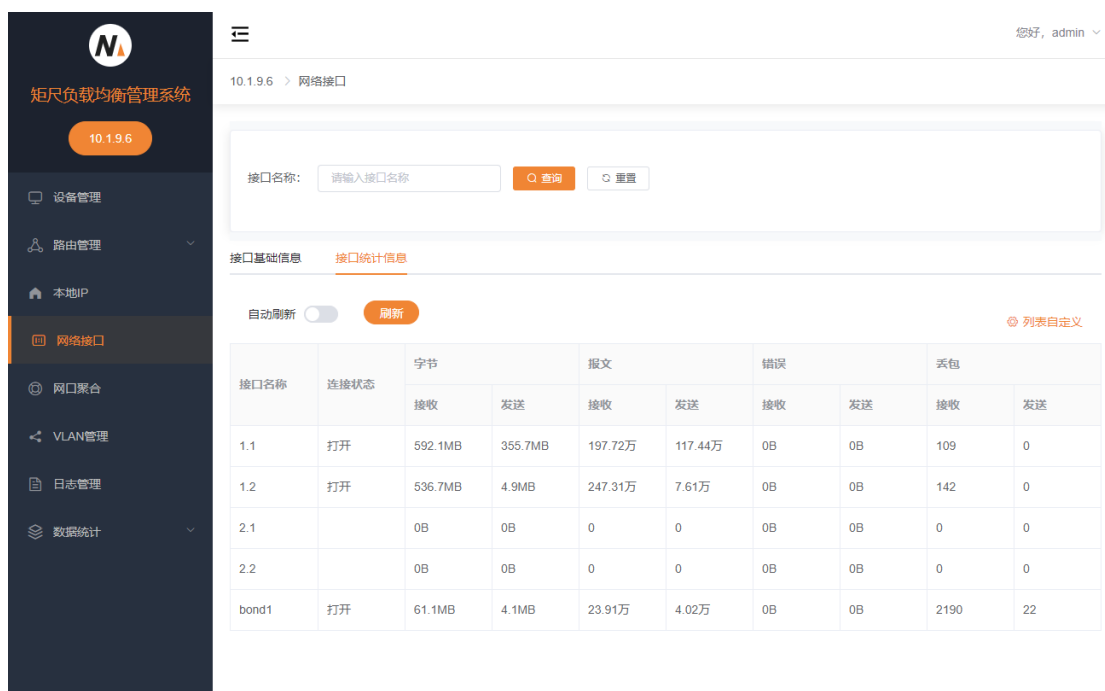
可通过“接口名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

可点击【配置 MTU】按钮，设置该接口 MTU，取值范围为 576 到 9065 之间的整数。



● 数据区域:

点击列表 tab 页签“接口统计信息”，接口统计信息所示:

