



APV 10.4.3

命令行使用手册

北京信安世纪科技股份有限公司

二零二五年

版权声明

©2025 北京信安世纪科技股份有限公司 版权所有

本文档受版权保护，未经信安世纪许可，任何人不得以任何理由和形式使用、复制、传播和编辑本文档，除非是在版权法的许可范围内。

本手册所涉及的案例均是当前情况，信安世纪有权利随时更改，恕不提前通知。对于本手册内容，包括但不限于隐含的商业性能和特定用途适应性说明，信安世纪不承担任何责任。

如因本手册的描述造成设备性能、使用和按键操作问题，进而引发相关事故并造成损失的，信安世纪不承担任何责任。



警告：未经信安世纪许可，任何人不得对信安世纪 APV 设备进行任何改动，否则将无权继续使用该设备。

商标声明

本手册中所涉及的产品名称仅作识别之用。手册中涉及的其他公司的注册商标或版权属各商标注册人所有，恕不逐一系列明。

合格声明

信安世纪自主声明信安世纪 APV 系列产品符合 FCC 规范第 15 部分的规定。操作本设备需要满足以下条件：（1）本设备不会产生有害干扰，（2）本设备必须能够接受收到的所有干扰，包括可能导致意外操作的干扰。

关于信安世纪

北京信安世纪科技股份有限公司（股票代码：688201）成立于 2001 年 8 月，是一家科技创新型信息安全产品和解决方案提供商。公司以密码技术为基础支撑，致力于解决网络环境中的身份安全、数据安全、通信安全、移动安全、云安全和平台安全等信息安全问题，为金融、政府和企业等重要领域的核心业务系统提供先进的产品与解决方案，充分满足各类计算架构和应用场景下客户对新安全的需求，实现新业态与密码技术的深度融合。

联系信安世纪

请通过以下方式联系信安世纪：

- 官方网站：<https://www.infosec.com.cn/>
- 电子信箱：support@infosec.com.cn
- 地址：北京市海淀区建枫路（南延）6 号西三旗金隅科技园 2 号楼信安大厦
- 邮编：100096
- 电话：010-68025518、4006705518
- 电话联系时间：周一至周五早 9 点至晚 6 点

目录

版权声明.....	I
商标声明.....	I
合格声明.....	I
关于信安世纪.....	II
联系信安世纪.....	II
目录.....	III
第 1 章 命令行介绍.....	1
1.1 命令行符号含义.....	1
1.2 正则表达式.....	1
1.3 登录设备.....	3
1.4 访问控制的级别.....	3
1.5 命令行快捷键.....	5
第 2 章 基本系统配置.....	6
2.1 网站分类.....	39
2.2 网桥.....	40
2.3 端口镜像.....	42
2.4 系统健康检查.....	46
第 3 章 高级系统配置.....	58
3.1 LLDP.....	77
3.2 IP 域表.....	80
3.2.1 IP 域表通用命令.....	80
3.2.2 基于 GeoIP 的 IP 域表.....	82
3.3 VXLAN.....	92
第 4 章 链路聚合.....	98
第 5 章 集群.....	100
第 6 章 高可用性（HA）.....	108
6.1 HA 节点.....	108

6.2 HA 链路.....	109
6.3 浮动 IP 分组和浮动 MAC.....	110
6.4 HA 健康检查和失效切换.....	115
6.5 对端节点 HA 分组状态检查.....	118
6.6 配置同步.....	118
6.7 SSF.....	123
6.8 HA 一致性检查.....	125
6.9 HA 日志.....	126
6.10 通用配置.....	126
第 7 章 单系统映像 (SSI)	129
第 8 章 分区管理.....	131
8.1 系统模式.....	131
8.2 分区模式.....	144
第 9 章 SSL 加速.....	146
9.1 SSL 主机配置.....	146
9.2 SSL 证书管理.....	149
9.3 SSL 协议版本和密码套件.....	184
9.4 签名算法和椭圆曲线.....	190
9.5 TLSv1.3 特性选项	192
9.6 客户端认证.....	193
9.7 客户端认证高级选项.....	210
9.8 服务器认证.....	212
9.9 SSL 重协商.....	213
9.10 SSL 会话功能选项.....	214
9.11 SSL 错误页面定制	216
9.12 SSL 通道.....	218
9.13 SSL 通用命令.....	221
9.14 FIPS.....	224

9.15 密码卡.....	225
9.15.1 通用配置.....	225
9.15.2 三未密码卡.....	226
9.15.3 国芯密码卡.....	228
第 10 章 SSL 侦听.....	230
10.1 SSL 侦听功能和证书配置.....	230
10.2 域名列表.....	232
10.3 URL 过滤.....	236
第 11 章 安全应用访问（SAA）.....	244
11.1 AAA.....	244
11.1.1 SAML.....	249
11.1.2 RADIUS.....	252
11.1.3 LDAP.....	255
11.1.4 OAuth.....	259
11.1.5 会话管理.....	264
11.2 Web SSO.....	268
第 12 章 链路负载均衡（LLB）.....	271
12.1 LLB 路由.....	271
12.2 出向链路负载均衡.....	282
12.3 入向链路负载均衡.....	288
12.4 链路健康检查.....	290
12.5 LLB 支持 IP 地址组.....	293
12.6 LLB 统计功能.....	296
12.7 LLB 通用配置.....	298
第 13 章 全局服务器负载均衡（GSLB）.....	301
13.1 基本 SDNS 命令.....	301
13.2 SDNS 域名.....	306
13.3 SDNS 监听 IP 地址.....	312

13.4 SDNS 服务	313
13.5 SDNS 池	315
13.6 SDNS 区域	331
13.7 SDNS 策略	332
13.8 SDNS Monitor	335
13.9 SDNS 探测池	381
13.10 SDNS 静态和 IP 域表就近性规则	384
13.11 SDNS 动态就近性探测系统	387
13.12 DNS 资源记录	393
13.13 DNS 区域	411
13.13.1 基本设置	411
13.13.2 SDNS 转发	416
13.14 SDNS 全域名	417
13.15 RPZ 防火墙	422
13.16 SDNS DNSSEC	424
13.17 SDNS 数据中心同步	429
13.18 SDNS 链路	438
13.19 DNS 响应码重写	443
13.20 SDNS 解析失败自定义应答策略	444
13.21 TCP DNS	446
13.22 DOH	447
13.23 DNS ePolicy 集成	454
13.24 SDNS SSL 配置	455
13.25 SDNS 与 SLB 联动	456
13.26 DNS Proxy	457
13.27 External DNS 云原生方式容器平台对接方案	461
13.28 SDNS IANA	464
13.29 SDNS 日志	465

13.30	SDNS 统计功能	466
13.31	SDNS 配置备份	479
13.32	SDNS 配置加载	480
第 14 章	应用安全.....	482
14.1	防火墙.....	482
14.1.1	访问组.....	482
14.1.2	访问规则.....	483
14.1.3	防火墙.....	487
14.2	Web 应用防火墙（WAF）	488
14.3	高级访问控制.....	494
14.3.1	ACL 规则.....	494
14.3.2	HTTP ACL 规则	499
14.3.3	DNS ACL 规则.....	502
14.4	DDoS 攻击防御.....	505
14.4.1	TCP DDoS	507
14.4.2	UDP DDoS.....	507
14.4.3	DNS DDoS.....	507
14.4.4	SSL DDoS.....	508
14.4.5	HTTP DDoS.....	509
14.4.6	ACL 黑名单.....	512
第 15 章	IPv6 高级配置	516
15.1	DNS64 和 NAT64.....	516
15.2	DNS46 和 NAT46.....	518
15.3	通用配置.....	520
第 16 章	ePolicy.....	522
第 17 章	日志.....	525
17.1	基本设置.....	525
17.2	RFC 5424 Syslog	527

