



# 银河麒麟网络智能管理系统 V2.0.0——产品手册

麒麟软件有限公司

2025年 5 月 16 日

版权所有 © 2014–2025 麒麟软件有限公司，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 目录

第一部分 安装与配置 .....	7
1 环境规划与服务端安装流程 .....	7
第二部分 各模块使用说明 .....	7
2 首次登录 .....	7
2.1 账号申请 .....	7
2.2 系统登录 .....	7
2.3 密码重置 .....	8
2.4 密码修改 .....	8
2.5 退出登录 .....	9
2.6 启用操作 .....	10
3 首页 .....	10
3.1 模块简介 .....	10
3.2 首页内容介绍 .....	10
4 DHCP .....	12
4.1 模块简介 .....	12
4.2 子网 .....	12
4.3 共享网络 .....	20
4.4 主机预留 .....	24
4.5 租约搜索 .....	32
5 服务监控 .....	33
5.1 模块简介 .....	33
5.2 kea 应用监控 .....	33
5.3 服务器状态监控 .....	38
5.4 高可用监控 .....	39
6 异常告警 .....	40
6.1 模块简介 .....	40
6.2 异常告警规则 .....	40
6.3 查看异常告警信息 .....	42

7. 日志记录 .....	43
7.1 模块简介 .....	43
7.2 查看日志信息 .....	43
8 用户中心 .....	44
8.1 模块简介 .....	44
9 通用配置 .....	45
9.1 模块简介 .....	45
9.2 审核检查器 .....	45
9.3 通信检测 .....	47
9.4 其他配置 .....	47
10 数据统计 .....	48
10.1 模块简介 .....	48
10.2 DHCPv4 数据 .....	48
10.3 DHCPv6 数据 .....	49
第三部分 重点场景操作说明 .....	49
11 如何设置地址池范围 .....	50
12 如何设置 DHCP option .....	50
13 如何设置 DHCP 参数 .....	51
13.1 操作步骤 .....	51
13.2 具体参数介绍 .....	51
14 如何设置租约参数 .....	69
15 如何检查冲突地址 .....	69
第四部分 参考手册 .....	69
第五部分 附录 .....	70
16 术语解释 .....	70

## 银河麒麟网络智能管理系统介绍

欢迎您使用银河麒麟网络智能管理系统！

麒麟软件主要面向通用和专用领域打造安全创新操作系统产品和相应解决方案，以安全创新操作系统技术为核心，现已形成银河麒麟服务器操作系统、桌面操作系统、嵌入式操作系统、操作系统增值产品为代表的产品线。

银河麒麟网络智能管理系统，通过直观清晰易理解的 Web 界面，帮助系统管理员在大规模 IP 管理场景中完成高效运维管理工作，打造 IP 地址配置、地址池管理、网络管理、租约管理、日志管理、异常告警等多种核心场景解决方案。其易用性强、运行稳定，支持高可用与分布式部署方案，实现关键操作全流程闭环管理，能够在坚实的基础之上提升网络管控的可靠性、稳定性、易用性。

银河麒麟网络智能管理系统支持银河麒麟主流操作系统，支持在物理机、虚拟机和云环境中部署和配置。平台聚焦于 DHCP 地址配置、地址池管理、子网管理、网络管理、日志监控等领域，实现了大规模 IP 动态分配、地址的绑定预留及冲突检测、租约查询、服务健康度评估、日志记录&查询、数据统计展示、异常告警等功能，简化了 DHCP 配置操作，提升运维效率和质量。

### 文档约定标识

#### 【界面上的文本】或【屏幕、窗口中的按钮】

在 GUI 界面屏幕或窗口中的标题、词汇、或短语、菜单选项等会用全角方括号“【】”括起来。它用来标明某个 GUI 屏幕或 GUI 屏幕上的某个元素（譬如与复选框或字段相关的文本）。例如：请点击【确定】按钮等。

### 可替代的文字

用在例子中的文本，如使用这种*斜体*方式，表明该文本应被用户提供的数据所代替。

### 命令

带字符边框的表明是命令。



窍门：即一些有用的信息、小技巧等；



重要：提示请您需要格外重视的内容；



注记：提醒您关注的事项、注释；



警告：警示信息，告诫您采取或防止哪些操作；



小心：情况可能稍有复杂，请您谨慎操作。

## 第一部分 安装与配置

### 1 环境规划与服务端安装流程

参见《银河麒麟网络智能管理系统 V2.0.0\_产品安装部署手册\_V2.0.0》。

## 第二部分 各模块使用说明

### 2 首次登录

#### 2.1 账号申请

本平台通常是企业内部运营人员使用，所以不提供账号自注册功能。系统上线时会提供系统超级管理员账号，再由超级管理员登录后在【用户中心】模块创建用户账号，并为各用户账号分配角色。

#### 2.2 系统登录

打开浏览器（建议使用：Firefox，Chrome），在浏览器导航栏中输入 IP，打开银河麒麟网络智能管理系统登录页面。在用户登录界面输入正确的用户名和密码登录系统。默认用户名为 admin，默认密码为 admin。



图 2-1 银河麒麟网络智能管理系统登录界面

## 2.3 密码重置

超级管理员：忘记密码，可联系“麒麟软件有限公司”的相关对接人，重置密码。

普通用户：忘记密码，需跟超级管理员联系，超级管理员在菜单【用户中心】的用户列表中，针对需修改密码的用户，点击【编辑】按钮，即可修改密码（注：密码长度至少需 8 个字符）。

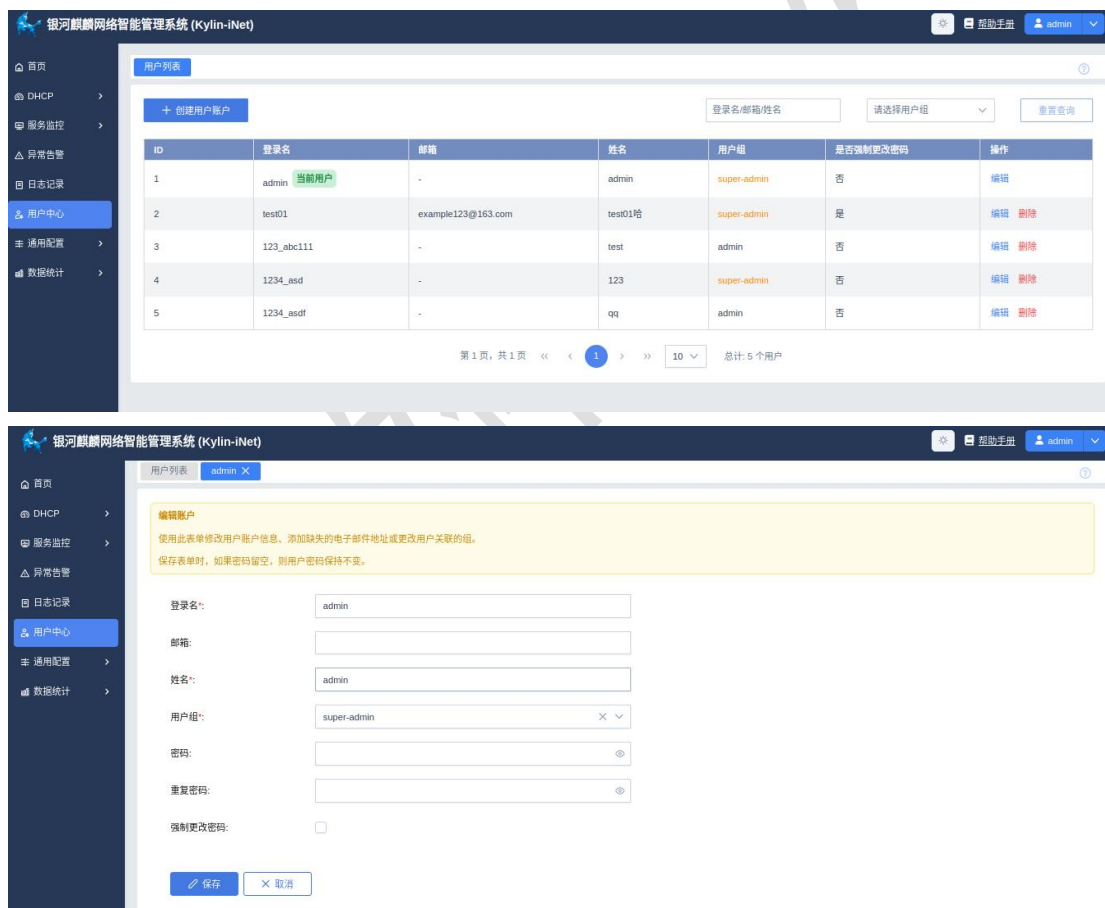


图 2-2 密码重置步骤

## 2.4 密码修改

管理员和普通用户，在首次登录成功后，都应及时修改默认密码。点击右上角



角用户账号下拉箭头，显示下拉菜单，点击【更改密码】，弹窗中输入“当前密码”、“新密码”、“确认密码”，点击【保存】即完成密码修改。



图 2-3 密码修改步骤

## 2.5 退出登录

完成业务操作后，为了保护账号安全，可以选择退出登录，点击右上角用户账号，在下拉列表中点击【退出登录】，即可退出账号在此系统的登录，页面自动跳转至登录页。



图 2-4 退出登录

## 2.6 启用操作

首次登录系统，导航栏不会展示【DHCP】板块，需完成机器授权后，才可进行 DHCP 相关操作和监控。

点击【服务监控】一下拉列表点击【服务器状态监控】，进入服务器列表页面，点击【未授权】标签按钮，筛选展示该系统中未授权的机器，针对需要授权的目标机器，点击操作列的【授权】，即可对该机器进行授权。

## 3 首页

### 3.1 模块简介

首页可整体概览 DHCP 服务状况，通过直观的图表展示 DHCPv4&DHCPv6 的服务使用情况，以及保障 DHCP 服务正常运行的主机服务状态信息，用户可在首页快速获取关键信息。

### 3.2 首页内容介绍

1) IP 总量及利用率面板：展示 DHCPv4 地址总量/利用率、DHCPv6 地址总量/利用率、DHCPv6 前缀总量/利用率。

2) 子网/共享网络总数统计面板：展示子网、共享网络（此处只统计关联了子网的共享网络）各自的总数及构成，标明了 DHCPv4、DHCPv6 子网的个数及占比、共享网络个数及占比。

3) DHCPv4/DHCPv6 面板：展示利用率 TOP5 的子网、共享网络（此处只统计关联了子网的共享网络）及对应统计信息（地址利用率、拒绝量），点击具体子网，跳转至对应子网详情页面，可查看并编辑子网配置（请参阅“4.2.2 更新

子网”章节），点击具体共享网络，跳转至对应共享网络页面，可查看并编辑共享网络配置（请参阅“4.3.2 更新共享网络”章节）。

4）服务状态面板：展示已监控的主机的基础信息，包括主机名、应用名称、主机运行的守护程序、通信状态、守护程序在过去 15 分钟和 24 小时内发送的平均 ACK 数、其高可用性状态、是否检测到 HA 故障，以及主机正常运行时间。点击主机名，跳转至对应服务器详情页面，可查看更多主机详细信息（请参阅“5.3.1 查看服务器详情”章节）；点击应用名称，跳转至对应应用详情页面，可查看更多应用程序详情信息（请参阅“5.2.1 查看 kea 应用基础信息”章节）。