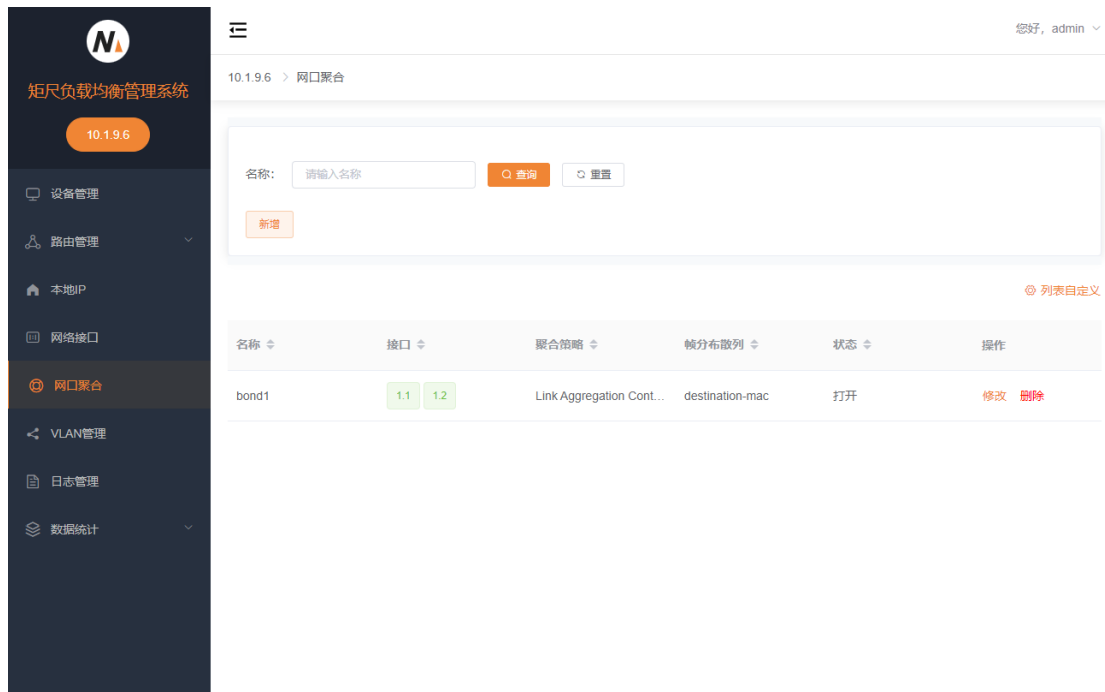


在接口统计信息页面，可设置数据的刷新方式和刷新频率，点击【刷新】按钮，也可进行手动实时刷新。

4.8.5 网口聚合

网口聚合主要实现，把一组物理端口联合起来，做为一个逻辑的通道，从而增加交换机之间的传输带宽，并实现链路冗余备份。

点击“网口聚合”菜单，默认展示当前按照用户创建时间倒序排列的网口聚合信息列表



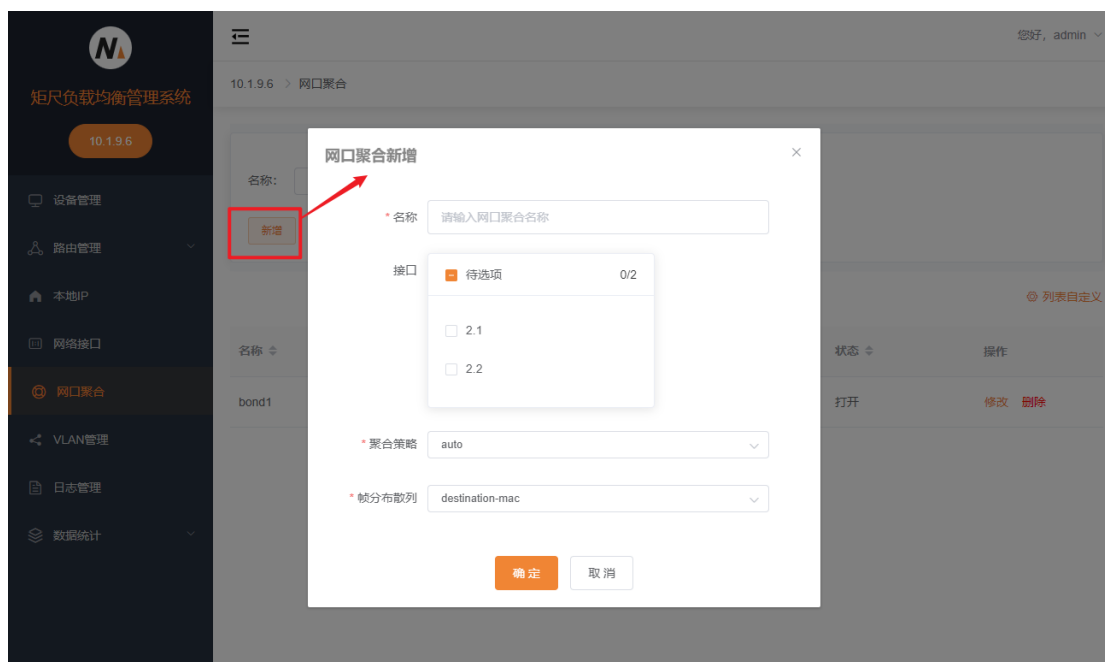