17.3 日志定制.....	528
17.4 本地和远程日志主机.....	534
17.5 单个系统日志禁用.....	539
17.6 日志报警.....	540
17.7 日志关联 SNMP trap.....	543
17.8 应用可视化.....	544
17.9 系统日志去重和限速.....	545
第 18 章 管理工具.....	546
18.1 配置管理命令.....	546
18.2 备份管理.....	571
25.2.1 配置备份.....	571
25.2.2 日志备份.....	583
18.3 USB 存储访问.....	592
18.4 基于角色的权限管理.....	593
18.5 三权分立功能.....	599
18.6 WebUI 双因素认证登录.....	600
18.7 配置同步命令.....	600
18.7.1 配置同步.....	600
18.7.2 同步回退.....	605
18.7.3 其他命令.....	605
18.8 SDNS 配置同步命令.....	607
18.9 SNMP 命令.....	607
18.10 故障检测命令.....	614
18.11 调试命令.....	616
18.12 远程管理命令.....	624
18.13 自定义配置脚本.....	625
18.14 带宽管理命令.....	627
18.15 登录界面管理命令.....	627

18.16 网卡管理命令.....	628
18.17 文件系统救援.....	628
18.18 一键巡检命令.....	630
附录一 SNMP OID 列表.....	632
附录二 功能规格.....	656

第1章 命令行介绍

设备的 CLI（Command Line Interface，命令行界面）允许管理员使用命令行直接对设备的主要功能进行配置和控制，从而最大化的利用设备强大丰富的功能，并且最大程度的发挥其出色的性能。

本手册将介绍如何正确配置和使用每一条命令。在本文的命令行介绍中，我们将采用下列字体和符号来代表不同含义：

1.1 命令行符号含义

表1 - 1 命令行符号含义

格式	含义
粗体	命令行主体采用加粗字体表示。
<i>斜体</i>	命令行参数采用斜体表示。
< >	表示用“< >”括起来的参数在配置时是必选的。
[]	表示用“[]”括起来的参数在配置时是可选的。 表示“no”、“show”和“clear”等子命令。
{ x y ... }	表示从两个或多个选项中选取一个或多个。
[x y ...]	表示从两个或多个选项中选取一个或者不选。



注意：

- 当参数取值为字符串时，推荐将参数取值置于双引号中，以确保设备能够正确执行命令。
- 输入命令行时，每行最多支持输入 2048 字节。

1.2 正则表达式

设备的部分命令行参数支持使用与 Perl 兼容的正则表达式。正则表达式匹配分为两种：快速正则表达式匹配和全正则表达式匹配。两种正则表达式支持的 Perl 元字符如下表所示：

表1-2 支持的 Perl 字符

类型	支持的 Perl 元字符
快速正则表达式	只支持以下三个 Perl 元字符： “^”表示匹配行的开始字符。 “*”表示匹配 0 个或多个在它之前的字符。 “\$”表示匹配行的结束字符。

类型	支持的 Perl 元字符
	典型配置示例： “^172.16.73.146/abc”表示匹配所有名称以“172.16.73.146/abc”开头的网络资源。 “abc*”（和“abc”效果相同）表示匹配所有名称包含“abc”字符的网络资源地址。 “.txt\$”表示匹配所有名称以“.txt”结尾的网络资源地址。
全正则表达式	与快速正则表达式相比，支持的 Perl 元字符更多： “^”表示匹配行的开始字符。 “.”表示匹配任何一个字符。 “+”表示匹配 1 个或多个在它之前的字符。 “*”表示匹配 0 个或多个在它之前的字符。 “?”表示匹配 0 个或 1 个在它之前的字符。 “\$”表示匹配行的结束字符。 “[]”表示匹配方括号内的任意字符。 “ ”表示匹配在它之前或之后的字符。 “()”表示将括号内的字符作为组进行匹配。



注意：

- 正则表达式中的“*”不同于通配符中的“*”。要避免在配置正则表达式时使用单独的“*”。正则表达式中的“.*”等同于通配符表达式中的“*”。
- 如果需要匹配 Perl 元字符，需要在元字符前加“\”用于转义。例如需要匹配“*”时，应配置“*”。
- 当一个命令中有两个或两个以上的参数支持使用正则表达式时，是否按照正则表达式进行匹配是由第一个参数是否配置成正则表达式决定的。如果支持使用正则表达式的第一个参数取值不是正则表达式，其他参数的正则表达式配置不生效。
- 对于既支持优先级参数，也支持全正则表达式匹配的命令，优先级的配置仅在都使用全正则表达式，或都使用快速正则表达式和精确匹配的配置之间生效。如果同时匹配的多条配置中，既包含使用全正则表达式的配置，也包含使用快速正则表达式或精确匹配的配置，设备会优先选择使用快速正则表达式或精确匹配的配置。

1.3 登录设备

当管理员通过 SSH 或者控制台终端成功连接到设备时，系统会提示用户输入登录用户名和密码。系统默认的初始登录用户名为“admin”，密码为“admin”。

设备提供的账号恢复机制允许管理员：

- 恢复初始登录账号的密码（如果管理员在修改密码后忘记密码）。
- 恢复被误删的初始登录账号。
- 恢复调试账号的密码。

要恢复初始登录账号的密码或恢复初始登录账号，请执行以下步骤：

1. 与设备建立 Console 连接。
 2. 在命令行界面下输入命令“**recovery**”。
 3. 将系统生成的 challenge 字符串复制并发送至公司客户支持来请求 response 字符串。“challenge:”提示符后面为 challenge 字符串的内容，例如“challenge: waker Parma baker galah woke”。
 4. 在命令行界面中粘贴由公司客户支持回复的 response 字符串并按回车键。response 字符串以“--begin--”开头，以“--end--”结束。
 5. 此时，命令行提示“输入 1 恢复调试账号的密码，输入 2 恢复 admin 账号的密码”。
- 如果要恢复“admin”账号的密码，输入 2。如果系统中存在初始登录（“admin”）账号，则该账号的密码将被重置为初始登录账号的密码（“admin”），访问权限将被重置为“Config 级别”。如果系统中不存在初始登录账号，则系统将创建一个密码为初始登录账号的密码，访问权限为“Config 级别”的初始登录账号。恢复初始登录账号或密码后，必须使用初始登录账号登录并修改密码，否则在系统重启后，只能使用恢复前的账号和密码登录。
 - 如果要恢复调试账号的密码，输入 1。如果系统中存在调试账号，则该账号的密码将被重置为仅根据设备序列号计算产生；如果系统中不存在调试账号，也不会创建调试账号。

此外，系统也支持通过 WebUI、XML-RPC、RESTful API 等方式连接设备。

1.4 访问控制的级别

设备的命令行接口提供四个级别（模式）的访问控制，对需要登录系统并进行特定配置操作的管理员进行权限管理。每个级别分别用不同的命令行提示符来表

示，其组成形式分别为：“设备的主机名称” + “>”或“#”或“(config)#”或“[test@设备的主机名称 ~]\$”。下文示例统一用 Demo 演示。

- User 级别

处于这个级别的用户只能使用一些非关键的设备功能，例如使用“ping”和“traceroute”等一些基本的网络诊断命令进行简单的网络故障诊断。

在命令行接口中，User 级别提示符的表现形式为“Demo>”。

- Enable 级别

处于这个级别的用户可以使用的命令大多数只能用于查看信息，比如“show version”命令可以用于查看设备软件版本的相关信息。

Enable 级别的用户对 User 级别的命令也具有操作权限。

想要进入 Enable 级别，使用者需要在 User 级别执行下面的命令：

```
Demo>enable
```

执行该命令后，系统会提示用户输入正确的 Enable 级别的密码。这个密码可以是先前配置好的，也可以是通过初始化安装设置的，缺省为空。

输入正确的 Enable 密码后，如果 CLI 提示符从“Demo>”转变为“Demo#”，则说明用户已经成功进入了 Enable 级别。

- Config 级别

最高的访问级别是 Config 级别（配置级别）。处于这个级别的使用者可以对设备的各项功能进行配置和管理，也可以修改已有的配置。系统默认同一时刻只能有一个用户进入 Config 级别。具有 Config 权限的用户，可以使用 User 级别和 Enable 级别的所有命令。