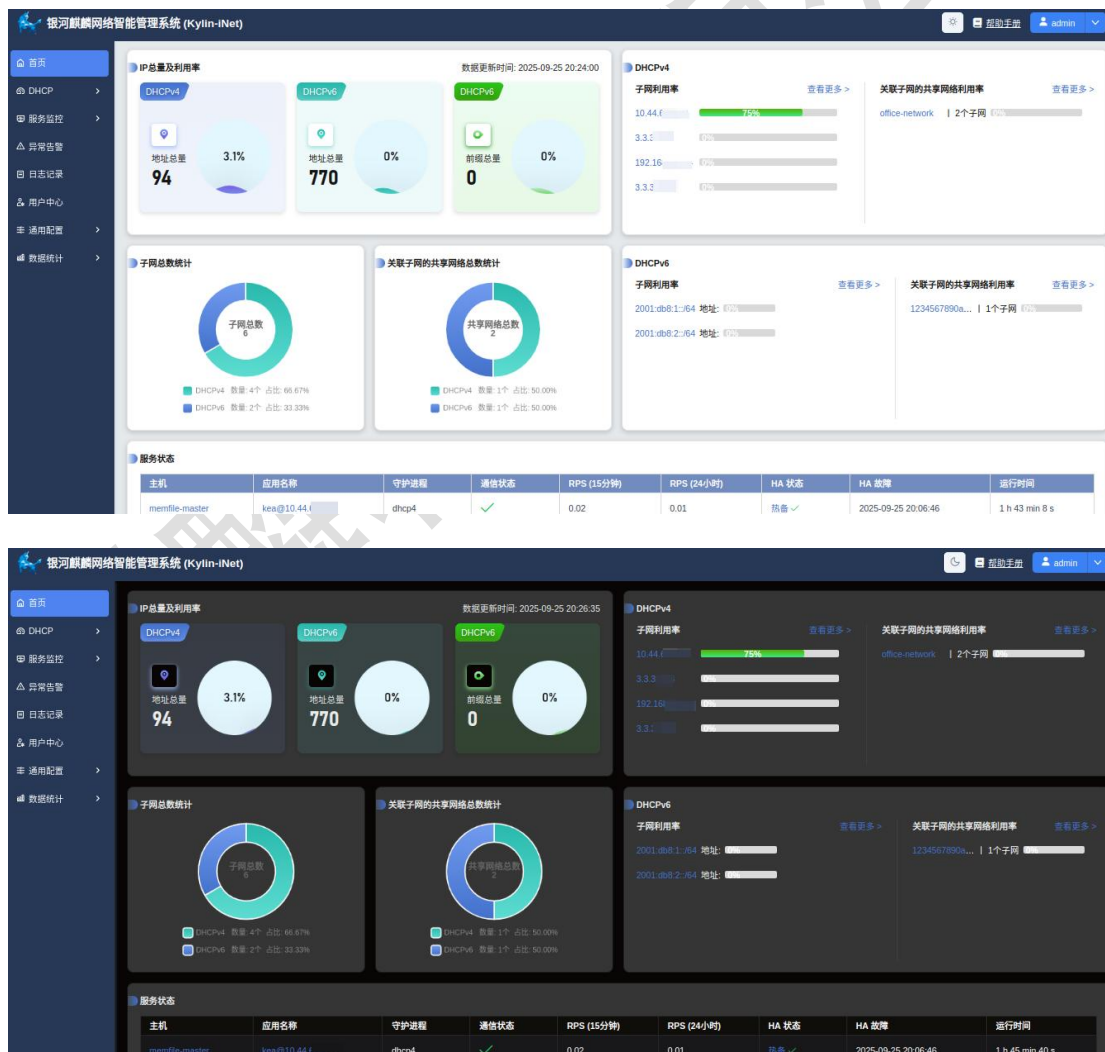


图 3-1 首页（日常模式与黑夜模式）

## 4 DHCP

### 4.1 模块简介

DHCP 模块为用户提供核心的 IP 配置管理功能，其中【子网】支持用户编辑及查看所有子网配置。【共享网络】支持用户编辑及查看所有共享网络配置。

【租约搜索】支持用户按多维度搜索查看租约信息，用于排查特定 IP 或委托前缀是否有租约分配问题。【主机预留】支持用户指定部分地址为预留地址，不参与地址分配。

### 4.2 子网

操作入口：登录平台后，点击【DHCP】—下拉列表点击【子网】

#### 4.2.1 新建子网

在【子网】页面点击【新建子网】按钮，按下述步骤创建子网：

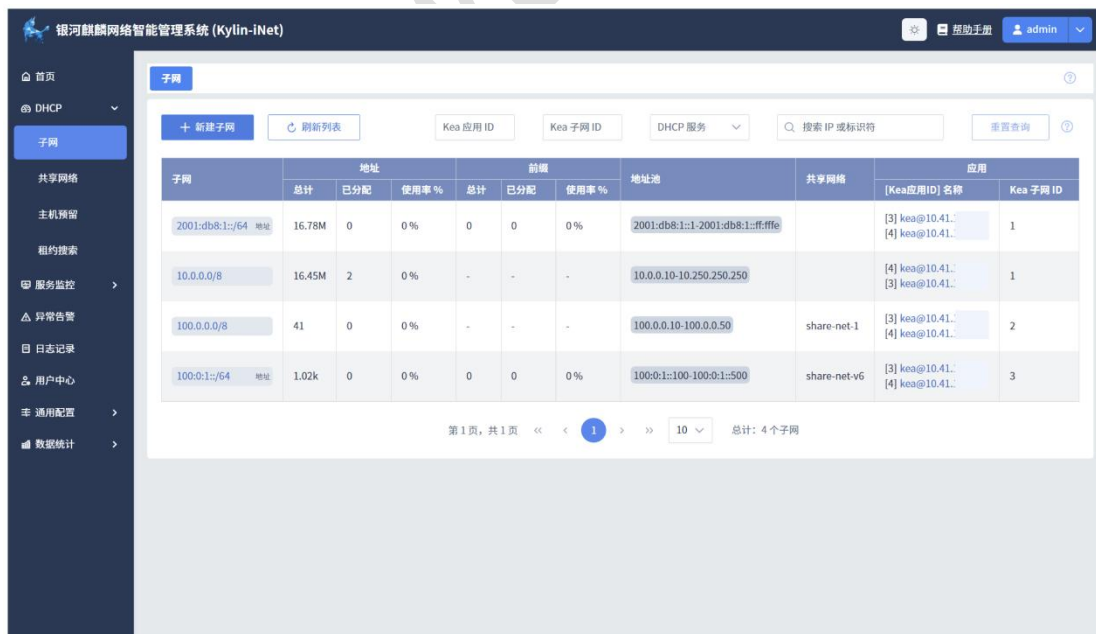


图 4-1 子网页面

#### ① 填写子网名称

填写有效子网名称，IPv4 地址（例如 192.0.2.0/24）或 IPv6 前缀（例如 2001:db8:1::/64）。填写完名称后，点击【确认】按钮，可继续配置子网信息。

图 4-2 填写子网名称

## ② 填写基础配置（选择 DHCP 服务器及共享网络）

可定义通用子网配置，并即时部署至多台 DHCP 服务器。在需要服务冗余的场景下，可在多个实例中配置同一子网（例如 高可用性部署或共享租约数据库的部署）。

选择 DHCP 服务器，该子网将被同步至所选的服务器。注：服务器列表仅包含与子网前缀（IPv4/IPv6）匹配的实例，且仅显示已运行 subnet\_cmds 钩子库的服务器。

图 4-3 选择 DHCP 服务器

为新子网分配共享网络，共享网络下拉列表为空可能由以下两种原因导致：  
所选 Kea 实例中不存在共享网络；为子网选择的某些 Kea 实例未配置共享网络声


明。



图 4-4 选择共享网络

若所选实例不存在共享网络，只需在创建子网前新建一个共享网络即可（请参阅“4.3.1 新建共享网络”章节）。

若缺少共享网络声明，需更新共享网络并将其分配至所有计划部署该子网的服务器。例如：假设需将新子网同时部署至服务器 1 和服务器 2，但该子网当前仅属于已分配至服务器 1 的共享网络。此时需先编辑该共享网络，添加对服务器 2 的分配（请参阅“4.3.2 更新共享网络”章节），再创建新子网并选择服务器 1 和服务器 2，此时共享网络列表应包含更新后的共享网络，可从列表中选择该共享网络。

 注：选定共享网络后，子网分配关系不可更改。如需修改分配，需先点击所选共享网络名称右侧的【X】按钮解除关联。移除共享网络后即可重新调整子网分配关系。

### ③ 添加地址池

点击【添加地址池】按钮，可创建地址池，需填写地址范围、分配 DHCP 服务器、设置地址池 DHCP 参数、地址池 DHCP 选项。点击【删除该地址池】按钮，可移除对应的地址池。

子网通常包含一个或多个地址池（支持 IPv4 和 IPv6），也可包含委托前缀

池（仅限 IPv6）。DHCP 服务器从这些地址池的可用资源中向客户端分配租约。

**地址范围：**通过起始地址（第一个地址）、结束地址（最后一个地址）来定义地址范围，两个地址必须与子网前缀匹配（即均位于该子网内），且起始地址必须小于或等于结束地址。若起始地址与结束地址相同，则该池仅包含单一地址。IPv6 子网可添加委托前缀池。委托前缀池范围的定义方式稍有不同，且其前缀无需匹配（属于）子网前缀。委托前缀池由实际前缀（如 3000::/64）和委托前缀长度（如 96）组成。委托前缀长度必须大于等于前缀长度，例如  $96 > 64$ 。若两者相等，则该池仅包含单一前缀。注：地址范围不能为空，不允许存在空池。

**分配 DHCP 服务器：**在某些场景中，多个 DHCP 服务器可共享相同子网但配置不同地址池。此配置可避免因地址池重叠导致不同服务器向客户端分配相同地址的冲突。若需使地址池在所有服务器中生效，需选择全部服务器。

**填写地址池 DHCP 参数：**填写客户端类(Client Class)、Pool ID、Require Client Classes。

**填写地址池 DHCP 选项：**点击【添加选项】，可输入或下拉选择地址池 DHCP 选项，设置该选项对应的数据格式和具体值，若勾选【始终发送】复选框，表示该选项被配置为始终返回给 DHCP 客户端，即使客户端未请求也会进行发送。

1. 点此按钮新增地址池，可添加多个地址池 + 添加地址池

2. 填写地址范围

3. 选择服务器

4. 填写地址池的DHCP参数

5. 填写地址池的DHCP选项

勾选此框，可分别给各个服务器设置各自的选项参数值

点此按钮，可设置选项格式及具体参数值

图 4-5 添加地址池



#### ④ 填写 DHCP 参数

这些参数涉及该子网内租约分配的不同维度。默认情况下，子网中每个 DHCP 服务器将继承相同的 DHCP 参数值。

若需为不同服务器设置不同的参数值，可点击【解锁】标，对应参数的配置表单将拆分为独立模块，此时可在不同服务器的输入框中分别设定不同数值。

The screenshot displays the 'DHCP 参数' (DHCP Parameters) configuration page. It is divided into two main sections: '基础参数' (Basic Parameters) and '租约参数' (Lease Parameters). In the '基础参数' section, there are two rows for 'Allocator' configuration, each with a text input (containing 'kea@10.44'), a dropdown menu (set to '/dhcp4'), and a '(未指定)' (Not specified) dropdown. To the right of each row are '清除' (Clear) and '解锁' (Unlock) buttons. The 'Authoritative' section has a checkbox labeled '未设置' (Not set) and a '清除' (Clear) button. A tooltip points to the '解锁' button, stating '解锁后可针对每个服务器单独设置参数' (After unlocking, parameters can be set individually for each server). The '租约参数' section contains three rows for 'Valid Lifetime', 'Min Valid Lifetime', and 'Max Valid Lifetime', each with a text input, a '清除' (Clear) button, and a '锁定' (Lock) button.

图 4-6 填写 DHCP 参数

#### ⑤ 填写 DHCP 选项

DHCP 选项模块用于定义向子网内客户端返回的特定 DHCP 选项。点击【添加选项】可设置多个选项。通常情况下，分配给同一子网的不同服务器会采用相同的选项配置。但通过类似于上述 DHCP 参数的差异化机制，也可实现选项配置的个性化设置，勾选【分开设置各服务器选项】即可针对每个服务器单独设置 DHCP 选项，并为不同服务器指定各自的选项集合。

配置 DHCP 选项时，首先需选择选项代码，然后点击代码选框旁边的蓝色按钮，可选择该选项的各个字段类型，需根据选项要求填入适当数值。若某 DHCP 选项包含字段数组，需扩展数组字段，可展开蓝色按钮的下拉列表，选择需添加到数组中的正确字段类型。





再关联至新的共享网络。

④ **关于地址池的变更：**删除地址池，已分配的 IP 租约仍将保留，客户端可继续使用直至租约过期；被删除地址池的 IP 将拒绝续租请求，客户端需从现有地址池中重新获取新租约。

⑤ **更改操作：**点击【撤销更改】按钮，可清除更改内容，恢复原始配置信息；点击【取消】按钮，将关闭该页面且不生效任何修改。

### 4.2.3 筛选子网

#### ① 子网列表展示信息

-子网名称：点击可进入子网详情页，查看具体配置信息及进行编辑、删除操作。

-地址使用情况统计：展示地址池总量、已分配的量级、使用率。

-地址池：展示具体的地址池范围。

-共享网络：展示该子网分配的共享网络信息。

-应用名称：展示 kea 应用 ID 及名称，点击可进入相关应用详情页面。

-子网 ID：展示对应应用的子网 ID。

#### ② 筛选条件

当前支持的筛选条件包括：应用 ID、子网 ID、DHCPv4/v6 服务选择、按 IP 或标识符搜索。

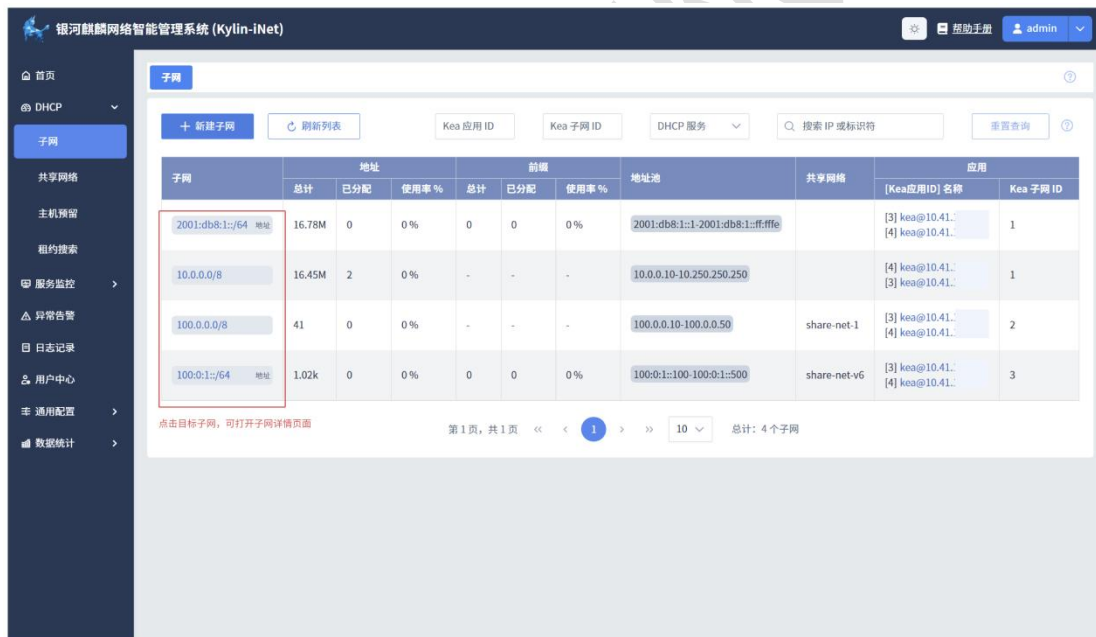
### 4.2.4 查看子网

在【子网】页面的子网列表中，点击目标子网，进入子网详情页，可查看该子网的具体配置信息。

可查看子网的所有服务器信息，点击目标服务器可跳转至该服务器详情页。

可查看子网的所有地址池范围，以及地址池利用率情况。第一个饼图展示该子网下的整体地址池统计数据，其余饼图则展示各个服务器的地址池利用率，统计信息包含总计、已分配量级（分配的租约数量，包含已拒绝的租约）、已使用量级（分配的租约数量，不包含已拒绝的租约）、已拒绝量级、不确定量级（仅当已拒绝的租约数量大于已分配的租约数量时，才显示该信息）。