- **查询区域：**

可通过“聚合网口名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

- **数据区域：**

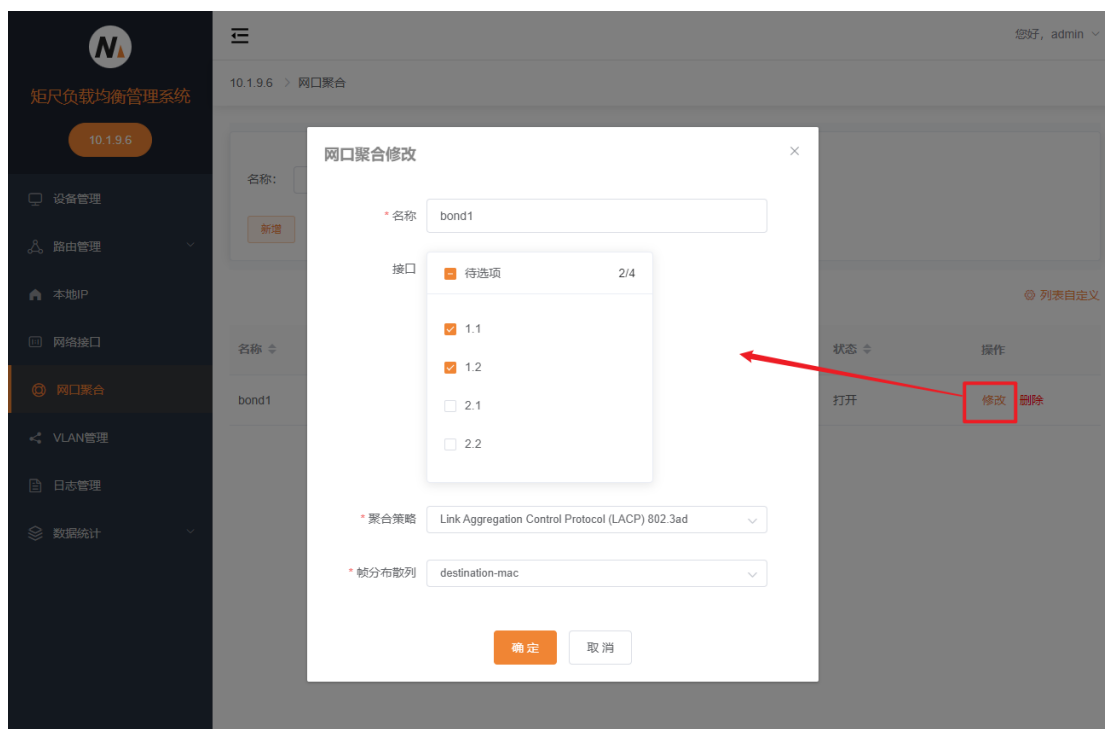
接口状态有三种：打开（绿色）、关闭（红色）、未接电缆（灰色）

点击列表上方【新增】按钮，弹框打开网口聚合新增页面，可添加/配置新的网口聚合信息。