想要进入 Config 级别，使用者需要在 Enable 级别下执行下面的命令：

```
Demo#config terminal
```

执行该命令后，如果 CLI 命令行提示符从“Demo#”变为“Demo(config)#”，则说明用户已经成功进入了 Config 级别。

此外，系统支持多登录 Config 级别功能，即同一时间允许多个管理员账户处于 Config 级别或同一管理员账户开启多个 Config 级别的 SSH 连接。管理员可以通过执行“**config multiconfig enable**”命令进行启用。



注意：在设备系统中，用户可以分为两个等级：Enable 和 Config。Enable 等级的用户只对 Enable 级别的命令具有操作权限，无法进入 Config 级别进行配置。

- 调试级别

除上面的级别外，系统中还存在用于内部调试的账号。处于这个级别的用户可以使用 Linux 系统中的大部分用于查看信息的命令。

在命令行接口中，调试级别提示符的表现形式为 “[test@Demo ~]\$”。

1.5 命令行快捷键

设备的软件具有很强的交互性。使用 CLI 命令时，允许用户仅输入命令的第一个或前几个字母，只要该命令的前几个字母不与其他命令的前几个字母相同，设备就可以识别该命令，此时用户可以直接点击“回车键”，执行此命令。

用户可以使用的其它快捷键如下表所示。

表1-3 CLI 快捷键

CLI 快捷键	操作
^a/^e	将光标移动到行的开头/结尾。
^f/^b	将光标向前/向后移动一个字符。
Esc-f	将光标向前移动一个单词。
Esc-b	将光标向后移动一个单词。
^d	删除光标对应的字符。
^k	删除光标处到行尾的内容。
^u	删除输入的行。

提示：“^”使用这个符号时，需要按住键盘上的 Control (Ctrl) 键，同时按“^”之后的字母。

第2章 基本系统配置

本章介绍基本的系统配置命令，包括：

- 系统 IP 地址、路由和接口的配置
- 系统优化参数配置
- 邮件报警和邮件中继功能配置
- 系统健康检查功能的配置

?

该命令用于显示所有当前访问级别下可以使用的命令行的第一个关键字，或显示当前命令行的下一个关键字或参数项。

help

该命令用于显示所有当前访问级别下可以使用的命令行的第一个关键字。

enable [recovery]

命令“**enable**”用于进入 Enable 级别。执行该命令后，系统将提示管理员输入 Enable 级别的密码，系统默认的 Enable 密码为空。命令“**enable recovery**”用于重置进入 Enable 级别的密码，具体步骤如下：

1. 在用户级别命令行中输入“**enable recovery**”，命令行会出现一个 challenge 字符串。
2. 将 challenge 字符串发送到客户支持邮箱。客户支持人员会通过 E-mail 回复一个 response 响应代码。
3. 将响应代码粘贴到命令行并执行，Enable 密码将被重置为空（缺省值）。

disable

该命令用于从当前级别回退到普通用户级别（User 级别）。

exit

该命令用于从 Config 级别退回到 Enable 级别。在 Enable 级别或是 User 级别下执行该命令将退出命令行模式。

quit

该命令用于退出命令行模式。在配置过程中，管理员可以在任何时候执行该命令。

switch user <user_name> <password> [segment_name]

该命令用于将当前的管理员账户切换到其他管理员账户的指定分区。切换管理员账户后，之前的用户会话将会关闭。

user_name	该参数指定要切换的管理员账户的用户名。取值可以是系统管理员账户或分区管理员账户的用户名。
password	该参数指定要切换的管理员账户的密码。
segment_name	可选。该参数指定要切换的分区。如果不指定该参数，即取值为空时，表示默认切换到管理员账户绑定的所有分区中按照字典顺序排列排名第一的非“API”权限的分区。 默认值为空。

show tech

该命令用于抓取并显示实时的系统信息及设备运行状态。

show system openport

该命令用于显示系统当前开放的所有端口。

show system warning [module]

该命令用于显示实时的系统警告信息。

module	可选。该参数指定功能模块名称，取值必须为： • system: 显示系统模块相关警告信息，例如 CPU 风扇、CPU 温度、系统温度、电源、SSL 加速卡、网卡等硬件问题。 • slb: 显示 SLB 模块相关警告信息，例如虚拟服务和后台服务的并发连接数（cc）和每秒新建连接数（cps）等超限问题。 • all: 系统和 SLB 模块警告信息都显示。 默认值为“all”。

show system status

该命令用于显示系统状态信息，包括 CPU 使用率、硬盘分区使用率、内存使用率（小于 1% 时不显示）、温度、风扇速度、电源和接口状态等等。

show system ipmi <type> <mode> [entryid|sensorid|entityid|sensortype]

该命令用于显示当前系统事件日志（System Event Log, SEL）或者传感器数据记录（Sensor Data Records, SDR）相关信息。

type	该参数指定要显示的信息的类型，取值必须为：

- sel: 表示显示当前系统事件日志的相关信息。
- srd: 表示显示当前传感器数据记录相关信息。

mode

该参数指定显示信息的模式。

当参数“type”取值为“sel”时，该参数取值必须为：

- list: 表示列出所有的 SEL 信息，包括“ID”、“Date”、“Time”、“Sensor Type/Num”、“Description”和“EventDirection”。
- get: 表示显示与参数“entryid”指定的过滤字符串一致的 SEL 的详细信息，包括：SEL Record ID（系统事件日志记录 ID）、Record Type（记录的类型值，例如：02 为 Generic Discrete，即通用离散）、Timestamp（事件时间戳）等详细信息，关于其他字段相关信息，请参考 IPMI 规范。

当参数“type”取值为“sdr”时，该参数取值必须为：

- list: 表示列出所有的 SDR 信息，包括“Name”、“Type”、“State”、“Entity”和“Value”。
- get: 表示显示与参数“sensorid”指定的过滤字符串一致的所有 SDR 的详细信息，包括：Sensor ID（传感器 ID，标识传感器的唯一 ID）、Entity ID（实体 ID，传感器数据区 SDR 中与特定传感器相关联的实体标识符）、Sensor Type (Threshold)（一个传感器具体的类型和阈值配置）等详细信息，关于其他字段相关信息，请参考 IPMI 规范。
- type:
 - 当不指定参数“sensortype”时，将显示 SDR 所有的类型名称与类型值的对应关系，类型值以两位 16 进制数显示，例如：类型名称为“OS Boot”对应的类型值为“0x1f”。
 - 当指定参数“sensortype”时，将显示与“sensortype”指定的过滤字符串一致的所有 SDR 的详细信息，包括：“Name”、“Type”、“State”、“Entity”和“Value”。
- entity:
 - 当不指定参数“entityid”时，将显示所有的 SDR 的 Entity ID 与 Entity 的对应关系。例如：Entity

ID 为“0”对应的 Entity 为“Unspecified”。

- 当指定参数“entityid”时，将显示与“entityid”指定的过滤字符串一致的 SDR 的详细信息，包括：“Name”、“Type”、“State”、“Entity”和“Value”。

entryid sensorid	可选，该参数指定用于显示相关信息的过滤字符串。
sensortype entityid	该参数在下面几种情况需要配置： • entryid: 日志条目 ID。当参数“type”取值为“sel”，参数“mode”取值为“get”时需要配置该参数，且取值必须与命令“show system ipmi sel list”显示的“ID”的取值一致。 • sensorid: 传感器 ID。当参数“type”取值为“sdr”，参数“mode”取值为“get”时需要配置该参数，且取值必须与命令“show system ipmi sdr list”显示的“ID”的取值一致。 • sensortype: 传感器类型。当参数“type”取值为“sdr”，参数“mode”取值为“type”时，选择配置该参数（详见参数“mode”），且取值必须与命令“show system ipmi sdr type”显示的类型值的取值一致。 • entityid: 实体 ID。当参数“type”取值为“sdr”，参数“mode”取值为“entity”时，选择配置该参数（详见参数“mode”），且取值必须与命令“show system ipmi sdr entity”显示的“ID”的取值一致。