可查看各服务器的 DHCP 参数信息，以及 DHCP 选项配置，选项旁显示“始终发送”标签，表示该选项将始终返回给 DHCP 客户端，即使客户端未请求，也会发送该选项数据。“空选项”标签表示该选项未包含有效信息，“global”标签，表示该选项是全局级别的。



子网	地址			前缀			地址池	共享网络	应用	
	总计	已分配	使用率 %	总计	已分配	使用率 %			[Kea应用ID] 名称	Kea 子网 ID
2001:db8:1::/64 地址	16.78M	0	0%	0	0	0%	2001:db8:1::1-2001:db8:1::ffff		[3] kea@10.41. [4] kea@10.41.	1
10.0.0.0/8	16.45M	2	0%	-	-	-	10.0.0.10-10.250.250.250		[4] kea@10.41. [3] kea@10.41.	1
100.0.0.0/8	41	0	0%	-	-	-	100.0.0.10-100.0.0.50	share-net-1	[3] kea@10.41. [4] kea@10.41.	2
100.0.1::/64 地址	1.02k	0	0%	0	0	0%	100.0.1::100-100.0.1::500	share-net-v6	[3] kea@10.41. [4] kea@10.41.	3



图 4-8 查看子网详情

## 4.2.5 删除子网

在【子网】页面的子网列表中，点击目标子网，进入子网详情页，点击下方的【删除】按钮，即可删除该子网，仅当子网所在的服务器加载了 subnet\_cmds 钩子库时，才能执行删除操作。

## 4.3 共享网络

操作入口：登录平台后，点击【DHCP】一下拉列表点击【共享网络】

### 4.3.1 新建共享网络

共享网络可将具有相同配置参数的子网进行聚合管理，为连接至不同子网的 DHCP 客户端提供统一的地址分配空间。

在【共享网络】页面点击【新建共享网络】按钮，按下述步骤创建共享网络：



图 4-9 新建共享网络

### ① 选择 DHCP 服务器

需将共享网络绑定至一个或多个 DHCP 服务器，所有服务器须为相同类型（DHCPv4 或 DHCPv6），选定首个服务器后，后续可选服务器列表将自动呈现同类型设备。在选定服务器后，共享网络将在所选服务器中同步创建。

### ② 填写共享网络名称

需确保名称具有唯一性。

### ③ 填写 DHCP 参数和 DHCP 选项

此处定义的 DHCP 参数与 DHCP 选项将作为全局设置，自动应用于后续加入该共享网络的所有子网，若子网单独定义了相同参数/选项，其配置将覆盖掉共享网络层级的全局设置。此外，若需针对不同服务器配置不同的共享网络参数，可点击【解锁】标，对应参数的配置表单将拆分为独立模块，此时可在不同服务器的输入框中分别设定不同数值，类似于新建子网流程（请参阅“4.2.1 新建子网”章节）。

### ④ 提交共享网络配置

完成上述信息填写后，点击【提交】按钮，即可保存配置并创建共享网络。

 注：共享网络创建后，需要再创建子网，并绑定共享网络，共享网络才

能生效。

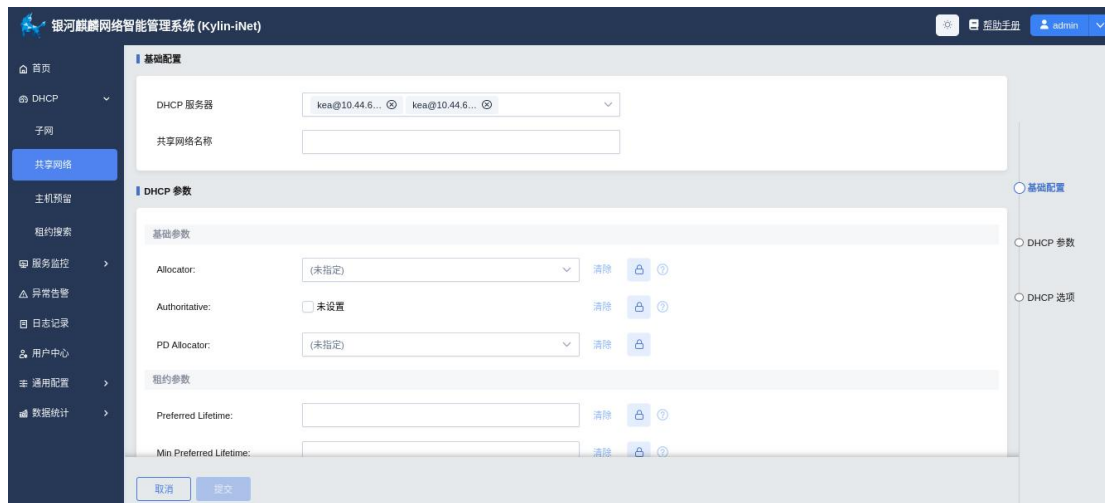


图 4-10 新建共享网络的参数配置

### 4.3.2 更新共享网络

在【共享网络】页面的列表中，点击目标共享网络，进入共享网络详情页，可查看该共享网络的具体配置信息，点击下方的【编辑】按钮，进入编辑页面，具体配置操作请参阅“4.3.1 新建共享网络”章节。

更新共享网络需注意的事项：

- ① **前提条件：**仅当共享网络所在的服务器加载了 subnet\_cmds 钩子库时，才能执行更新操作。
- ② **服务器解绑：**移除某台服务器时，该共享网络及其下属所有子网将同步从该服务器中删除。若后续重新将该服务器加入共享网络，所有子网会自动恢复关联。

### 4.3.3 筛选共享网络

#### ① 共享网络列表展示信息

-共享网络名称：点击可进入共享网络详情页，查看具体配置信息，进行编

辑、删除操作。

-地址使用情况统计：展示地址池总量、已分配的量级、使用率。

-子网：展示该共享网络关联的所有子网信息。

-应用名称：点击可进入相关应用详情页面。

## ② 筛选条件

当前支持的筛选条件包括：应用 ID、DHCPv4/v6 服务选择、按共享网络名称搜索。

### 4.3.4 查看共享网络

在【共享网络】页面的列表中，点击目标共享网络，进入详情页，可查看该共享网络的具体配置信息。

可查看共享网络的所有服务器信息，点击目标服务器可跳转至该服务器详情页。

可查看共享网络的所有地址池范围，以及地址池利用率情况。第一个饼图展示所有服务器的整体地址池统计数据，其余饼图则展示各个服务器的地址池利用率，统计信息包含总计、已分配量级（分配的租约数量，包含已拒绝的租约）、已使用量级（分配的租约数量，不包含已拒绝的租约）、已拒绝量级、不确定量级（仅当已拒绝的租约数量大于已分配的租约数量时，才显示该信息）。

可查看各服务器的 DHCP 参数信息，以及 DHCP 选项配置，选项旁显示“始终发送”标签，表示该选项将始终返回给 DHCP 客户端，即使客户端未请求，也会发送该选项数据。“空选项”标签表示该选项未包含有效信息，“global”标签，表示该选项是全局级别的。



### 4.3.5 删除共享网络

在【共享网络】页面的列表中，点击目标共享网络，进入详情页，点击下方的【删除】按钮，即可删除该共享网络。仅当共享网络所在的服务器加载了 subnet\_cmds 钩子库时，才能执行删除操作。

删除共享网络，也将同步移除其包含的所有子网，若需保留原共享网络中的子网，可在删除前逐个访问该共享网络下的子网，在子网编辑页面中删除对应共享网络。

## 4.4 主机预留

操作入口：登录平台后，点击【DHCP】一下拉列表点击【主机预留】

### 4.4.1 主机预留说明

① 主机预留由一个或多个 DHCP 标识符构成（如 MAC 地址、DUID 或客户端 ID），用于建立客户端与预留资源的关联。当客户端 DHCP 报文通过标识符匹配到主机预留时，将返回给客户端相关资源。

② 平台可检索到的预留配置：通过服务器配置文件定义的预留、通过 Host Commands 高级钩子库访问主机数据库后端实现的预留。

### 4.4.2 配置主机预留

操作入口：登录平台后，点击【DHCP】一下拉列表点击【主机预留】一点点击【新建主机】按钮。按下述步骤创建子网：



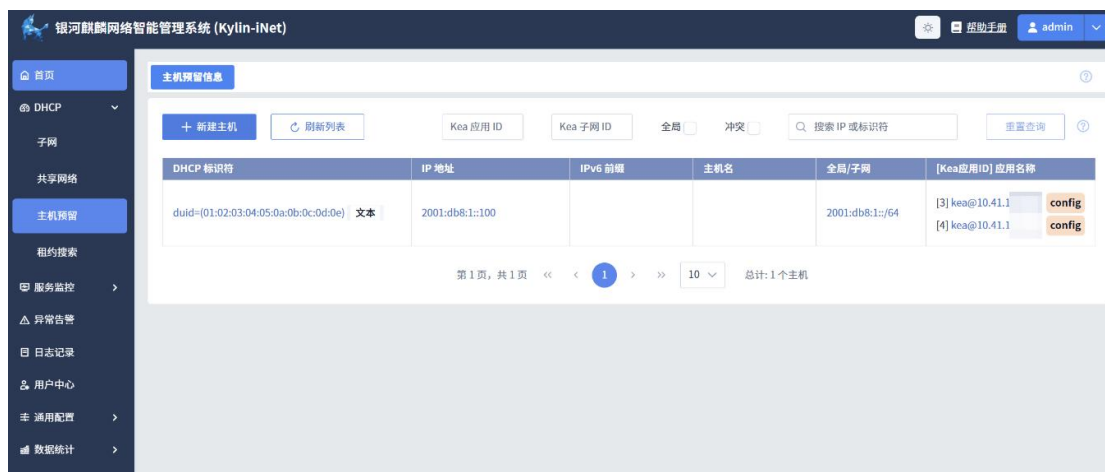


图 4-11 配置主机预留

### ① 前提条件

目标服务器必须配置加载了 Host Commands 钩子库。

### ② 选择全局级别/子网级别主机预留

开启【全局预留】，设置的预留地址将全局生效。

当为多个 DHCP 服务器配置同一主机预留时,通常各服务器需包含相同参数集（IP 地址、主机名、启动字段、客户端类别及 DHCP 选项）。默认情况下,新建多服务器主机预留会向每个服务器发送完全相同的配置。如需为不同服务器指定差异化的启动字段、客户端类别或 DHCP 选项等配置内容,需启用【配置单个服务器值】,此模式下需为每个 DHCP 服务器单独指定完整的启动字段、客户端类别及 DHCP 选项等配置内容。若某服务器参数留空,则该服务器将不接收相关配置。

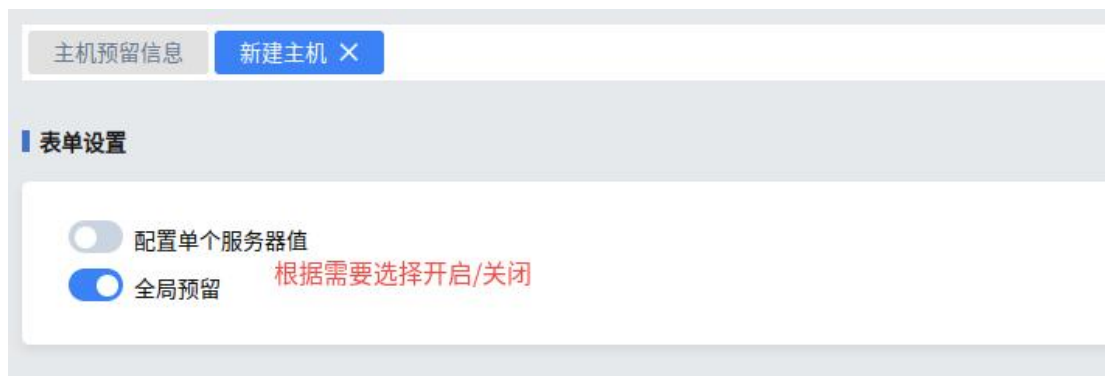


图 4-12 配置预留层级

### ③ 选择 DHCP 服务器和子网

至少选择一个服务器，注：只有加载了 host\_cmds 模块的服务器才会显示在 "DHCP 服务器" 下拉选项中。

在子网下拉列表中选择具体子网，若开启了【全局预留】，将禁用子网选择功能。



图 4-13 选择服务器&amp;子网

### ④ 填写 DHCP 标识符

为了关联 DHCP 客户端，需选择标识符类型（可用标识符根据 DHCPv4/DHCPv6 而有所区别）。标识符支持十六进制或文本格式输入。例如：

hw-address 通常以十六进制字符串表示（如 ab:76:54:c6:45:31）；而 circuit ID 等标识符常使用文本格式（如 circuit-no-1）。

1. 选择标识符  
hw-address

2. 选择格式  
hex

3. 按格式要求填写具体值  
例如 01:02:03:04:05:06

图 4-14 填写 DHCP 标识符

### ⑤ 填写预留地址

填写主机名及 IP 地址，关于 IP 地址，若为 IPv4，最多可指定一个 IPv4 地址，若为 IPv6，则可填写多个 IPv6 地址和委托前缀。

1. 填写主机名  
主机名:

2. 选择IPv6地址或前缀  
IP 预留: IPv6 address

3. 填写具体值  
e.g. 2001:db8:1::

添加 IP 预留

主机名:

IP 预留: IPv4 address

IPv4只需填写一个IP预留

图 4-15 填写预留地址

### ⑥ 设置配置文件获取方式（DHCPv4）

某些场景下，客户端在获取 IP 地址后，仍然需要其他配置参数，若客户端需要通过 TFTP 服务器获取配置文件，可填写下述字段：

下一个服务器（Next Server）、服务器主机名（Server Hostname）、启动文

件名（Boot File Name）。

这些配置既可在全局作用，也可限定某特定子网，当同时存在全局和子网层级的配置时，子网配置的优先级高于全局配置。若将子网层级的值设为“0.0.0.0”，则表示不向客户端发送该字段；若设为空字符串，则表示未定义子网层级的配置，此时将自动继承全局配置。