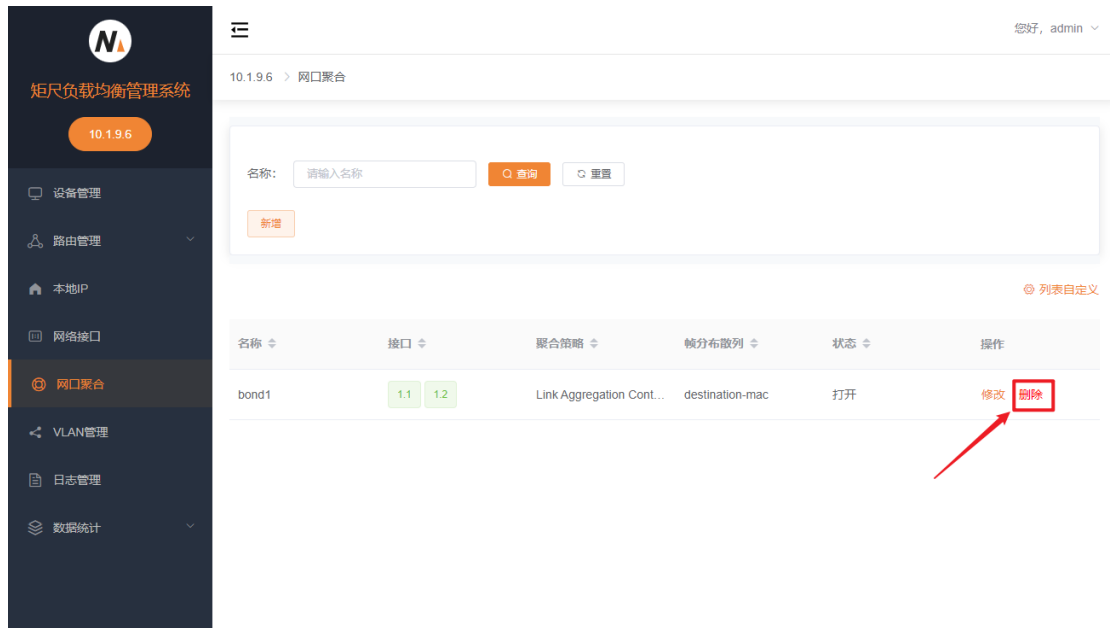


注：网口一旦聚合后，聚合网口中的网络接口将不会独立存在再次聚合成其他聚合网口

选择需要修改的网口聚合信息，点击此用户所在行操作栏的【修改】按钮，弹框打开网口聚合信息修改页面。



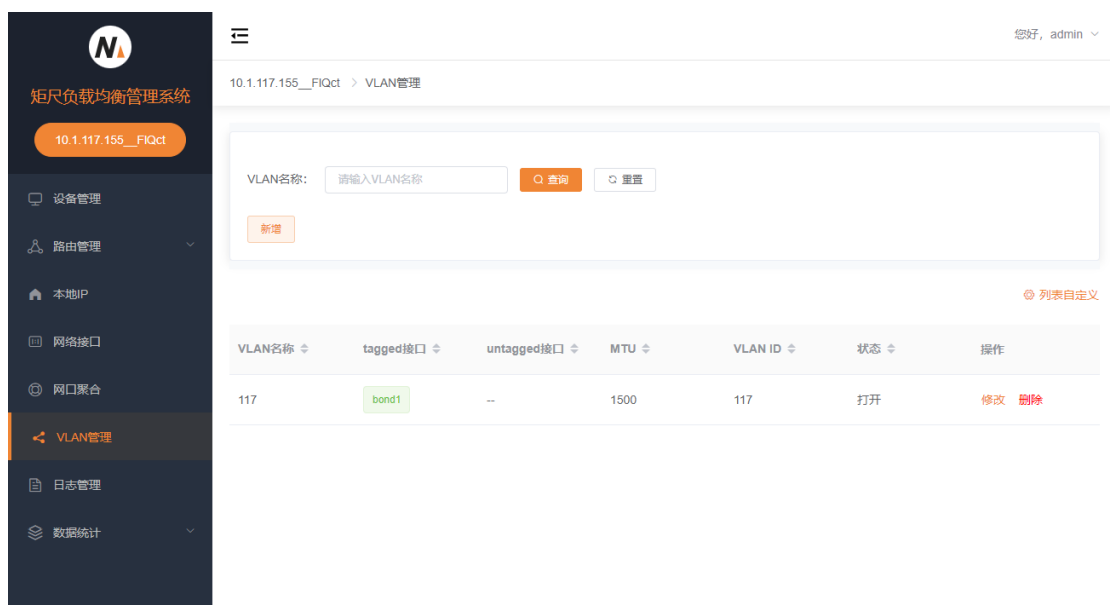
选择需要删除的网口聚合信息，然后操作栏的【删除】按钮，可对网口聚合信息进行删除操作。