注意：命令只支持以下设备：

APV_1800、APV_2800、APV_5800、APV_6850、APV_7850、APV_8850、APV_9650D、APV_9650F、APV_9650E、APV_11600D、APV_12800 和 APV_7860。

ip address <interface_name> <ip_address> {netmask|prefix} [overlap]

该命令用于设置系统接口、MNET 接口、VLAN 接口或聚合接口的 IP 地址和子网掩码或前缀长度。

interface_name 该参数指定接口的名称，接口可以为系统接口、VLAN 接口、VXLAN 接口和聚合接口。

对于系统接口，可以通过命令“**interface name**”自定义接口名称。默认系统接口名称为 port1、port2、port3、

port4 等。

对于聚合接口，默认名称为 bond1、bond2、bond3、bond4 等。

ip_address	该参数指定接口 IP 地址，取值必须为 IPv4 或 IPv6 地址。
netmask prefix	该参数指定 IP 地址对应的子网掩码或前缀长度。 “netmask”用于配置 IPv4 地址对应的子网掩码，取值可以是点分地址格式或是一个 0 至 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，取值必须为 0 至 128 之间的整数。
overlap	可选，该参数指定接口的 overlap 选项，表示该接口所属子网与已有接口的子网重叠，每个子网只能配置一个使用 overlap 选项的接口。只有当配置了 NUMA SLB（单一虚拟 IP，反向代理模式下）时，才需要配置此参数。 VLAN 接口不能设置该参数。系统支持最多配置 16 个使用 overlap 选项的接口。

示例：

```
Demo(config)#ip address port1 209.120.10.2 255.255.255.0
Demo(config)#ip address port2 209.120.10.1 255.255.255.0 overlap
```

no ip address <interface_name> [ip_type]

该命令用于删除指定接口的 IP 地址配置。

interface_name	该参数指定接口名称。
ip_type	可选，该参数指定需要删除的 IP 地址类型，取值必须为： 4：表示 IPv4 地址。 6：表示 IPv6 地址。 默认值为 4。

show ip address

该命令用于显示接口名称和对应的 IP 地址及子网掩码。

clear ip address

该命令用于删除所有接口的 IP 地址配置。在删除系统 IP 地址之前，需要先将接口上的虚拟 IP 配置删除。

ip statistics {on|off}

该命令用于启用或禁用 IP 统计信息功能。该功能默认设置为禁用。

除了 IP 相关统计以外，该功能也会控制是否统计虚拟服务、后台服务的 CPS 信息。CPS 统计信息可以通过 “**show statistics slb all**” 命令查看。

该功能是否开启不影响虚拟服务和后台服务的 CPS 限速功能（通过 “**slb virtual application cps**” 和 “**slb real application cps**” 命令配置）。

show ip statistics

该命令用于显示 IP 统计信息功能的状态。

show statistics ip [ip_address]

该命令用于显示指定的 IP 地址的统计信息。如果不指定参数 “ip_address”，则将显示所有 IP 地址的统计信息。

示例：

Demo(config)#show statistics ip					
Host: AN					
Current Time: 06/26/12 15:00					
IP	Pkts In	Bytes In	Pkts Out	Bytes Out	Start Time
=====					
10.8.6.62	14565	1242430	48147	9178799	06/25/12 16:22
192.168.1.10	0	0	0	0	06/21/12 14:37
172.5.6.26	0	0	0	0	06/21/12 14:37
10.212.196.33	0	0	0	0	06/21/12 14:37
21da:d3:0:2f3b:2aa:ff:fe28:9c5a	0	0	0	0	06/21/12 14:37

Total:	14565	1242430	48147	9178799	

clear statistics ip [ip_address]

该命令用于清除指定 IP 地址的统计信息。如果不指定参数 “ip_address”，则将清除所有已经配置 IP 地址的统计信息。

ip dhcp {on|off} <interface_name>

该命令用于启用或禁用指定系统接口的 DHCP 功能。启用该功能后，指定系统接口将通过 DHCP 服务器自动获取 IP 地址。该功能默认设置为禁用。

interface_name 该参数指定系统接口名称，可以通过 “**interface name**” 命令来自定义系统接口名称。默认系统接口名称为 port1、port2、port3、port4……。



注意：启用指定系统接口的 DHCP 功能后，如果执行命令“**write memory**”，系统将不保存该系统接口上的静态 IP 配置。

ip arp <ip_address> <mac_address>

该命令用于为系统配置一条静态 ARP 表项，系统重启后，静态 ARP 表项依然保存在系统中，动态 ARP 表项将被清除。最多允许配置 128 条静态 ARP 表项。

ip_address 该参数指定远程主机的 IP 地址。取值必须为 IPv4 地址。

mac_address 该参数指定远程主机的 MAC 地址。

no ip arp <ip_address>

该命令用于删除指定 IP 地址对应的静态或动态 ARP 表项。

show ip arp [ip_address]

该命令用于显示指定 IP 地址对应的 ARP 表项。如果不指定参数“ip_address”，将显示所有静态 ARP 表项和系统学习到的动态 ARP 表项。

clear ip arp

该命令用于删除所有静态和动态 ARP 表项。

ip host <host_name> <ip_address>

该命令用于添加一条 DNS 资源记录，用于 DNS 解析。

host_name 该参数指定域名。

ip_address 该参数指定与域名对应的 IP 地址。

no ip host <host_name> [ip_address]

该命令用于删除一条 DNS 资源记录。

show ip host

该命令用于显示所有的 DNS 资源记录。

clear ip host

该命令用于删除所有 DNS 资源记录。

ip route default <gateway_ip>

该命令用于配置系统的默认路由。默认路由只能配置一条。

gateway_ip 该参数指定默认网关的 IP 地址，取值必须为 IPv4 或 IPv6 地址。



注意：对于分区模式，如果配置了 IPv4 类型的默认路由（通过命令“**ip route default**”），需要在系统模式下通过该命令配置 IPv4 类型的默认路由。

no ip route default <gateway_ip>

该命令用于删除系统的默认路由。

ip route static <destination_ip> {netmask|prefix} <gateway_ip>

该命令用于为系统配置一条静态路由。静态路由可以配置多条。

destination_ip 该参数指定静态路由的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

netmask|prefix 该参数指定目的 IP 地址对应的子网掩码或前缀长度。

- 参数“**netmask**”用于配置 IPv4 地址对应的子网掩码，取值应为点分地址格式。
- 参数“**prefix**”用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

gateway_ip 该参数指定静态路由的网关 IP 地址，取值必须为 IPv4 或 IPv6 地址。如果指定的是一个 IPv6 链路本地地址，必须同时指定端口号，参数取值采用“IPv6_link-local_address%port_number”的格式。

注意：出于可用性考虑，不建议将该参数取值配置为本地 IP 地址，例如：系统接口 IP 地址、IP 地址池中的 IP 地址等等。

no ip route static <destination_ip> {netmask|prefix} <gateway_ip>

该命令用于删除一条静态路由配置。

show ip route

该命令用于显示静态路由、默认路由、管理路由和动态路由信息。

clear ip route

该命令用于删除已配置的静态路由、默认路由和动态路由信息。

show route match <source_ip> <source_port> <destination_ip> <destination_port> <protocol> [interface_name] [action_table]

该命令用于显示系统中与指定的源 IP、源端口、目的 IP、目的端口、协议类型匹配的路由或者路由组，或显示与指定的源 IP、源端口、目的 IP、目的端口、协议类型、接口和访问规则类型匹配的访问规则。

source_ip	该参数指定源 IP 地址。
source_port	该参数指定源端口号。
destination_ip	该参数指定目的 IP 地址。
destination_port	该参数指定目的端口号。
protocol	该参数指定协议类型，取值必须为： • tcp: 表示 TCP 协议类型。 • udp: 表示 UDP 协议类型。 • icmp: 表示 ICMP 协议类型。 • ah: 表示采用 AH（Authentication Header，认证报头）网络认证协议，仅用于匹配访问规则。 • esp: 表示采用 ESP（Encapsulating Security Payload，封装安全负载）网络认证协议，仅用于匹配访问规则。 • any: 表示任意协议类型。
interface_name	可选，该参数指定接口名称。 默认值为空（空值应使用双引号），表示所有接口。
action_table	可选，该参数指定访问规则类型，取值必须为： • 1: 表示允许类型的访问规则。 • 2: 表示拒绝类型的访问规则。 默认值为 1。