注：这些字段仅适用于 DHCPv4 服务器，编辑 DHCPv6 时不可用。

### ⑦ 关联客户端类别

可为主机关联一个或多个客户端类别。服务器会将选定类别分配给来自该主机的 DHCP 报文。点击【列表】按钮，从监控的服务器配置中获取类别列表，选择目标类别并点击【插入】，若列表中未展示所需类别，可直接在输入框键入类名并按回车确认，点击类别名旁的 X 图标可删除该关联。



注：客户端类别通常在 Kea 配置中定义。

### ⑧ 设置 DHCP 选项

DHCP 选项面板用于定义向子网内客户端返回的特定 DHCP 选项。若为【全局预留】，则分配给同一子网的不同服务器会采用相同的选项配置。若为【配置单个服务器值】，则可针对每个服务器单独设置 DHCP 选项，并为不同服务器指定各自的选项集合。

配置 DHCP 选项时，首先需选择选项代码，然后点击代码选框旁边的蓝色按钮，可选择该选项的各个字段类型，需根据选项要求填入适当数值。若某 DHCP 选项包含字段数组，需扩展数组字段，可展开蓝色按钮的下拉列表，选择需添加到数组中的正确字段类型。

点击字段旁的【X】，可删除对应字段，点击【删除选项】，可移除整个选

项配置。

图 4-16 展示了 DHCP 选项配置界面。界面顶部显示“DHCP 选项”，下方有“DHCP 选项 / kea@10.4 / dhcp4”的路径。左侧有一个“选项1”的列表，右侧有一个“删除选项1”的按钮。中间部分是一个配置区域，包含一个下拉菜单，当前选择的是“(2) 时间偏移量”，旁边有一个“始终发送”的复选框。下方有两个“int32”类型的输入框，每个输入框右侧都有一个红色的“X”图标。底部有一个“+ 添加选项”的按钮，旁边有提示文字“点击可添加更多选项”。

图 4-16 设置 DHCP 选项

#### ⑨ 保存提交

完成上述信息填写后，点击【提交】按钮，即可保存配置并推送至 DHCP 服务器。

### 4.4.3 筛选主机预留

#### ① 展示信息

-DHCP 标识符：以"hw-address=0a:1b:bd:43:5f:99"格式显示的 DHCP 标识符类型（此处 hw-address 表示 MAC 地址标识符类型）。

-IPv4 地址/IPv6 前缀：每个主机可能包含多个地址预留。

-主机名：显示可选的主机名预留配置（通过 Hostname 或 Client FQDN 选项分配）。

-全局/子网：显示预留地址所属的子网前缀，若为全局预留（即适用于服务器所有子网），则显示"global"标识而非子网前缀。

-应用名称：高可用性配置下通常显示多个节点链接。在这种情况下，每个 HA 对等体使用相同的配置，并可以向同一组客户端分配 IP 地址和委托前缀，包

括通过主机预留进行静态分配。如果 HA 对等体配置正确，它们共享的预留信息将在“应用名称”列中有两个链接。链接旁的标签可说明预留的配置来源：配置文件（通过本地配置文件定义）、数据库（通过 Host Commands 钩子库访问数据库定义）

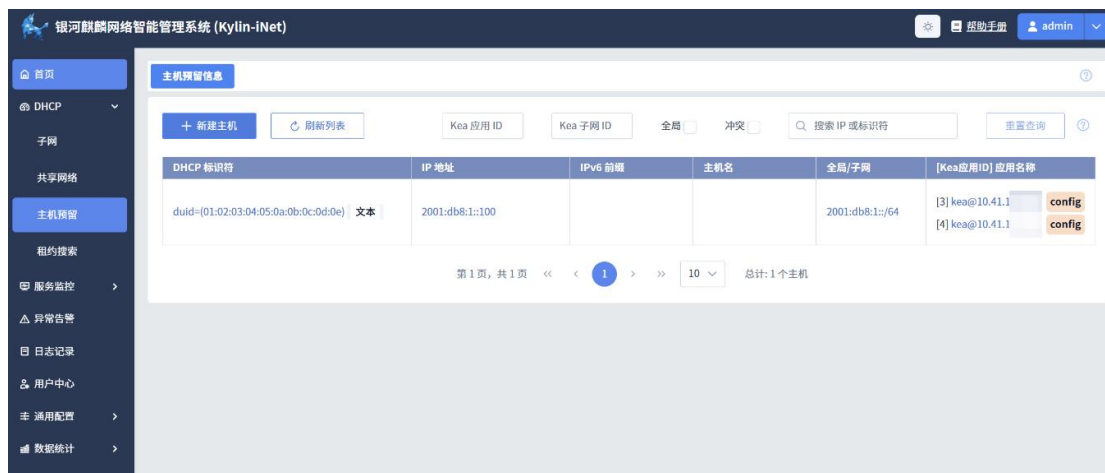


图 4-17 主机预留列表

## ② 筛选条件

可通过下述维度进行筛选：

- 标识符（支持十六进制值无冒号格式，例如 1b:bd:43 或 1bbd43 均可）
- 预留 IP、主机名
- 全局筛选（勾选该复选框，结果将显示全局级别的预留，再次单击该复选框，筛选结果将排除全局级别预留）
- 冲突筛选（可用此项筛选配置冲突的主机，单击该框一次，结果将显示配置文件与主机数据库之间存在配置冲突的主机信息，再次单击，筛选结果将排除存在配置冲突的主机）
- kea 应用 ID、kea 子网 ID：可按照相关 ID 进行搜索，结果将呈现对应 ID

## 关联的预留信息

### ③ 主机预留状态说明

IP 地址和 IPv6 前缀旁会显示使用主机预留的使用状态，相关状态说明如下所示：

状态	说明
使用中（in use）	分配给客户端的有效租约，标识客户端拥有预留，或者 该预留包含 flex-id/circuit-id，导致无法检测冲突项
已过期（expired）	分配给客户端的租约中至少有一个已过期
被拒绝（declined）	该地址在至少一个服务器上被拒绝
冲突（in conflict）	至少一个预留租约被分配给了未预留的客户
未使用（unused）	给定的预留没有租约

表 4-1 预留状态说明

### ④ 主机预留来源说明

主机预留有两种方式

第一种方式：在 kea 配置文件中指定主机预留（推荐该方式）。

第二种方式：使用主机数据库后端，将给定的 kea 服务器配置为使用 Host Commands 高级钩子库（该库可从主机数据库中存储和获取主机预留的控制命令，若未加载 host\_cmds，平台将只显示配置文件中指定的主机预留）。

平台将定期从主机数据库后端获取预留信息，平台刷新信息的默认间隔时间为 60 秒，若需调整间隔时间，可在【配置】页面设置（请参阅“9.4 其他配置”

章节)。

## 4.5 租约搜索

1) 操作入口：登录平台后，点击【DHCP】一下拉列表点击【租约搜索】

2) 筛选条件：

① 筛选维度：在搜索框中，可通过 IP 地址、委托前缀、MAC 地址、客户端 ID、DUID、主机名等任意一项进行筛选。

筛选维度	示例
IP 地址	192.0.2.3
委托前缀	2001:db8::1
MAC 地址	01:02:03:04:05:06
DHCPv4 客户端 ID	01:02:03:04
DHCPv6 DUID	00:02:00:00:00:04:05:06:07
主机名	myhost.test.org

表 4-2 租约筛选条件示例

② 筛选格式：可带空格表示，如 01 02 03 04 05 06；可用十六进制数字表示法，如 010203040506；可用通用的 MAC 地址表示法，如 01:02:03:04:05:06

③ 不支持的筛选格式：目前不支持使用部分文本进行搜索，例如：只使用部分 IPv4 地址 192.0.2；除被拒状态的租约信息以外，其他状态也无法搜索到。

④ 如何搜索被拒状态的租约：要查找已拒绝的租约，请在搜索框中输入 state:declined





图 4-18 租约搜索

## 5 服务监控

### 5.1 模块简介

服务监控模块提供应用及服务器监控服务，以及高可用状态监控，其中【kea 应用监控】展示 kea 应用的相关信息，【服务器状态监控】展示监控的服务器的相关信息，【高可用监控】展示高可用运行状况。

### 5.2 kea 应用监控

操作入口：登录平台后，点击【服务监控】一下拉列表点击【kea 应用监控】

#### 5.2.1 查看 kea 应用基础信息

进入【kea 应用监控】页面，列表视图展示应用名称、运行状态及主机基础信息，点击左上角的【刷新列表】按钮或操作列的【刷新】按钮，可刷新应用状态。点击【重新同步 Kea 配置】，可获取所有服务器配置信息并更新到平台展示中。

点击目标 kea 应用，跳转至该 kea 应用的详情页，详情页会展示该应用的各

类守护进程（如 DHCPv4、DHCPv6、DDNS 及 Kea 控制代理 CA）。点击对应的守护进程标签页，可切换查看各类守护进程的具体信息。

DHCPv4、DHCPv6 中，点击【主机预留】，跳转至预留页面（请参阅“4.4.3 筛选主机预留”章节）；点击【子网】，跳转至子网页面（请参阅“4.2.4 查看子网”章节）；点击【共享网络】，跳转至共享网络页面（请参阅“4.3.4 查看共享网络”章节）；点击【全局配置】，跳转至 DHCP 参数和选项编辑页面；点击【原始配置】，可查看 JSON 格式的配置信息，点击【展开】按钮，可一键展开/折叠全部节点，点击【刷新按钮】，可实时拉取最新配置数据，点击【下载按钮】，将完整配置导出为文本文件。

DDNS、CA 中，点击【原始配置】，可查看 JSON 格式的配置信息。

此外，详情页中还展示了守护进程运行状况、钩子库信息、日志事件、数据存储信息、审查报告、高可用性等相关信息。

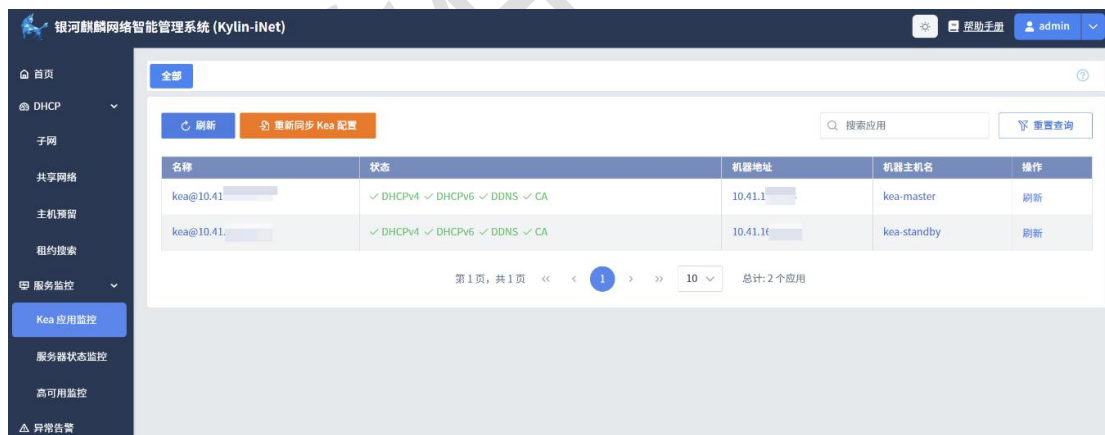




图 5-1 查看应用详细信息

## 5.2.2 修改应用名称

平台会为各应用分配默认名称，若需修改名称，在 kea 应用详情页，点击【重命名】按钮进入编辑模式，命名可参考以下方式：

① **默认命名格式**：[应用类型]@[机器地址]，若使用此格式，[机器地址]必须是本系统监控的机器的地址或 FQDN，否则，将会报错。

② **双@格式**：例如 dhcp@@machineX，此种情况下，machineX 可以不是系统中已有的主机，可以使用非主机名标识物理位置。

③ **自定义命名**：例如"Floor 1 DHCP"、"Floor 2 DHCP"，允许包含空格且无需遵循默认命名格式，无需包含@。



图 5-2 修改应用名称

### 5.2.3 查看日志记录

平台支持对 Kea 等监控应用的日志进行实时诊断。在日志记录器模块，展示以下信息：

- ① 日志记录器名称：标识日志来源模块（如"kea-dhcp4"）。
  - ② 类别：定义日志事件类别（如 INFO 表示信息同步、WARN 表示警告、ERROR 表示报错）。
  - ③ 输出位置：显示日志路径，点击可跳转至日志详情页查看完整日志记录。
- 在日志详情页里，点击左上角的【+】按钮，新增展示 4000 字符内容，点击【-】按钮，减少 4000 字符内容。

### 5.2.4 查看审查报告

由于 DHCP 服务器的参数配置较为复杂，误配置易导致服务异常或性能降低，所以平台通过配置检查器实现自动化配置诊断，标记潜在的配置问题，提供优化建议报告，以提升监控能力。

在 kea 应用详情页，下拉到【配置审查报告】模块，可查看具体报告信息。默认只展示有问题的报告，下方列表的蓝色标签展示具体的检查器名称，方便用户知晓具体是哪个配置维度有问题。若需查看所有报告，点击【检查器】旁的筛选按钮进行切换。

点击【检查器】，可设置各检查器，若不需要某些维度的审查，可禁用相关检查器。



图 5-3 查看审计报告

## 5.2.5 查看高可用性

在 kea 应用详情页，下拉到【高可用性】模块，可查看高可用详情。系统支持主备模式的高可用架构，当主节点发生故障时，从节点将成为新的主节点以保障服务持续可用。

点击左侧的下拉箭头，可展开高可用详细信息，可分别查看本机与伙伴节点的状态详情，涉及心跳状态、状态、作用域、状态时间、故障转移进度等。当节点间心跳通信中断超过最大心跳延迟阈值时，会显示故障转移进度信息；若启用了伙伴节点监控，会显示未确认客户端数（未能获取租约的客户端）、连接中的客户端数（尝试向伙伴节点申请租约的客户端）、已分析数据包数（用于诊断故障转移延迟的样本）。