4.8.6 Vlan 管理

VLAN 管理主要实现划分 VLAN 的目的，把内网划分为不同的网段，以控制流量、减少设备投资、简化网络管理、提高网络的安全性，而且更加便于管理。

点击“VLAN 管理”菜单，默认展示当前按照用户创建时间倒序排列的 VLAN 信息列表。

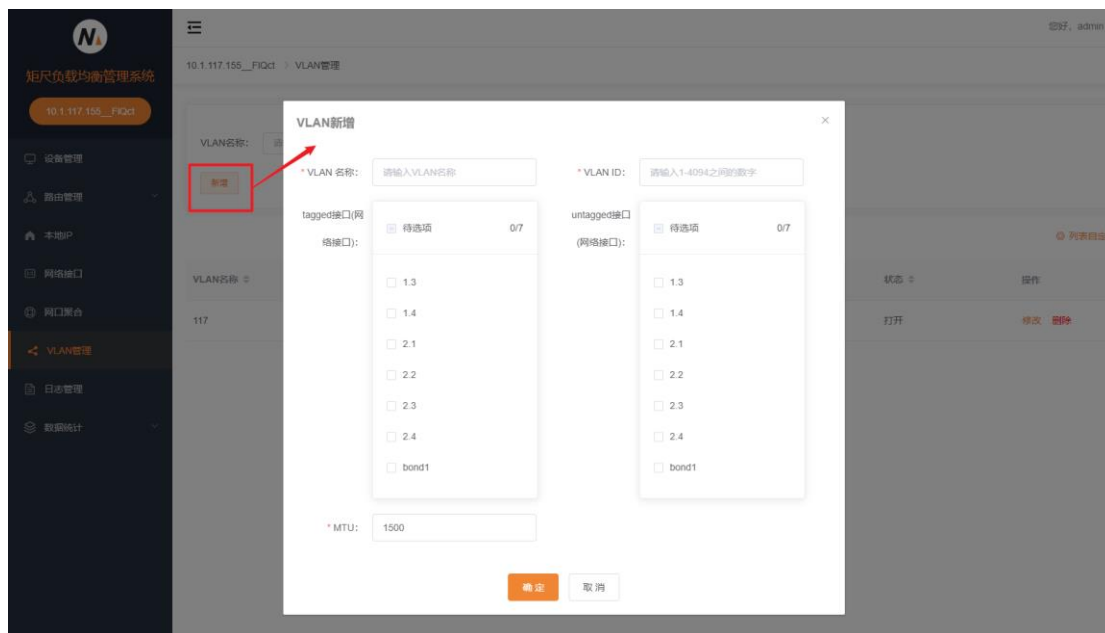


● 查询区域:

可通过“VLAN 名称”属性，进行条件查询操作。点击【查询】按钮执行查询操作，点击【重置】按钮将查询条件清空；

● 数据区域:

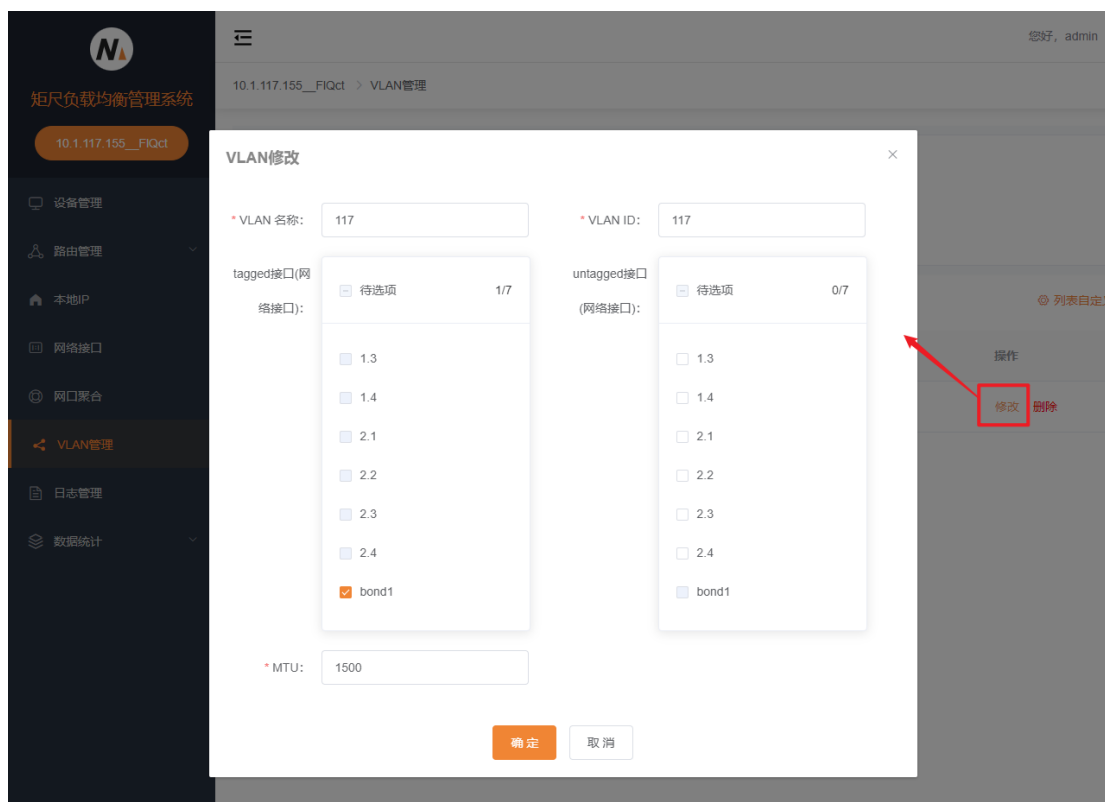
点击列表上方【新增】按钮，弹框打开 VLAN 新增页面，可添加/配置新的 VLAN 信息。