注意：如果配置了 NAT，且匹配了 NAT 规则，执行“**show route match**”也将显示匹配的 NAT 配置以及命中的虚拟 IP 地址。

interface mac <interface_name> <mac_address>

该命令用于为指定的系统接口配置 MAC 地址。

interface_name	该参数指定系统接口名称。
mac_address	该参数指定系统接口的 MAC 地址。当系统接口上配置了 VLAN、MNET、聚合接口或 SLB 虚拟服务时，MAC 地址也不变。

no interface mac <interface_name>

该命令用于将指定接口的 MAC 地址恢复为默认值。

clear interface mac

该命令用于将所有接口的 MAC 地址恢复为默认值。

interface name <interface_id> <interface_name>

该命令用于设置系统接口名称。

interface_id 该参数指定系统接口序号。根据设备型号的不同，设备支持的系统接口数量也有所不同。

默认接口序号为 port1、port2、port3、port4……。

interface_name 该参数指定自定义的接口名称，取值必须为长度不超过 31 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。

no interface name <interface_id>

该命令用于将指定的系统接口名称恢复为默认设置。



注意：如果在配置 FWDMAC 类型（通过命令“**slb real fwdmac**”）和 l2mac 类型（通过命令“**slb real l2mac**”）的后台服务时使用了系统接口名称，则执行该命令时不会将该系统接口名称恢复为默认设置。

clear interface name

该命令用于将所有系统接口名称都恢复为默认设置。



注意：如果在配置 FWDMAC 类型（通过命令“**slb real fwdmac**”）和 l2mac 类型（通过命令“**slb real l2mac**”）的后台服务时使用了系统接口名称，在执行该命令时会除该系统接口以外的所有系统接口名称恢复为默认设置。

interface description <interface_id> <description>

该命令用于设置指定接口的描述信息。

interface_id 该参数指定系统接口序号。接口可以为系统接口、VLAN 接口、VXLAN 接口和聚合接口。

默认系统接口序号为 port1、port2、port3、port4 等。默认聚合接口序号为 bond1、bond2、bond3、bond4 等。

注意：根据设备型号的不同，设备支持的系统接口数量也有所不同。

description 该参数指定接口描述信息，取值必须为长度不超过 255

个字节的字符串。

no interface description <interface_name>

该命令用于删除指定接口的描述信息。

interface mtu <interface_id> <mtu>

该命令用于修改指定接口的 MTU（Maximum Transmission Unit，最大传输单元）值。系统默认的 MTU 值为 1500 字节。

interface_id 该参数指定接口名称，取值必须为 VLAN 接口名称、聚合接口名称或物理接口的默认序号（例如 port1、port2、port3.....）。

mtu 该参数指定接口的 MTU 值，单位为字节。接口支持的 MTU 最大值会根据接口网卡型号的不同而变化（部分接口网卡支持的 MTU 最大值可达 65535 字节）。

如果参数“interface_id”为 VLAN 接口名称，而且其父接口为 10G 以太网接口，那么以太网帧头部则会加入 4 个字节的 VLAN tag 信息。在这种情况下，参数取值至少比父接口的 MTU 值小 4。



注意：

1. 当一个聚合接口和绑定的物理接口上都配置了 MTU 时，通过聚合接口发送的报文大小以聚合接口的 MTU 为准。
2. 根据 RFC 2460，IPv6 协议要求因特网上的所有 Linux 接口的 MTU 必须不小于 1280 字节。

clear interface mtu <interface_id>

该命令用于将指定接口的 MTU 值恢复为默认设置。

interface_id 该参数指定接口名称，取值必须为 VLAN 接口名称、聚合接口名称、物理接口的默认序号（例如 port1、port2、port3.....）或“all”。取值为“all”时表示将所有接口的 MTU 值恢复为默认设置。

interface speed <interface_id> <speed_option>

该命令用于设置指定系统接口的接口速度和工作模式。如果接口与其它设备（例如特定速度的双工模式路由器和交换机）连接在一起使用，需要通过设置系统接口速度和工作模式来满足这些要求。管理员可以使用“**show interface**”命令查看当前速度设置。

interface_id 该参数指定系统接口序号。根据设备型号的不同，设备

支持的系统接口数量也有所不同。

默认接口序号为 port1、port2、port3、port4……。

speed_option

该参数指定接口速度和工作模式，取值必须为：

- 10half：表示 10 兆半双工。
- 100half：表示 100 兆半双工。
- 100full：表示 100 兆全双工。
- 1000full：表示 1000 兆全双工。
- auto：表示自适应。万兆（10G）以太网接口只能设置为自适应。

默认值为“auto”。

clear interface speed [interface_id]

该命令用于删除指定接口的接口速度和工作模式设置。如不指定参数“interface_id”，将删除所有接口的接口速度和工作模式设置。

interface promisc <interface_id> {enable|disable}

该命令用于启用或禁用指定系统接口的混杂模式。启用混杂模式的系统接口支持对目的 MAC 地址为非本地 MAC 地址的数据包进行处理。该功能默认设置为禁用。

interface_id

该参数指定系统接口的序号。根据设备型号的不同，设备支持的系统接口数量也有所不同。

默认接口序号为 port1、port2、port3、port4……。

clear interface promisc

该命令用于禁用所有系统接口的混杂模式。

interface management <interface_id> <gateway_ip>

该命令用于将指定的系统接口或聚合接口设置为管理接口，并指定网关 IP 地址。如果系统接口上承载了 VLAN 配置，则不能设置为管理接口。系统仅支持配置一个管理接口，该管理接口上可同时指定一个 IPv4 网关和一个 IPv6 网关。

管理接口只支持管理流量，例如 WebUI、SSH、SNMP 以及 RESTful API 等流量。

interface_id

该参数指定系统接口或聚合接口的序号，例如 port1、bond1。

gateway_ip

该参数指定网关 IP 地址，取值可以为 IPv4 和 IPv6 地址。网关 IP 不能为 0.0.0.0，也不能和系统接口的 IP 地址相

同。

no interface management <interface_id> <gateway_ip_type>

该命令用于删除指定的管理接口。

interface_id 该参数指定系统接口或聚合接口的序号，例如 port1、bond1。

gateway_ip_type 可选，该参数指定网关 IP 地址的类型，取值必须为：

- 4：表示删除 IPv4 网关。
- 6：表示删除 IPv6 网关。

默认值为 4。

clear interface management

该命令用于清除所有的管理接口

show management

该命令用于显示所有的管理接口。

interface bandwidthtimer [interval]

该命令用于设置接口带宽的统计间隔。

当不配置该命令时，默认的统计间隔是 300 秒。管理员可以通过“**show interface**”命令查看接口带宽的统计间隔设置。

interval 可选。该参数指定接口带宽的统计间隔，单位为秒，取值必须为 5 至 300 之间的整数。

默认值是 300。

no interface bandwidthtimer

该命令用于将接口带宽的统计间隔恢复为系统的默认设置。

interface shutdown <interface_id>

该命令用于手动关闭指定的物理接口。关闭指定物理接口后，系统将发生以下变化：

- 网关状态变为 Down
- 接口不再允许配置以下属性：
 - 接口 MTU 值、管理接口、MAC 地址、混杂模式，以及接口速度和工作模式

- 接口保留以下属性的配置权限：
 - 接口名称、接口描述、接口带宽的统计间隔
- 当关闭指定物理接口后，该物理接口关联的所有 VLAN 接口显示 no carrier
- 当聚合接口下的所有物理接口都关闭后，聚合接口显示 no carrier
- 分区中的接口状态变为 Down，网关状态为 Down