更详细的高可用部署方案请参阅《银河麒麟网络智能管理系统 V2.0.0—高可用部署手册\_V2.0.0》。

高可用性	此服务器	伙伴服务器
Relationship #1	primary	standby 于 Kea@10.4
心跳状态	正常	正常
控制状态	未知	未知
状态	不可用	不可用
作用域	无	无
状态时间	2025-09-26 11:25:35	2025-09-26 11:25:38
状态时长	31 分钟前	31 分钟前
上次进入伙伴宕机状态时间	2025-09-25 20:06:57	2025-09-25 20:06:46
未确认客户端数	无可用信息	无可用信息
连接中的客户端数	无可用信息	无可用信息
已分析数据包数	无可用信息	无可用信息
故障转移进度	无	无
摘要	服务器未响应任何 DHCP 流量。	服务器未响应任何 DHCP 流量。

状态将在 1 秒后刷新。

图 5-4 查看高可用性

## 5.3 服务器状态监控

操作入口：登录平台后，点击【服务监控】—下拉列表点击【服务器状态监控】

### 5.3.1 查看服务器详情

进入【服务器状态监控】页面，列表视图展示主机名、位置、守护进程、CPU 数量、CPU 负载、总内存量、内存使用率、运行时间、错误信息等内容。

点击右上角的【刷新】按钮或操作列的【刷新机器状态信息】按钮，可刷新应用状态。点击右上角的【已授权】按钮，筛选展示该系统中已授权的机器。点击右上角的【未授权】按钮，筛选展示该系统中未授权的机器，即通过代理令牌方式注册的机器，在未授权机器中，点击操作列的【授权】，即可对该机器进行授权。

点击目标服务器，跳转至该服务器的详情页，详情页会展示该机器更多详细信息，例如 CPU、内存、内核信息等。



图 5-5 查看服务器列表详情

### 5.3.2 删除服务器

点击操作列的【删除】，将终止服务器与目标机器上运行的代理进程之间的连接，服务器将不再监控该机器。但代理进程仍会持续运行，要完全关闭代理进程，必须手动执行操作，例如可通过 SSH 连接到该机器并在机器端停止代理进程。

### 5.3.3 导出故障排查数据

为了有效诊断故障问题，系统收集了日志、配置文件、数据库信息等内容，并将其打包为 tar.gz 压缩文件。在服务器列表页面，点击操作列的【导出】，或者进入详情页，点击页面底部的【导出故障排查数据】按钮，均可下载压缩文件，可集中查看包括配置信息、日志片段、服务器设置、警告及错误事件、高可用性状态等内容。

## 5.4 高可用监控

操作入口：登录平台后，点击【服务监控】一下拉列表点击【高可用监控】

进入【高可用监控】页面，列表视图展示主机名、kea 应用、对应的 DHCP 服务、该主机的备节点、高可用心跳状态、控制状态、是否可用的状态、概况等



内容，便于用户快速了解高可用运行情况。



主机名	Kea应用	DHCP服务	备节点	心跳状态	控制状态	状态	概况
memfile-master	kea@10.44.1	DHCPv4	10.44.1	正常 ✓	未知 ○	不可用 ▲	服务器未响应任何 DHCP 流量。
memfile-master	kea@10.44.1	DHCPv6	10.44.1	正常 ✓	未知 ○	不可用 ▲	服务器未响应任何 DHCP 流量。
memfile-backup	kea@10.44.1	DHCPv4	10.44.1	正常 ✓	未知 ○	不可用 ▲	服务器未响应任何 DHCP 流量。
memfile-backup	kea@10.44.1	DHCPv6	10.44.1	正常 ✓	未知 ○	不可用 ▲	服务器未响应任何 DHCP 流量。

图 5-6 查看高可用监控详情

## 6 异常告警

### 6.1 模块简介

为提升网络稳定性、安全性和性能，系统加强了对 DHCP 异常情况的主动监控与处理，可提前预判风险，帮助用户快速定位问题，最小化故障影响。该模块提供详细的异常告警记录，涵盖 DHCP 服务状态监控、数据库状态监控、地址池利用率监控、高可用状态监控、租约冲突检测、高频请求检测、非法设备识别等方面。

### 6.2 异常告警规则

异常对象	异常类型	检测内容	规则
服务异常	agent 异常	agent 是否正常运行	服务停止判定为异常
	kea 应用异常	kea 应用 DHCPv4、DHCPv6、DDNS、CA 等进程是否正常运行	
	数据库异常	数据库主备节点是否正常运行	



地址池异常	高利用率	检测各子网各地址池的利用率阈值	利用率阈值 $\geq 90\%$ 后，利用率每上涨 1%，都会告警记录一次
租约异常	租约冲突	检测同一个 IP 地址是否重复绑定	<p>通过 ICMP Echo Request /Reply 机制来判断地址是否冲突。</p> <p>注：若某些设备不响应 ICMP Echo（ping）请求，默认的冲突检测机制就可能误判这些设备“未占用地址”，此时将不会有告警记录，从而误将已使用的 IP 地址重新分配给其他客户端，导致冲突</p>
请求异常	高频请求	检测某一时段内，相同 mac 发送的请求地址累积量级大于设定阈值	默认 1 分钟内，相同 mac 发送的请求地址累积量级 $\geq 50$
	非法设备	<p>检测 dhcp option 报文中带有的设备信息</p> <ul style="list-style-type: none"> <li>●Option 61（client id）：唯一标识客户端设备，如 mac 地址</li> <li>●Option 60（Vendor Class id）：标识设备厂商及型号</li> <li>●Option 1（Client Identifier）：设备唯一标识符，即客户端的 DUID</li> <li>●Option 16（Vendor Class）：标识厂商信息</li> </ul>	校验 option 60、61、1、16 中的信息是否合法，根据黑名单中的匹配规则进行匹配，匹配成功则认为是非法设备
高可用异常	心跳异常	监控高可用的心跳状态	丢包，服务中断即视为心跳异常
	服务切换	检测主备服务切换事件	监控到主备切换事件，进行通知：

			① 主机宕机 ② 备机接管 ③ 主服务恢复
	备节点异常	检测备节点运行状态	备节点异常时进行告警记录

表 6-1 异常告警规则说明

## 6.3 查看异常告警信息

操作入口：登录平台后，点击【异常告警】

在【异常告警】页面，可通过【告警日期】、【处理状态】、【推送状态】、【异常对象】、【异常类型】、【服务器】、【告警等级】进行筛选查看。

列表中展示具体的告警时间、告警等级、异常对象、异常类型、异常详情、异常持续时间、处理状态和推送状态信息。若检测到对应异常状态恢复正常，则【处理状态】更新为【已处理】。



告警ID	告警时间	告警等级	异常对象	异常类型	异常详情	异常持续时间	处理状态	推送状态
200	2025-09-22 11:18:25	紧急(p0)	服务异常	Kea应用异常	kea@10.41.1 的 DHCPv4 Daemon服务停止	5 m 42 s	已处理	未推送
199	2025-09-22 11:04:40	紧急(p0)	服务异常	Kea应用异常	kea@10.41.1 的 DHCPv4 Daemon服务停止	19 m 56 s	已处理	未推送
198	2025-09-22 11:04:10	紧急(p0)	服务异常	Kea应用异常	kea@10.41.1 的 DHCPv4 Daemon服务停止	4 m 12 s	已处理	未推送
197	2025-09-22 10:40:31	紧急(p0)	高可用异常	备节点异常	kea-standby@10.41.1 的主节点的 DHCPv6 正常, 备节点的 DHCPv6 异常	1 m 1 s	已处理	未推送
196	2025-09-22 10:40:31	紧急(p0)	高可用异常	备节点异常	kea-standby@10.41.1 的主节点的 DHCPv4 正常, 备节点的 DHCPv4 异常	1 m 1 s	已处理	未推送
195	2025-09-22 10:30:12	紧急(p0)	服务异常	Agent异常	kea-standby@10.41.1 的 stork-agent服务异常	3 m 53 s	已处理	未推送
194	2025-09-22 10:09:39	紧急(p0)	服务异常	Kea应用异常	kea-master@10.41.1 的 DHCPv6 Daemon服务停止	31 m 23 s	已处理	未推送
193	2025-09-22 10:09:39	紧急(p0)	服务异常	Kea应用异常	kea-master@10.41.1 的 DHCPv4 Daemon服务停止	31 m 23 s	已处理	未推送
192	2025-09-22 10:09:39	紧急(p0)	服务异常	Kea应用异常	kea-master@10.41.1 的 CA Daemon服务停止	31 m 23 s	已处理	未推送
191	2025-09-22 10:09:39	紧急(p0)	服务异常	Kea应用异常	kea-standby@10.41.1 的 CA Daemon服务停止	30 m 52 s	已处理	未推送

图 6-1 异常告警

## 7. 日志记录

### 7.1 模块简介

该模块提供详细的日志记录信息，汇总了系统操作日志、服务运行状态日志等内容。

### 7.2 查看日志信息

操作入口：登录平台后，点击【日志记录】

日志事件的等级涉及三类：信息（Info：信息提示，如用户登录、配置更改...）、警告（Warn：服务状态变更提示，如服务重启、服务禁用...）、错误（Error：报错提示，如服务失败、通信中断...）。

在日志页面，可按机器、守护进程、操作人、事件级别等维度筛选展示，并可点击链接跳转至对应详情页。

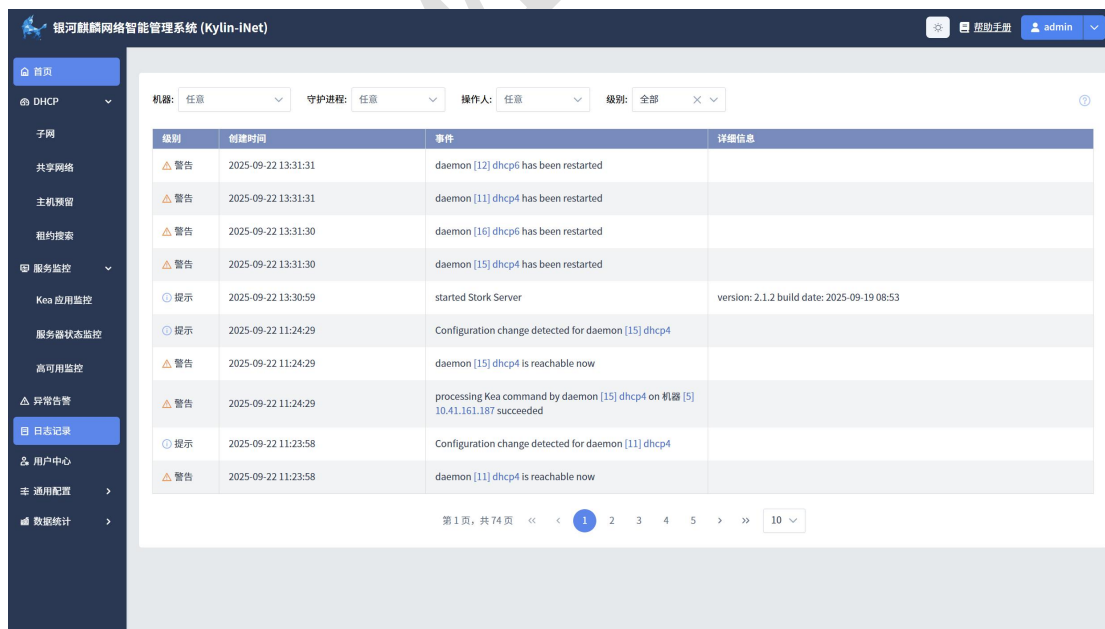


图 7-1 查看日志事件详情

## 8 用户中心

### 8.1 模块简介

该模块提供用户管理能力，可创建新账户，并管理所有用户信息。

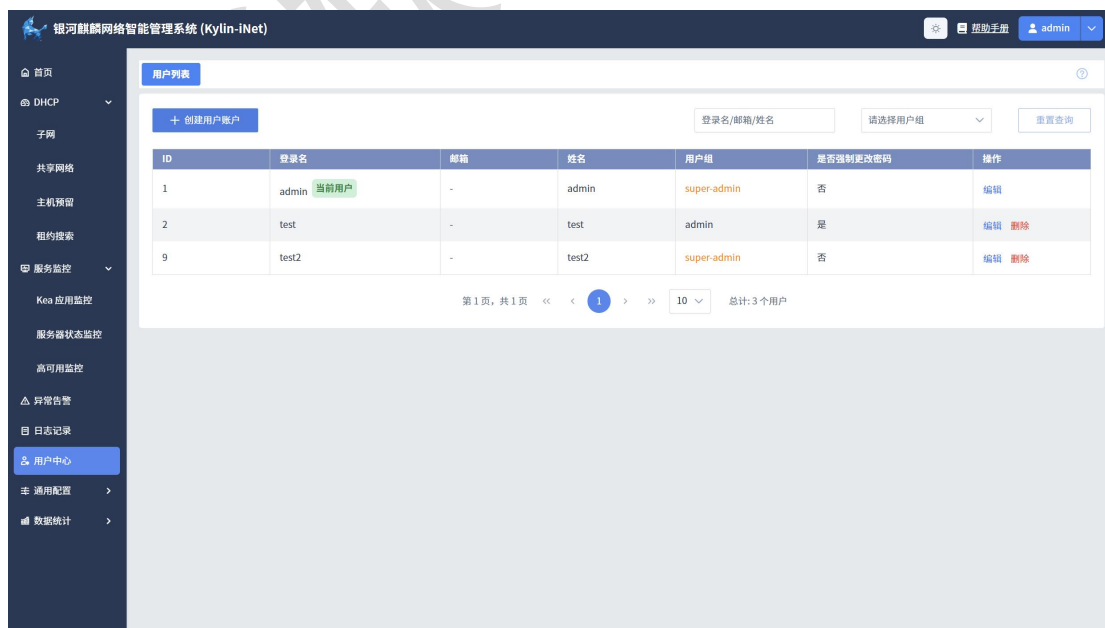
#### 8.2.1 新建用户

在【用户中心】页面，点击【创建用户账户】按钮，进入新建账户页面，必填项：用户登录名、姓名、用户组、密码（密码长度至少为 8 个字符）。

用户必须关联到对应的用户组。目前有两个可用组：超级管理员（super-admin）和管理员（admin）。属于超级管理员组的用户对系统拥有完全控制权，包括创建和修改用户账户。属于管理员组的用户具有类似的操作权限，但不允许创建和修改用户账户。