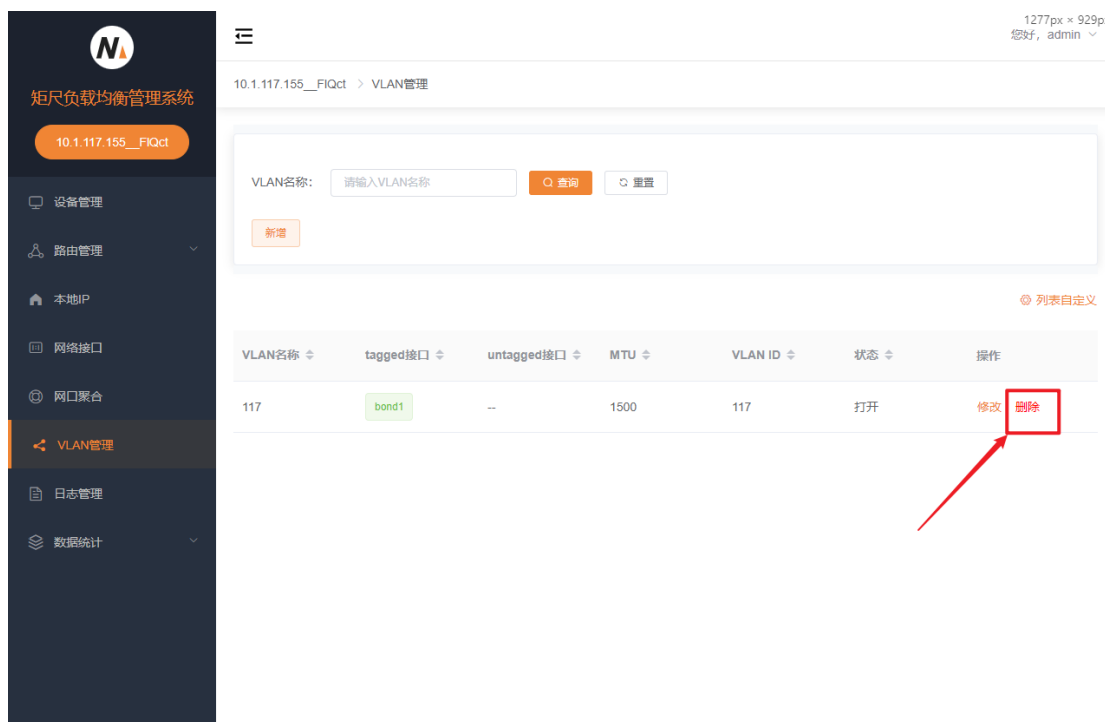
注:

- 同一个 VLAN 中，tagged 和 untagged 接口不能选择同一网络接口/聚合网口；
- 接口一旦聚合以后，就不能单独选择了；比如有四个接口 2.1、2.2、2.3、2.4，把 2.1 和 2.2 聚合（external1）以后，待选项只会有三个：external1、2.3、2.4；
- tagged 可以跨 VLAN 重复选择，但是 untagged 不可以；比如创建了两个 VLAN，分别为 VLAN1 和 VLAN2，VLAN1 的 tagged 选择了 2.1，VLAN2 的 tagged 也可以选择 2.1，但是如果 VLAN1 的 untagged 选择了 2.2，VLAN2 就不能选择 2.2 了

选择需要修改的 VLAN 信息，点击此用户所在行操作栏的【修改】按钮，弹框打开 VLAN 信息修改页面。



选择需要删除的 VLAN 信息，然后操作栏的【删除】按钮，可对 VLAN 信息进行删除操作。



注：如果需要删除的 VLAN 已被接口地址、路由进行关联，无法删除成功

4.8.7 日志管理

用户可以导出健康检查错误日志、负载均衡错误日志、业务访问日志、配置错误日志。

点击“日志管理”，进入日志菜单：

开启日志功能：



可配置四类日志的协议、IP、端口、和标签：



点击“日志导出”标签，选择一项日志类型进行导出。



当右上角总开关关闭时，用户不能进行配置或导出操作，当开关开启时，用户在没有对 syslog 进行配置时，可以通过日志导出功能导出相应的日志记录。当用户对 syslog 进行配置时，日志导出功能将无法使用，日志将根据 syslog 协议推送到用户配置的指定服务器 ip 和 port。

4.8.8 数据统计

设备页面的数据统计分别有 4 个二级菜单，其中设备性能、网络接口、设备会话三个菜单功能同 4.3.2，展示的是当前设备下的数据。

4.9 变更执行

当集群管理、SLB 本地负载下的功能变动（包括新增、修改、删除）触发需要变更执行操作时，会在页面头部【变更执行】按钮旁出现红色感叹号，点击感叹号可查看触发变更的事件列表。



点击【变更执行】按钮将会弹出任务列表，任务状态有未开始、执行中、执行成功、执行失败四种，执行失败的任务可在状态旁点击重新执行，点击【结束任务】可清空所有任务。