如果使用该命令手动关闭了物理接口，管理员可通过“**show interface**”命令的查看到接口状态信息显示为“status: down (Administratively down)”。

interface_id 该参数指定接口名称。取值必须为物理接口的默认序号（例如 port1、port2、port3.....）。



注意：手动关闭物理接口后，接口状态将显示为“Administratively down”。此时，系统已不再检测接口状态。如果继续拔掉接口线，接口状态依旧为“Administratively down”。

no interface shutdown <interface_id>

该命令用于取消指定物理接口的关闭状态。

clear interface shutdown

该命令用于取消所有物理接口的关闭状态。

show interface [interface_id]

该命令用于显示指定系统接口、VLAN 接口、VXLAN 接口或聚合接口的相关配置和统计信息。如不指定参数“interface_id”，则将显示所有接口的相关配置和统计信息。

下表列出了该命令中各项输出的含义：

表2-1 输出信息

输出信息	含义
Input queue size	当前输入队列长度。
Input queue max	最大输入对列长度。
Runt	通过了地址过滤、长度低于最小帧长度（64 字节）、CRC 校验正确的帧数量。
Giant	通过了地址过滤、长度大于最大帧长度、CRC 校验正确的帧数量。
Jabber	通过了地址过滤、长度大于最大帧长度、CRC 校验错误的帧数量。CRC 校验错误可能是由网卡损坏或电子干扰造成的。
CRC	校验错误的报文数量。
Flow Control	接收到的未知流控帧数量。

Fragments	通过了地址过滤、长度低于最小帧长度、CRC 校验错误的分片数量。
Frame	接收到的校正错误报文数量(报文的字节长度不是整数)。
Lengths	接收到的长度错误事件数量。
No Buffers	接收到帧时系统没有可用内存存储该帧的次数。
Overruns	丢包数量。当接收 FIFO 没有足够的空间存储收到的报文时就会丢弃，原因可能是分配的缓存太小，或者 PCI 总线带宽不够。
Carrier extension errors	物理接口上出现载波延伸错误时收到的报文数量。
Collisions	发送方检测到的冲突总数（不包括发送报文后发现的冲突）。
Late collisions	工作在 10-100Mb/s 速率下发送了 64 字节后，或者工作在 1000Mb/s 速率下发送了 512 字节后检测到的冲突数量。
Deferred	因为物理线路忙或其它设备正在发送导致的发送延迟事件。
Single Collisions	成功发送的报文只遇到一次冲突的次数。
Multiple Collisions	成功发送的报文遇到 1 次以上 16 次以下冲突的次数。
Excessive collisions	发送一个报文遇到 16 次或大于 16 次冲突的次数。
Packet drop (not permit)	因未匹配任何允许访问控制规则而丢弃的报文数量。
Packet drop (deny)	因匹配拒绝访问规则而丢弃的报文数量。



注意：

- 如果 IP 统计信息功能为禁用（默认），该命令的输出结果中 WebWall 允许或者丢弃的数据报的数目都为 0。
- 在查看 VLAN 接口或聚合接口的流量统计前，需要先通过“**ip statistics on**”命令启用 IP 统计信息功能。

system tune accel mq

该命令用于启用设备的多队列（Multi-queue）负载均衡加速功能。当配置了多个虚拟 IP 时，可以使用该命令来启用四层 SLB 和 LLB 的加速功能。如果要使用该功能，管理员必须首先通过“**slb directfwd on**”命令启用快速转发功能。



注意：当使用“**system tune accel mq**”命令启用负载均衡加速功能之后，数据无法在设备上的 10GB 接口和 1GB 接口之间传输。

no system tune accel mq

该命令用于禁用设备的多队列负载均衡加速功能。

system tune attackfilter <filter_level>

该命令用于设置无效 IP 数据报的过滤级别。

filter_level

该参数指定无效 IP 数据报的过滤级别，取值必须为：

- 0：表示禁用 IP 数据报过滤功能，即允许任何数据

报通过以太网卡进入系统。

- 1: 表示设备将丢弃符合以下任一情况的数据报:
 - 源 IP 或目的 IP 为 0.0.0.0。
 - 源 IP 为 255.255.255.255。
 - 源 IP 为 224.x.x.x。
 - TCP 或 UDP 端口为 0。此时，管理员需要在特定接口上设置防火墙以预防可疑的网络攻击。
- 2: 表示设备将丢弃符合以下任一情况的数据报:
 - 源 IP 或目的 IP 为 0.0.0.0。
 - 源 IP 为 255.255.255.255。
 - 源 IP 为 224.x.x.x。
 - TCP 或 UDP 端口为 0。此时，管理员需要在特定接口上设置防火墙以预防可疑的网络攻击。
 - 源 IP 为本地 IP 地址（但数据报通过以太网接口被接收）。

默认值为 0。

no system tune attackfilter

该命令用于将无效 IP 数据报的过滤级别恢复为默认设置。

show system attackfilter

该命令用于显示被设备丢弃的攻击包的统计信息。

system tune ip randomid {on|off}

该命令用于启用或禁用为 IP 数据报设置随机编号的功能。启用该功能后，数据报编号随机产生。禁用该功能后，数据报编号连续递增。该功能默认设置为禁用。

no system tune ip randomid

该命令用于将 IP 数据报设置随机编号的功能恢复为默认值。

system tune route numaaccel {on|off}

该命令用于启用或禁用 NUMA 下的路由加速功能。该功能默认设置为禁用。



注意：由于使用该功能可能影响其它流量的通信，所以建议管理员在使用该功能前联系公司技术支持。

no system tune route numaaccel

该命令用于将 NUMA 下的路由加速功能恢复为默认设置。

system tune hwcksum {on|off}

该命令用于启用或禁用网卡信息校验功能。该功能对 IPv4 和 IPv6 类型的报文都可以生效。该功能默认设置为启用。

no system tune hwcksum

该命令用于将网卡信息校验功能恢复为默认设置。

system tune numa {auto|off}

命令“**system tune numa auto**”用于开启系统对 NUMA（Non-uniform Memory Access，非一致性内存访问）功能的自动探测。执行该命令后，支持 NUMA 功能的设备会自动开启该功能，不支持 NUMA 功能的设备则不会开启该功能。该功能默认设置为禁用。

命令“**system tune numa off**”用于关闭 NUMA 功能。

对“**system tune numa**”命令的配置仅在设备重启后生效，具体配置可以通过命令“**show system tune**”查看。



注意：开启系统对 NUMA 功能的自动探测后：

- 在未配置跨域聚合接口的应用场景下，流量会从后台服务或网关连接的系统接口发送出去。
- 在配置了跨域聚合接口的应用场景下：
 - 业务流量：通过入接口所属的 NUMA 域内的其他系统接口发送出去。
 - 非业务流量：IP 流量会通过入接口所属的 NUMA 域内的其他系统接口发送出去，UDP 和 TCP 流量会通过其他 NUMA 域发送出去。

show system numa

该命令用于显示 NUMA 功能的开启状态、NUMA 域中的接口信息以及网卡与域的绑定关系（可以通过该命令判断网卡是否跨域）。

默认情况下，该功能是启用的。

system tune tcpidle <idle_time>

该命令用于设置 TCP 连接的最大闲置时间。超出闲置时间后，TCP 连接将被终止。系统默认的 TCP 连接的最大闲置时间 300 秒。

idle_time 该参数指定 TCP 连接的最大闲置时间，单位为秒。取值必须为 60 到 7200 之间的整数。

no system tune tcpidle

该命令用于将 TCP 连接的最大闲置时间恢复成默认值。

system tune tcp retransmit timeout <timeout>

该命令用于设置 TCP 数据重发的超时时间。系统默认的 TCP 数据重发的超时时间为 1000 毫秒。建议管理员在没有获得公司技术支持的情况下不要修改默认配置。

timeout 该参数指定 TCP 数据重发的超时时间，单位为毫秒，取值必须为 100 至 4,294,967,295 之间的整数。

no system tune tcp retransmit timeout

该命令用于将 TCP 数据重发的超时时间恢复到默认值。

system tune tcp retransmit dupacks <dupacks>

该命令用于设置收到多少重复 ACK 包后进行 TCP 快速重传。系统默认收到 3 个重复 ACK 包后进行 TCP 快速重传。建议管理员在没有获得公司技术支持的情况下不要修改默认配置。