邮箱为可选项，但也建议填写，若填写了邮箱，用户可使用登录名或邮箱进行登录。

若勾选【强制更改密码】，则会要求用户登录后必须修改密码。



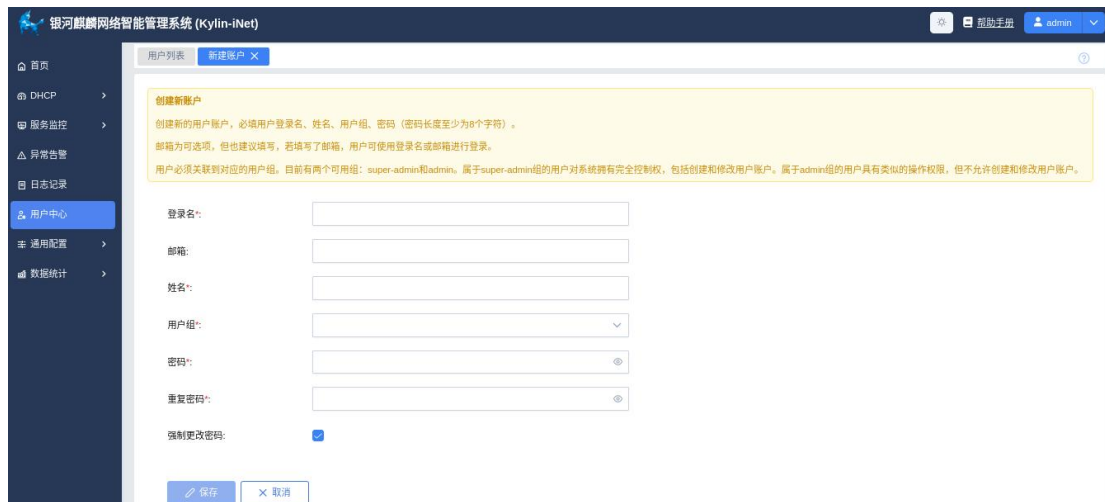


图 8-1 新建用户

## 8.2.2 编辑用户信息

在【用户中心】页面，点击【编辑】，可修改用户所有信息，例如用户组、密码等，保存时，若密码留空，则用户密码保持原密码不变。

在用户详情页，点击【删除】，可删除对应的用户账户。不过无法对当前账号进行编辑、删除。

# 9 通用配置

## 9.1 模块简介

该模块提供系统通用的配置能力，其中【审核检查器】显示各配置审查器状态及描述，用以分析守护进程配置，检查配置问题。【通信检测】展示服务通信状态，若通信有问题会在此进行详情展示。【其他配置】支持用户进行各类数据刷新时间的设置。

## 9.2 审核检查器

操作入口：登录平台后，点击【通用配置】—下拉列表点击【审核检查器】

DHCP 服务器的运行受到众多配置参数控制，若参数使用不当可能导致服务异常或服务器性能低下。通过配置审核检查器，可帮助识别服务器配置中的潜在问题。

该页面罗列了可用的审核检查器，每个检查器负责分析某一方面的配置问题，用于检查对应的配置。列表展示了检查器状态、名称、描述、选择器、触发器。

状态指示该检查器当前是禁用还是启用状态。若不需要某些维度的审查，可禁用对应的检查器。若有状态变更，必须点击【提交】按钮，以保存并生效变更。

选择器定义了其适用的守护进程类型：

选择器	适用进程
each-daemon	适用于所有类型的守护进程
kea-ca-daemon	适用于控制代理（Control Agents）
kea-dhcp-daemon	适用于 DHCPv4 和 DHCPv6 守护进程
kea-dhcp-v4-daemon	适用于 DHCPv4 守护进程
kea-dhcp-v6-daemon	适用于 DHCPv6 守护进程

表 9-1 选择器类型

触发器指示了触发该检查器的条件，目前有以下三种条件：

触发器	触发条件
manual	手动触发，即按用户请求执行
config change	检测到守护进程配置变更时触发
host reservations change	检测到主机预留数据库变更时触发

表 9-2 触发条件



注：选择器与触发器均无法由用户配置。

状态	名称	描述	选择器	触发器
Enabled	address_pools_exhausted_by_reservations	此检查验证 IP 池中的所有可用地址是否未被主机预留。	kea-dhcp-daemon	manual config change host reservations change
Enabled	agent_credentials_over_https	此检查验证当配置了 HTTP 身份验证凭据（即基本身份验证）时，麒麟 DHCP 代理是否使用 TLS 与 Kea 控制代理进行通信。	kea-ca-daemon	manual config change
Enabled	ca_control_sockets	此检查验证 Kea 控制代理配置是否包含控制套接字。	kea-ca-daemon	manual config change
Enabled	canonical_prefix	此检查验证子网前缀是否为规范形式。	kea-dhcp-daemon	manual config change
Enabled	dispensable_shared_network	此检查验证共享网络是否可以移除。	kea-dhcp-daemon	manual config change
Enabled	dispensable_subnet	此检查验证子网是否可以移除。当 host_cmds 钩子库已加载时，将跳过该检查项，因为数据库中可能存在主机预留项。	kea-dhcp-daemon	manual config change host reservations change
Enabled	ha_dedicated_ports	此检查验证高可用性的多线程模式是否与专用 HTTP 监听器一起启用，并且对方是否通过专用监听器公开的 HTTP 端口进行通信，而不是通过 Kea 控制代理。	kea-dhcp-daemon	manual config change
Enabled	ha_mt_presence	此检查验证当 Kea 以多线程模式运行时，高可用性钩子是否也以多线程模式运行。	kea-dhcp-daemon	manual config change
Enabled	host_cmds_presence	此检查验证当使用主机后端时，host_cmds 钩子库是否已加载。	kea-dhcp-daemon	manual config change
Enabled	lease_cmds_presence	此检查验证 lease_cmds 钩子库是否已加载。	kea-dhcp-daemon	manual config change
		当为左列主机配置钩子库时，请确保在配置钩子库时，钩子库已加载。		manual config change

图 9-1 查看审核检查器

## 9.3 通信检测

操作入口：登录平台后，点击【通用配置】一下拉列表点击【通信检测】

该页面展示服务通信状态。若有通信问题，会提示哪个机器、应用出现的具体通信问题是什么，并标有感叹号三角形图标，鼠标移至图标上可查看错误详情。

## 9.4 其他配置

操作入口：登录平台后，点击【通用配置】一下拉列表点击【其他配置】

关于安全设置，新服务器使用专用的 REST API 端点进行注册，并在已连接的服务器重新启动时，用相同端点重新注册这些机器。由于实际上不常注册新机器，因此可以禁用该选项以防止恶意注册虚假机器，而管理员可以在需要新注册时随时重新启用。

关于间隔设置，可以设置系统获取&刷新数据的时间间隔，即上一次尝试从



服务器获取特定信息到下一次尝试开始之间的时间段,刷新时间针对 agent 和 kea 生效。可设置的内容涉及:受监控机器上应用运行状态的刷新时间、获取主机预留信息的刷新时间、获取服务器状态信息的刷新时间、获取高可用性的刷新时间。

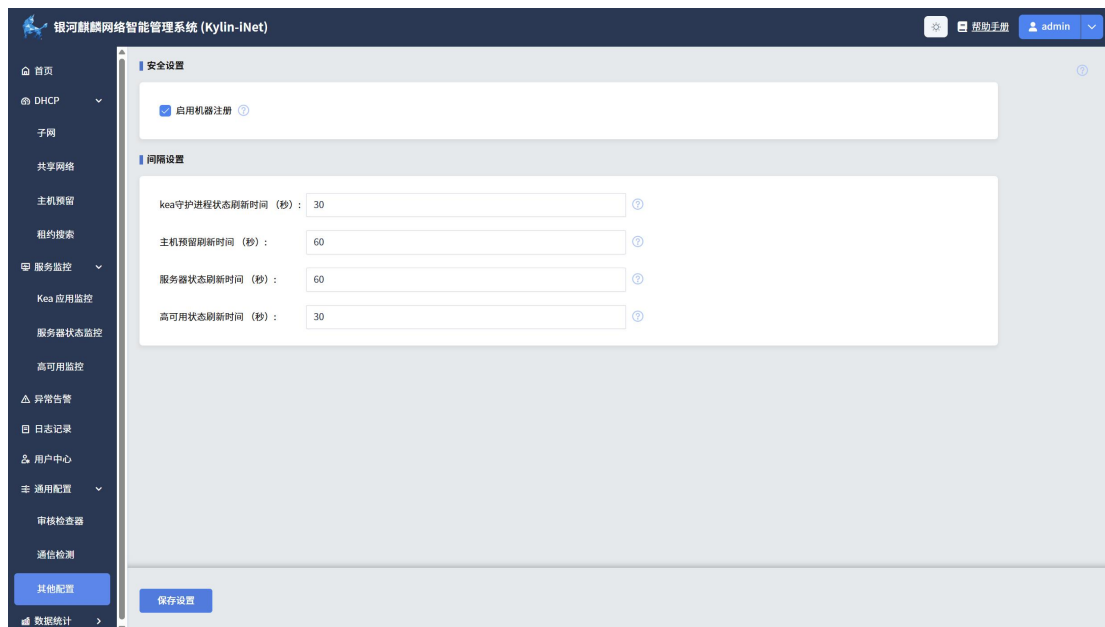


图 9-2 查看通用设置

## 10 数据统计

### 10.1 模块简介

该模块统计展示 DHCPv4、DHCPv6 的服务运行数据,用于量化评估 DHCP 服务在地址分配、地址利用等方面的实际表现。

### 10.2 DHCPv4 数据

操作入口:登录平台后,点击【数据统计】一下拉列表点击【DHCPv4】

筛选维度:可按服务器、子网筛选,也可选择具体时间范围(可快捷选择“最近 12 小时”、“最近 1 天”、“最近 7 天”、“最近 14 天”,也可自定义时间



范围，时间范围需 $\leq 90$ 天）。

可设置步长，查看不同时间粒度的数据情况。可自动刷新方式，用户停留在该页面时，将按设置的刷新方式来刷新数据。

在每个数据面板中，点击某图例，可只展示该图例对应子网的数据。

展示数据：地址池分配率（计算口径：已分配的地址量/地址池总量）、地址池拒绝率（计算口径：被拒绝的地址量/地址池总量）、地址池总量、被拒绝的地址总量、已分配的地址总量、已回收的过期地址总量等内容。



图 10-1 查看数据面板

### 10.3 DHCPv6 数据

操作入口：登录平台后，点击【数据统计】一下拉列表点击【DHCPv6】

操作要求与 DHCPv4 类似，请参阅 10.2 章节。

## 第三部分 重点场景操作说明



生产环境上所有配置请谨慎操作，建议测试环境验证无误后再上生产！

## 11 如何设置地址池范围

操作步骤：

登录平台后，点击【DHCP】—下拉列表点击【子网】—点击【新建子网】或者点击目标子网，进入子网详情页，点击【编辑】，可编辑更改地址池范围。

在具体的子网配置详情中，可设置该子网的地址池范围，每个子网可设置一个或多个地址池，填写地址范围（起始地址-结束地址），若存在多个 DHCP 服务器共享相同子网但配置不同地址池的情况，还需在对应地址池下选择 DHCP 服务器。

详细操作请参阅“4.2.1 新建子网”章节中的第四点“添加地址池”。

## 12 如何设置 DHCP option

操作步骤：

①子网操作：登录平台后，点击【DHCP】—下拉列表点击【子网】—点击【新建子网】或者点击目标子网，进入子网详情页，点击【编辑】，下拉至 DHCP 选项模块，可编辑更改 DHCP 选项。勾选【分开设置各服务器选项】即可针对每个服务器单独设置 DHCP 选项，并为不同服务器指定各自的选项集合。

②共享网络操作：登录平台后，点击【DHCP】—下拉列表点击【共享网络】或者点击目标共享网络，进入共享网络详情页，点击【编辑】，下拉至 DHCP 选项模块，可编辑更改 DHCP 选项。

DHCP 选项面板用于定义向子网内客户端返回的特定 DHCP 选项。通常情况下，分配给同一子网的不同服务器会采用相同的选项配置。也可勾选【分开设置

各服务器选项】，即可针对每个服务器单独设置 DHCP 选项，并为不同服务器指定各自的选项集合。

详细操作请参阅“4.2.1 新建子网”章节中的第五点“填写 DHCP 选项”以及“4.3.1 新建共享网络”章节。

## 13 如何设置 DHCP 参数

### 13.1 操作步骤

①子网操作：登录平台后，点击【DHCP】一下拉列表点击【子网】再点击【新建子网】或者点击目标子网，进入子网详情页，点击【编辑】，下拉至 DHCP 参数模块，可编辑更改 DHCP 参数。

②共享网络操作：登录平台后，点击【DHCP】一下拉列表点击【共享网络】或者点击目标共享网络，进入共享网络详情页，点击【编辑】，下拉至 DHCP 参数模块，可编辑更改 DHCP 参数。

详细操作请参阅“4.2.1 新建子网”章节中的第四点“填写 DHCP 参数”以及“4.3.1 新建共享网络”章节。

### 13.2 具体参数介绍


#### 13.2.1 Allocator

在分配 IPv4、IPv6 地址时，会优先分配客户端明确请求的特定地址、为客户端预留的地址。若客户端未请求特定地址且无预留 IP，或请求地址被其他客户端占用时，服务器应在地址池中寻找其他可用地址进行分配。Allocator 就是负


责此类情况下的地址分配任务。

目前有三类分配机制：iterative、random、flq(Free Lease Queue)


**Iterative：**迭代分配，系统会记录最后一个已分配的 IP 地址，随后对下一客户端分配该地址的连续递增值，例如：分配顺序为：192.0.2.10 → 192.0.2.11 → 192.0.2.12 依此类推。由于地址查找与分配耗时极短，当地址池利用率较低且下一个地址大概率可用时，此机制可达到最优性能表现。

 注：该机制会导致一个问题：在多个服务器共享租约数据库的场景下，各服务器可能会独立为不同客户端分配相同地址，导致跨服务器的地址分配出现冲突，而 random 机制可缓解该问题。

**Random：**随机分配，适用于多个服务器共享租约数据库的场景，可最大程度降低在相同时间或接近的时间段内为不同客户端分配相同地址的风险，此外，由于地址分配随机、不可预测，该机制能有效抵御基于地址分配规律发起的攻击。

 注：Random 机制的运行效率略低于 Iterative，同时，因为系统需记录已随机分配的地址，内存消耗会增加。

**FLQ：**建议在地址池利用率极高的子网环境中部署使用。当子网地址池接近耗尽时，Random 或 Iterative Allocator 需要反复校验拟分配地址是否存在有效租约，可能导致寻址耗时显著增加。极端情况下（例如：地址池完全耗尽），校验次数会达到子网地址总量级别，这将导致每个 DHCP 请求的响应时间延长。FLQ 通过动态追踪租约状态（持续移除已分配租约、添加释放或回收的租约），为每个地址池维护实时可用的空闲地址列表。该机制能够在恒定时间内获取可用地址，完全规避地址池利用率对分配效率的影响。

 注：FLQ 会显著增加服务器启动及配置重载时间，其内存消耗也会随所管理的地址池总容量而增加，所以需预留足够内存资源来维护空闲地址列表；此外，必须启用租约回收功能，并将 reclaim-timer-wait-time 参数设置为较低值，确保服务器可以高频回收过期租约至空闲地址列表（过期租约在未被服务器回收前不会被 FLQ 识别为可用地址）。

项目	地址池低利用率性能表现	地址池高利用率性能表现	是否随机分配租约	启动及配置重载效率	内存消耗
Interative	非常高	低	否	快	低
Random	高	低	是	快	高
FLQ	高	高	是	慢	高

表 13-1 分配机制的性能表现对比

### 13.2.2 Authoritative

当 authoritative 设置为“true”时，服务器将对未知客户端的 INIT-REBOOT 请求统一返回 DHCPNAK 应答。该参数可在全局、共享网络和子网层级设置，未明确指定时将自动继承上级作用域的配置。同一共享网络内的所有子网必须采用相同的 authoritative 配置。

### 13.2.3 Cache Max Age & Cache Threshold

客户端在短时间内发起多次续租请求时，会导致服务器频繁执行租约更新及数据库写入操作，引发服务器性能损耗。通过设置缓存参数，限定租约更新频率。缓存阈值（cache-threshold）与缓存最大时效（cache-max-age），均无默认值，

用户可自行设置。这两个参数可在全局、共享网络和子网层级设置，优先级为：  
子网层级配置 > 共享网络层级配置 > 全局配置（兜底策略）。

cache-max-age：若配置该参数，则与租约已持续时间比对，超期租约不可复用。若将 cache-max-age 设为 0，租约缓存功能将被禁用。

cache-threshold：配置取值在 0.0-1.0 之间，租约已持续时间需小于等于 valid lifetime 乘以该阈值比例。注：该参数值  $\leq 0.0$  或  $> 1.0$  时，租约缓存功能将被禁用。

示例：设置 valid-lifetime=2000，cache-threshold=0.25，cache-max-age=600。  
若租约有效时间为 2000 秒，可复用的最大时间为 600 秒，复用阈值为 500 秒（ $2000 \times 0.25$ ，即若租约持续时间未超过 500 秒，则可复用该租约）

#### 13.2.4 租约相关参数

参数	含义	必选/可选	注意事项
Preferred lifetime	默认首选租期	DHCPv6 的必选配置，DHCPv4 无此配置	若未设置 preferred lifetime 参数值，或其设定值 $> \text{valid lifetime}$ 时，服务器将按照 $\text{valid lifetime} \times 0.625$ 作为分配基准。
Min preferred lifetime	首选租期最小值	DHCPv6 的可选配置，DHCPv4 无此配置	/

Max preferred lifetime	首选租期最大值	DHCPv6 的可选配置，DHCPv4 无此配置	/
Valid lifetime	默认有效租期，定义了服务器分配 IP 地址的租约有效时间	DHCPv4/v6 必选配置	填写整数数值
Min valid lifetime	有效租期最小值	DHCPv4/v6 可选配置	/
Max valid lifetime	有效租期最大值	DHCPv4/v6 可选配置	/
Renew timer	指定 T1(续租时间)的值(以秒为单位)	DHCPv4/v6 可选配置	<p>若设置 T1，必须满足 <math>T1 &lt; T2</math>。</p> <p>若 T1 配置值大于 T2，服务器在发送 IA 选项中将默认 <math>T1=0</math></p> <p>这种灵活配置的方式可能让 T1、T2 超出租约期限，导致租约直接过期而未产生续租行为。</p>

Rebind timer	指定 T2(重新绑定时间) 的值 (以秒为单位)	DHCPv4/v6 可选配置	<p>推荐配置原则：<math>T1 &lt; T2 &lt; \text{preferred lifetime} &lt; \text{valid lifetime}</math></p> <p>自主续租模式:若配置 <math>T1=T2=0</math>，客户端可自主决定续租时间。注意：若需设置 <math>T1=T2=0</math>，必须先进行测试，需验证客户端实现是否合规，已知部分缺陷客户端可能会立即触发续租。</p>
Calculate tee times	启用该参数时(默认值 true)，T1 与 T2 基于有效租约时间的百分比计算生成	DHCPv4/v6 可选配置	DHCPv6 默认启用 calculate tee times，以确保向客户端发送非零的 T1/T2
T1 percent	定义 T1 占有效租约时间的百分比值	DHCPv4/v6 可选配置	<p>范围：0.0–1.0，必须小于 T2 percent。</p> <p>默认值：DHCPv6 的默认值为 0.5；DHCPv4 的默认值为 0.5</p>



T2 percent	定义 T2 占有效租约时间的百分比值	DHCPv4/v6 可选配置	范围：0.0–1.0，必须大于 T1 percent。  默认值：DHCPv6 的默认值 0.8；DHCPv4 的默认值为 0.875
------------	--------------------	----------------	---

若客户端请求值超出边界范围时，则按需向上或向下取整至最近的有效值：

- 请求值 < 最小值 → 采用最小值
- 请求值 > 最大值 → 采用最大值
- 请求值介于最小/最大值之间 → 采用请求值
- 若未指定请求值 → 采用默认值

确定最终生效的租期时间的优先级逻辑如下图所示：

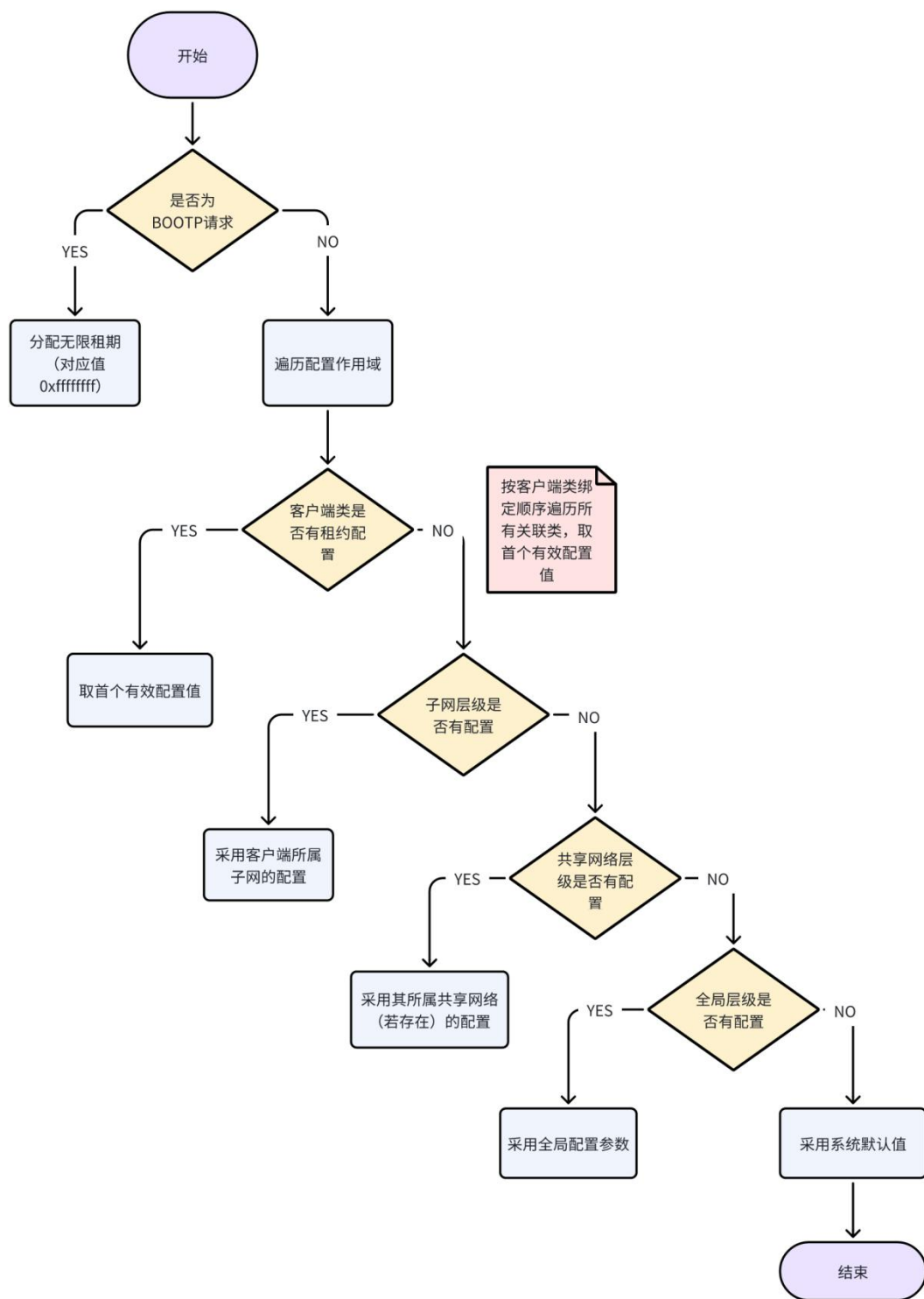


图 13-1 租期优先级流程图

### 13.2.5 DDNS 相关参数


DHCP-DDNS 服务器（简称 D2）代表 DHCPv4 和 DHCPv6 服务器执行 DDNS 协议。其工作流程如下：

DHCP 基于地址租约变更事件生成 DDNS 更新请求（NameChangeRequests (NCRs)），并将这些请求提交至 D2 处理。D2 执行智能路由匹配，将每个请求关联至对应的 DNS 服务器。D2 为准确路由 DNS 更新请求，需维护两类域名解析目录：正向 DNS 域名列表与反向 DNS 域名列表（统称“DDNS 域名列表”）。

#### ① 正向域名匹配机制：

D2 采用最长前缀匹配方式，将请求中的 FQDN 与正向域名列表进行逐级比对。


例如：当 FQDN 为 "myhost.sample.example.com." 时，若存在 "sample.example.com." 和 "example.com." 两个正向域名，系统将选取 "sample.example.com." 作为最优匹配

 注：若无法匹配有效域（如 FQDN 为 "bogus.net" 而列表仅含上述两项），请求将被拒绝。若未配置正向域列表，D2 将自动忽略请求中的正向更新操作。

#### ② 反向域名匹配机制：

D2 根据租约地址构造反向 FQDN，执行逻辑与上述逻辑一致。

例如：租约地址“172.16.1.40”，对应的反向 FQDN 为 "1.16.172.in-addr.arpa."，若存在 "1.16.172.in-addr.arpa." 和 "16.172.in-addr.arpa" 两反向域名，系统将选择 "1.16.172.in-addr.arpa." 作为最优匹配。

 注：当租约地址无法匹配反向域（如 192.168.1.50 与上述两项不匹配）时，

请求将被拒绝。若未配置反向域列表，D2 将自动忽略请求中的反向更新操作。

参数	含义	说明
DDNS Send Updates	DDNS 启用更新	<p>1. 该参数决定在给定层级（全局、共享网络、子网）是否启用 DDNS 更新。</p> <p>2. 即使 DDNS Send Updates 为 “false”，影响 FQDN 的参数仍会生效，以支持由客户端自行负责 DNS 更新的环境（参数包括：DDNS Replace Client Name、NNDS Generated Prefix、DDNS Qualifying Suffix、Hostname Char Set、Hostname Char Replacement）。</p> <p>3. 通常在以下场景生成 DDNS 更新请求：</p> <ul style="list-style-type: none"> <li>① 响应 DHCPREQUEST 分配新租约。</li> <li>② 续期现有租约但关联的 FQDN 发生变更：该场景下，会生成两个 DDNS 请求，第一个用于删除旧 FQDN 的 DNS 条目，第二个用于添加新 FQDN 的 DNS 条目。</li> <li>③ 响应 DHCPRELEASE 释放现有租约：仅生成一个 DDNS 请求以删除相关条目。</li> </ul>
DDNS Override No Update	DDNS 覆盖无更新请求	<p>当该参数设为 true 时，即使客户端要求不进行更新，服务器仍会生成 DDNS 更新请求。</p>

DDNS Override Client Update	覆盖客户端更新	<p>客户端委托场景下，客户端声明其将自行执行正向 DNS 更新，并要求服务器处理反向 DNS 更新。通常情况下，服务器会遵循客户端意愿，仅生成用于更新反向 DNS 数据的 DDNS 请求。</p> <p>但是当 DDNS Override Client Update 参数设为 true 时，服务器会忽略客户端委托要求，生成同时更新正向和反向 DNS 数据的 DDNS 请求。</p>
DDNS Replace Client Name	替换客户端名称	<p>该参数支持以下三种行为模式：</p> <p>① never（永不替换）</p> <p>使用客户端提供的名称，若客户端未提供名称，则不生成名称。此为默认模式。</p> <p>② always（始终替换）</p> <p>替换客户端提供的名称。若客户端未提供名称，则为其生成一个名称。</p> <p>③ when-not-present（不存在时生成）</p> <p>使用客户端提供的名称。若客户端未提供名称，则为其生成一个名称。</p>
DDNS Generated Prefix	DDNS 生成前缀	<p>生成 FQDN 时使用的前缀由 DDNS Generated Prefix 参数指定。默认值为“myhost”。</p>