dupacks 该参数指定 TCP 进行快速重传之前收到的重复 ACK 包个数。

no system tune tcp retransmit dupacks

该命令用于将 TCP 快速重传前收到的重复 ACK 包数量恢复到默认值。

system tune tcp retransmit accelerate on

该命令用于启用或禁用 TCP 数据超时重发加速功能。该功能默认设置为禁用。

system tune tcp retransmit accelerate off

该命令用于禁用 TCP 数据超时重发加速功能。

no system tune tcp retransmit accelerate

该命令用于将 TCP 数据超时重发加速功能恢复为默认设置。

system tune tcp slowstart {on|off}

该命令用于启用或禁用 TCP 窗口缓慢恢复功能。该功能默认设置为启用。建议管理员在没有取得公司技术支持的情况下不要修改默认设置。

no system tune tcp slowstart

该命令用于将 TCP 窗口缓慢恢复功能恢复为默认设置。

system tune tcp delack count <count>

该命令用于配置设备在收到多少个数据报后发送 ACK 包。系统默认收到 4 个数据报后发送 ACK 包。

count 该参数指定延迟发送 ACK 包前收到的数据报的个数。
取值必须为 0 到 128 之间的整数。如取值为 0，表示不延迟发送 ACK 包。

system tune tcp delack timeout <timeout>

该命令用于配置在超时多长时间后发送 ACK 包。系统默认超时 100 毫秒后发送 ACK 包。

timeout 该参数指定延时发送 ACK 包的最大超时时间，单位为毫秒。取值必须为 100 到 5000 之间 10 的倍数。

no system tune tcp delack

该命令用于将 TCP 延迟发送 ACK 包的设置恢复为默认值。

system tune tcp syntimeout <max_timeout>

该命令用于设置 TCP SYN 包的最大超时时间。系统默认 TCP SYN 包的最大超时时间为 60 秒。

max_timeout 该参数指定 TCP SYN 包的最大超时时间，单位为秒。
取值必须为 60 到 600 之间的整数。

no system tune tcp syntimeout

该命令用于将 TCP SYN 包的最大超时时间设置恢复为默认值。

system tune tcp zwdefend {on|off}

该命令用于启用针对 TCP 零窗口攻击的防护功能。启用该功能后，当系统接收到零窗口报文时，将不再刷新该 TCP 连接的超时时间。如果客户端持续发送零窗口报文，该 TCP 连接在到达最大闲置时间后会被重置。该功能默认设置为禁用。

system tune tcp tso {on|off}

该命令用于启用或禁用 TSO（TCP Segmentation Offload，网卡 TCP 分段）功能。启用 TSO 功能后，由 TCP 层负责的大块数据分段工作将卸载到网卡来处理，从而减轻 CPU 的数据发送负荷。该功能的默认设置为禁用。

system tune tcp pktdropt <packet_drop_option>

该命令用于设置当 TCP 包被未被监听的端口接收并丢弃时的系统行为。该功能有利于防止任何试图探测系统中易被攻击服务的端口扫描，并且能减缓 DoS 攻击。当 TCP 包被未被监听的端口接收并丢弃时，系统默认不返回 TCP RST 报文。

- packet_drop_option** 该参数指定当 TCP 包被未被监听的端口接收并丢弃时的系统行为。取值必须为：
- 0: 表示系统将返回 TCP RST 报文。
 - 1: 表示对于 TCP SYN 报文, 系统将不返回 TCP RST 报文。对于其它 TCP 报文, 系统将返回 TCP RST 报文。
 - 2: 表示系统将不返回 TCP RST 报文。

no system tune tcp pktdropopt

该命令用于将 TCP 包被未被监听的端口接收并丢弃时的系统行为恢复到默认设置。

system tune tcp syncache {on|off}

该命令用于启用或禁用 Syncache 功能。Syncache 功能允许设备记录 TCP 选项设置, 避免 synflood 攻击。该功能默认设置为禁用。



注意: 为使 Window Scale、Timestamp option、SACK 或者 MSS 选项对系统或者特定虚拟服务生效, 必须先启用 TCP Syncache 功能。

system tune tcp option wscale {on|off} [shift_count]

该命令用于启用或禁用 TCP 窗口大小调整功能。该功能默认设置为禁用。

- shift_count** 可选, 该参数指定 TCP 窗口左移的位数。取值必须为 0 到 14 之间的整数。该参数仅在启用 TCP 窗口大小调整功能时才可用。
- 默认值为 3。



注意: 实际使用的窗口大小=TCP 报文中的窗口大小*2^{shift_count}

system tune tcp option timestamp {on|off}

该命令用于启用或禁用 TCP 时间戳功能。该功能默认设置为禁用。

system tune tcp option sack {on|off}

该命令用于启用或禁用 TCP 选择性确认功能。该功能默认设置为禁用。

system tune tcp rmem_max [size]

该命令用于修改系统的最大接收缓存大小。如不配置该命令, 系统默认最大接收缓存大小为 131,072 字节。

size 可选，该参数指定系统最大接收缓存大小，单位为字节。取值必须为 65,536 到 1,073,725,440 之间的整数。

默认值为 131,072。如果不指定参数“size”，系统设置将恢复成默认值。

system tune tcp timewait [timeout]

该命令用于设置 TCP 数据传输的等待时间。如不配置该命令，系统默认的 TCP 数据传输的等待时间为 50 秒。建议管理员在没有取得公司技术支持的情况下不要修改默认设置。

timeout 可选。该参数指定 TCP 数据传输的等待时间，单位为秒。取值必须为 1 到 50 之间的整数。

默认值为 50。如果不指定参数“timeout”，系统设置将恢复成默认值。

no system tune tcp timewait

该命令用于将 TCP 数据传输的等待时间恢复为默认值。

system tune tcp finacc {on|off}

该命令用于启用或禁用 TCP FIN 加速功能。

启用该功能时，在需要关闭 TCP 连接时，如果该连接仍有未发送的数据，系统会通过向最后一个发送的数据报文上添加 FIN 标签来加速 TCP 连接的关闭。

禁用该功能时，系统会将最后一个数据报文和 FIN 报文分开发送。默认情况下，该功能是启用的。

system tune tcp pureack on

该命令用于启用系统在进行 TCP 三次握手时是否将 ACK 报文和数据报文合并发送的功能。启用该功能后，系统进行 TCP 三次握手时，单独发送 ACK 报文。该功能的默认设置为禁用。

system tune tcp pureack off

该命令用于禁用系统在进行 TCP 三次握手时是否将 ACK 报文和数据报文合并发送的功能。禁用该功能后，系统进行 TCP 三次握手时，如果存在数据报文，将 ACK 报文和数据报文同时发送。

show statistics tcp [global|virtual_service|all]

该命令用于显示 TCP 连接的详细信息以及每一种状态下的 TCP 连接数。

global|virtual_service|all 可选。该参数指定显示的连接数统计信息的类型。取值必须为：

- **global**: 显示全局连接数统计信息。
- **虚拟服务名称**: 显示指定的虚拟服务的连接数统计信息。
- **all**: 显示全局及所有虚拟服务的连接数统计信息。

默认值为 **global**。

示例:

```
Demo#show statistics tcp
LISTEN: 1
SYN_SENT: 0
SYN_RCVD: 0
ESTABLISHED: 0
CLOSE_WAIT: 0
FIN_WAIT_1: 0
CLOSING: 0
LAST_ACK: 0
FIN_WAIT_2: 0
TIME_WAIT: 432
```

相比命令 “**show memory**” 的输出结果，该命令中的 “**TIME_WAIT**” 项数值与 “**show memory**” 输出结果中 “**TCP small pcb**” 项的 “**USED**” 列相同。从 “**LISTEN**” 项到 “**FIN_WAIT**” 项所有数值的和与 “**tcp pcb**” 项的 “**USED**” 列所显示的数值相同。

show statistics reset

该命令用于显示 TCP 重置错误码的统计。

示例:

```
Demo(config)#show statistics reset
Total:
ID      Times      Reason
0x2159  1          shunt_reset 为 on 时，连接关闭
```