DDNS Qualifying Suffix	DDNS 限定 后缀	<p>1. 生成完整 FQDN 或补全名称时使用的后缀由 DDNS Qualifying Suffix 参数指定。建议在启用 DDNS 更新时配置此参数。该参数无默认值。</p> <p>2. 当需补全名称时，按以下格式生成名称： [candidate-name].[ddns-qualifying-suffix].</p> <p>其中[candidate-name]为 DHCPREQUEST 提供的名称。例如，若 candidate-name 为“some-computer”且 DDNS Qualifying Suffix 设为“test.com”，则生成的 FQDN 为：some-computer.test.com.</p> <p>3. 当需生成完整名称，按以下格式生成名称： [ddns-generated-prefix]-[address-text].[ddns-qualifying-suffix].</p> <p>其中[address-text]为 IP 地址的字符串。例如，若 IP 为“172.16.1.10”（IPv4）、“3001:1::70E”（IPv6），后缀设为“test.com”且使用默认前缀“myhost”，则生成的 FQDN 为： myhost-172-16-1-10.example.com. （IPv4）、 myhost-3001-1--70E.test.com.（IPv6）。</p>
DDNS Update On Renew	DDNS 续约 更新	<p>若该参数设置为 true，服务器在每次租约续期时都会强制更新 DNS 信息，即使 DNS 信息未发生任何</p>

		<p>变化。不过这可能会影响系统性能，特别是在有大量频繁续期客户端的情况下，更易影响性能。</p>
DDNS Conflict Resolution Mode	DDNS 冲突解决模式	<p>该参数提供四种模式选项：</p> <p>① check-with-dhcid</p> <p>此为默认模式，指示 D2 执行符合 RFC 4703 标准的冲突解决。仅当现有 DNS 条目包含 DHCID 记录且与客户端的 DHCID 匹配时，才允许覆盖该条目。</p> <p>② no-check-with-dhcid</p> <p>允许任意客户端覆盖现有 DNS 条目（无论这些条目是否包含 DHCID 记录）。新条目将包含所属客户端的 DHCID 记录。</p> <p>③ check-exists-with-dhcid</p> <p>仅当现有 DNS 条目包含 DHCID 记录时才允许覆盖（无需与客户端的 DHCID 匹配）。此模式可保护静态 DNS 条目（不含 DHCID 记录的条目），同时允许动态条目（含 DHCID 记录的条目）被任意客户端覆盖。</p> <p>④ no-check-without-dhcid</p> <p>允许任意客户端覆盖现有 DNS 条目，且新条目不包含 DHCID 记录。</p>

Hostname Char Set	主机名字符集	<p>1. 可能存在以下场景：客户端在主机名或 FQDN 中提供包含非法字符的值。针对该情况，可利用 Hostname Char Set 和 Hostname Char Replacement 两个参数进行处理。</p> <p>2. 最常见的应用场景是确保仅包含 RFC 1035 允许的字符（A-Z、a-z、0-9、“-”）。</p> <p>3. Hostname Char Set 描述非法字符集的正则表达式，遵循 POSIX 扩展正则表达式语法。空字符（0x00）会被视为非法字符并会被替换或删除。该参数的默认值为 “^A-Za-z0-9.-”。即匹配任何非字母、数字、点号、连字符或空字符的字符。</p>
Hostname Char Replacement	主机名字符替换	<p>1. 该参数用于设置替换主机名中非法字符的字符串（可为空），若为空字符串，非法字符将被直接删除。默认值为空字符串 “ ”。</p> <p>示例：Hostname Char Set 默认为 “^A-Za-z0-9.-”，若 Hostname Char Replacement 设为 “x”，那么“x”会替换所有非字母、数字、点号或连字符的字符。客户端提供的名称 “myhost-\$(123.org”，将被替换为 “myhost-xx123.org”。</p> <p>2. 若客户端发送的名称仅非法字符有差异（例如</p>



		“host-1[” 和 “host-1#” )，替换后将生成相同名称(都更改为 “host-1” ), 这种情况下仅允许其中一个客户端注册该名称。
--	--	---

### 13.2.6 Client Class

客户端在多维度上均有差异，例如客户端在网络拓扑结构中的差异，客户端行为模式的差异（例如智能手机与笔记本电脑的操作差异）、客户端所需特定参数配置的差异。

为了提升管理效率，可将具有相同属性的客户端划分为统一的客户端类别，以实现配置参数的批量管理。传入数据包与客户端类的关联方式涉及下述四种方式：基于厂商关联；基于逻辑表达式关联；基于主机预留、共享网络、子网等固定配置关联；基于钩子库进行自定义关联。

客户端分类可在下述场景中发挥作用：

报文过滤、子网选择、地址池选择、租约限制、流量速率控制、DDNS 优化配置、TFTP 服务器地址与启动文件字段的定向设置。

### 13.2.7 Four Over Six Interface 相关参数

DHCPv4-over-DHCPv6 传输机制由 RFC 7341 定义，需通过 DHCPv4 与 DHCPv6 服务器协同实现。以下任意一项参数存在都可使子网与 DHCPv4-over-DHCPv6 一起使用：

① 4 over 6 subnet：采用与源地址匹配的前缀（例如 IPv6 地址，其后跟斜线和前缀长度，“2001:db8:1:1::/64”）

② 4 over 6 interface id: 获取中继接口 ID 选项值

③ 4 over 6 interface: 获取与传入接口名称匹配的接口名称

### 13.2.8 Interface

服务器网络接口配置说明: DHCPv4/v6 服务器必须配置为在特定网络接口上监听。基础配置逻辑如下:

① 全局监听模式: 使用通配符 “\*” , 能监听所有可用接口。

② 混合配置模式: 同时使用通配符 “\*” 与明确的接口名称。只有当需要临时覆盖接口名称列表并监听所有接口时, 才应用该模式。例如: interfaces: eth1, eth3, \*

③ 多地址监听模式: 某些场景下, 需要监听配置了多个 IP 地址的接口, 可在接口名称后附加对应 IP 地址, 例如: interfaces: eth1/10.0.0.1, eth3/192.0.2.3

关于 Interface, 有两个参数可以配置:

① Interface: 定义哪个本地网络接口可用于访问给定子网 (用于本地直接流量)

② Interface ID: 指定中继设备使用的 interface-id 选项值, 以标识中继上发送响应包的接口 (用于中继流量)

这两个参数是相互排斥的, 子网不能同时通过本地和中继访问。同时配置会报错, DHCPv6 服务器会拒绝这样的配置。

### 13.2.9 Next Server

某些场景下, 客户端在获取 IP 地址后, 仍然需要其他配置参数, 若客户端需要通过 TFTP 服务器获取配置文件, 可填写下述字段:

下一个服务器（Next Server）、服务器主机名（Server Hostname）、指定引导文件名（Boot File Name）

这些配置既可在全局作用，也可限定某特定子网，当同时存在全局和子网层级的配置时，子网配置的优先级高于全局配置。若将子网层级的值设为“0.0.0.0”，则表示不向客户端发送该字段；若设为空字符串，则表示未定义子网层级的配置，此时将自动继承全局配置。

### 13.2.10 Relay Addresses

对于中继流量（Relayed Traffic），通常使用中继代理地址来选择子网。如果子网是独立使用的（未在共享网络中分组），则可以为每个子网指定不同的中继地址。若多个子网属于同一个共享网络，必须通过相同的中继地址进行选择（注：为共享网络中的各个子网指定不同的中继地址会报错）。最好是在共享网络级别指定中继地址，共享网络的所有子网会自动继承该值。

### 13.2.11 Reservation 相关参数

子网的部分地址范围被划分为动态池用于动态分配，主机预留可为特定客户端预留子网内的任意地址，若预留地址位于动态池内，则为池内预留（In-Pool Reservations），若预留地址位于子网内但不属于动态池，则为池外预留（Out-of-Pool Reservations）。目前预留有三种模式，全局预留 Reservations Global、子网预留 Reservations In Subnet、池外预留 Reservations Out Of Pool。


① **Reservations Global 参数：**该参数默认为“false”。在移动网络等部署场景中，客户端可能需要跨子网漫游，此时需确保特定参数的全局可用性。全局预留机制可满足该场景需求，可以在启用了“Reservations Global”的每个子网中使用，为跨子网漫游客户端保留主机名（常规的主机预留：绑定至特定子网 ID，

仅在该子网生效)。

全局预留地址必须在服务器为客户端选择的子网范围内, 否则地址将被忽略, 同时服务器会尝试动态分配地址。若所选子网属于某共享网络, 服务器将检查该地址在其兄弟子网中的有效性, 选择首个符合条件的子网, 若没有子网符合条件, 服务器会回退至动态地址分配。

② **Reservations In Subnet 参数:** 默认 “true”, 启用于网级地址池内主机预留功能。此模式执行全量检查, 安全性最高但性能影响最大, 此外该模式不涉及全局预留检查。

③ **Reservations Out Of Pool 参数:** 默认为 “false”, 仅允许动态地址池外的预留地址。此模式假设所有预留地址均不在动态池内, 可跳过池内地址的检查以提升性能。若存在池内地址预留配置时严禁启用此模式。

 注: 若同一客户端同时存在两种配置时, 子网预留的优先级高于全局预留。以上参数配置错误可能引发地址冲突, 建议生产环境启用前先严格校验预留地址与动态池的包含关系, 测试环境验证无误后再部署。

### 13.2.12 Store Extended Info

为支持租约查询等功能, 需为每个租约存储额外信息, 由于租约存储的信息量会影响系统性能与资源消耗, 可通过 Store Extended Info 参数控制该附加信息的存储, 此参数默认值为 “false”, 可在全局、子网层级、共享网络层级进行配置。若参数设为 “true”, 与请求租约 DHCPREQUEST 相关的信息将添加到租约的 user-context 中。

## 14 如何设置租约参数

操作步骤：

①子网操作：登录平台后，点击【DHCP】—下拉列表点击【子网】—点击【新建子网】或者点击目标子网，进入子网详情页，点击【编辑】，下拉至 DHCP 参数模块的【租约参数】部分，其中“Valid Lifetime”设置租约时长，“T1 Percent”、“T2 Percent”设置续约进程，当租期达到 X%（T1）时，客户端以单播方式向服务器请求更新租约，当租期达到 Y%（T2）时，若仍未收到服务器应答，客户端以广播方式请求更新租约(更多信息请参阅“13.2.3 租约相关参数”章节)。

②共享网络操作：登录平台后，点击【DHCP】—下拉列表点击【共享网络】或者点击目标共享网络，进入共享网络详情页，点击【编辑】，下拉至 DHCP 参数模块，参数设置同上。

## 15 如何检查冲突地址

操作步骤：

登录平台后，点击【DHCP】—下拉列表点击【主机预留】—勾选【冲突】复选框，单击该框一次，结果将显示配置文件与主机数据库之间存在配置冲突的主机信息，再次单击，筛选结果将排除存在配置冲突的主机。

## 第四部分 参考手册

序号	交付物名称	内容描述
1	银河麒麟网络智能管理系统 V2.0.0—产品安装部署手册	安装部署指南

	_V2.0.0	
2	银河麒麟网络智能管理系统 V2.0.0—产品手册_V2.0.0	产品说明手册
3	银河麒麟网络智能管理系统 V2.0.0—Kea-DHCP 安装使用手册_V2.0.0	kea 安装部署指南
4	银河麒麟网络智能管理系统 V2.0.0—Stork 安装手册_V2.0.0	stork 安装部署指南
5	银河麒麟网络智能管理系统 V2.0.0—高可用部署手册_V2.0.0	高可用安装部署指南
6	银河麒麟网络智能管理系统 V2.0.0—kea 配置说明手册_V2.0.0	后台服务配置文件指南
7	银河麒麟网络智能管理系统 V2.0.0—交付物料清单_V2.0.0	物料清单列表

## 第五部分 附录

### 16 术语解释

术语（中文）	术语（英文）	含义
子网	Subnet	子网是 DHCP 配置中的一个逻辑单元，对应一个物理或逻辑网络段。
共享网络	Shared Networks	共享网络是一个逻辑容器，允许将多个子网组合在一起，共享某些配置或资源。适用于同一物理网络中存在多个逻辑子网的情况。
应用	App	通过 DHCP 代理组件进行监管的程序实例，在部署场景中，此类实例通常指已集成的网络服务组件（如 DHCP 服务器），一个应用实例可聚合多个独立守护进程，如：包含 DHCPv4 守护进程和 DHCPv6 守护进程。
守护进程	Daemon	守护进程是一种在后台持续运行的特殊进程，用于执行特定的系统任务，通常在系统启动时自动

		<p>启动。</p> <p>在该系统中，守护进程属于应用中的一个程序，例如 DHCPv6 守护进程。</p>
机器/主机	Machine	运行 agent 并与服务器通信的物理或虚拟系统。
已授权机器	Authorized Machine	运行代理的机器已请求在服务器上注册,并在 web 平台上得到管理员的批准授权。
未授权机器	Unauthorized Machine	运行代理的机器已请求在服务器上注册,但在 web 平台上还未得到管理员的批准授权。
全局配置	Global Configuration	配置的一组参数，适用于给定服务器上的所有子网、共享网络或主机预留。
高可用	High Availability (HA)	高可用是一种故障恢复机制，目的是保障业务的连续可用。通常至少需要两个节点，若其中一个节点发生故障，另一个节点可无缝接管。
钩子库	Hook Library	<p>钩子库是一种编程工具集，其核心功能是通过事件拦截与行为注入机制，在相关执行点插入自定义代码，实现系统的动态功能扩展。</p> <p>在本系统中，利用钩子库扩展 DHCP 服务器功能，提供更详细诊断或更多操作控制，例如 subnet_cmds 钩子库可管理具体子网。</p>
主机预留	Host Reservation	<p>主机预留是一种实现 IP 资源精准分配的机制，通过硬件标识符将特定 IP 地址与终端设备绑定，确保相关设备在动态地址分配中可获取固定的网络配置。</p> <p>预留的地址将不参与常规的动态地址分配。</p>