注意：“Reason” 栏的语言由 “**log language**” 命令的设置决定。

system tune tlsidle <timeout_value>

该命令用于设置闲置状态的 TLS 连接的超时时间。如不配置该命令，闲置 TLS 连接会在 300s 后重置。

timeout_value 该参数指定闲置的 TLS 连接的超时时间，单位为秒。取值必须为 300 至 199,999,999 之间的整数。



注意：如果通过“**slb timeout**”命令设置的超时时间大于“**system tune tlsidle**”命令设置的超时时间，闲置 TLS 连接的超时时间以前者为准，反之以后者的设置为准。

no system tune tlsidle <timeout_value>

该命令用于重置闲置状态的 TLS 连接的超时时间为默认设置。

system tune sslcardtimeout <timeout>

该命令用于设置 SSL 加速卡处理数据时的超时时间。

当不配置该命令时，系统采用默认的超时时间设置，Nitrox V 系列的 SSL 加速卡默认超时时间为 4 秒，Nitrox I、NPX 以及 Nitrox III 系列为 600 秒。

timeout 该参数指定 SSL 卡处理数据时的超时时间，单位为秒，取值必须为 4 至 600 之间的整数。



注意：Intel QAT 卡超时时间为 600 秒，不支持修改超时时间。

no system tune sslcardtimeout

该命令用于将 SSL 加速卡的超时时间恢复为默认设置。

system tune pollactivity <activity>

该命令用于设置系统主进程轮询的活跃度，即连续轮询的次数。

系统支持两种轮询模式：

- 静态模式：在该模式下，当达到指定的连续轮询次数时仍未收到报文时，轮询会暂停 0.1 毫秒后再重新开始。
- 动态模式：在该模式下，CPU 能够自动适应业务负载大小，随业务负载动态变化。

当不配置该命令时，系统默认的轮询活跃度为 64。

activity 该参数指定轮询的活跃度，取值必须为 0 至 2,000,000,000 之间的整数。取值为 0 表示系统将使用动态模式轮询算法。取值不为 0 时，系统将使用静态模式轮询算法。

no system tune pollactivity

该命令用于将系统主进程轮询活跃度重置为默认值。

system tune dispatcher sipudp {on|off}

该命令用于启用或禁用 SIP UDP 分配算法。

启用 SIP UDP 分配算法后，当 SIP 请求命中 SIP UDP 类型的虚服务时，系统会按照该请求的源 IP、目的 IP、源端口和目的端口计算保持关系，将请求更均衡地分配给多个 CPU 内核。

禁用 SIP UDP 分配算法后，系统只按照 SIP 请求的源端口和目的端口计算保持关系。

该算法的默认设置为禁用。

system tune dispatcher epolicy on

该命令用于启用 ePolicy 分配算法。

启用 ePolicy 分配算法后，当请求命中 ePolicy 模块时，系统会按照该请求的源 IP、目的 IP、源端口和目的端口计算保持关系，将请求更均衡地分配给多个 CPU 内核。禁用 ePolicy 分配算法后，系统只按照请求的源端口和目的端口计算保持关系。

该算法的默认设置为禁用。

system tune dispatcher epolicy off

该命令用于禁用 ePolicy 分配算法。

system tune rxmode {interrupt|poll} [sleep_duration]

该命令用于配置 DPDK 接口的接收模式。命令 “**system tune rxmode interrupt**” 用于设置基于中断的接收模式，命令 “**system tune rxmode poll [sleep_duration]**” 用于设置基于轮询的接收模式。

当不配置该命令时，DPDK 接口默认会使用基于轮询的接收模式，流量较少时的睡眠时长为 100 微秒。

sleep_duration 可选，该参数指定采用基于轮询的接收模式下流量较少时的睡眠时长，单位为微秒。取值必须为 0 至 100 之间的整数。取值为 0 时，轮询将不会停止。

默认值为 100。

system tune arp timeout <timeout>

该命令用于修改 ARP 表项的超时时间。

当不配置该命令时，默认的超时时间为 3600 秒。

timeout 该参数指定 ARP 表项的超时时间，取值必须为 1 至 2,147,483,647 之间的整数。

system tune ndp timeout <timeout>

该命令用于修改 NDP 表项的超时时间。

当不配置该命令时，默认的超时时间为 86,400 秒。

timeout 该参数指定 NDP 表项的超时时间，取值必须为 1 至 2,147,483,647 之间的整数。

no system tune arp timeout

该命令用于将 ARP 表项的超时时间设置恢复为默认设置。

no system tune ndp timeout

该命令用于将 NDP 表项的超时时间设置恢复为默认设置。

system tune icmp replylimit [limit]

该命令用于设置每秒 ICMP 响应阈值。当每秒收到的 ICMP 响应数量超过指定的阈值时，后续的 ICMP 响应会被丢弃。

当不配置该命令时，系统默认的每秒 ICMP 响应阈值为 1000。

limit 可选，该参数指定每秒 ICMP 响应阈值，取值必须为 0 至 20,000 之间的整数。取值为 0 时表示不限制每秒 ICMP 响应数量。

默认值为 1000。

no system tune icmp replylimit

该命令用于将每秒 ICMP 响应阈值恢复为默认设置。

system tune rtos {on|off}

该命令用于启用或禁用实时操作系统（Real Time Operating System, RTOS）功能。该功能启用后，在使用客户端认证功能的 TCPS 负载均衡场景中，系统的响应速度将明显提升。对“**system tune rtos**”命令的配置仅在重启后生效且仅在物理设备上生效。该功能默认设置为禁用。

show system rtos

该命令用于显示 RTOS 功能的配置及开启状态。

system tune segment iprange <ip_address> {netmask|prefix}

该命令用于为分区 IP 自动分配 NAT 地址的功能配置一个 IP 网段。配置 IP 网段后，在处理分区 IP 的 NAT 转换时，系统将自动从该 IP 网段中选择一个 IP 地址作为分区 IP 的 NAT 转换地址。

ip_address 该参数指定 IP 网段的 IP 地址，可以为 IPv4 或 IPv6 地址。

netmask|prefix 该参数指定 IP 网段对应的子网掩码或前缀长度。

- “mask” 用于配置 IPv4 地址对应的子网掩码，取值可以为点分地址格式或 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，取值为 0 到 128 之间的整数。

no system tune segment iprange <ip_address> {netmask|prefix}

该命令用于删除为分区 IP 自动分配 NAT 地址的功能配置的 IP 网段。

show system tune

该命令用于显示系统优化参数设置。

clear system tune

该命令用于将系统优化参数全部恢复成默认设置。

system thread {single|auto}

该命令用于设置系统的运行线程模式。修改了系统的运行线程模式后，必须重启系统修改才会生效。

“system thread single” 表示系统单线程运行。

“system thread auto” 表示系统多线程运行。

默认为多线程运行。

show system thread

该命令用于显示系统的运行线程配置。

ip nameserver <ip_address>

该命令用于添加域名服务器。最多允许添加 3 台域名服务器。

ip_address 该参数指定域名服务器的 IP 地址。

no ip nameserver <ip_address>

该命令用于删除指定的域名服务器。

show ip nameserver

该命令用于显示域名服务器的 IP 地址。

fwd mode <fwd_mode>

该命令用于设置系统端口转发以及地址转换的工作模式。设备支持配置的端口转发的方式有非透明模式（需要转换源 IP 地址）和透明模式两种。系统默认的工作模式为透明模式。

fwd_mode 该参数指定端口转发以及地址转换的工作模式。取值必须为：

- **nontransparent**：表示非透明模式。在非透明模式下，将使用系统的管理 IP 做源 IP。
- **transparent**：表示透明模式。在透明模式下，将使用客户端 IP 做源 IP。



注意：端口转发功能不支持 FTP 协议的快速转发，在这种情况下，建议使用 SLB 功能。

no fwd mode

该命令用于将系统端口转发以及地址转换的工作模式恢复成默认设置。

show fwd

该命令用于显示系统端口转发以及地址转换的工作模式。

system date <year> <month> <date>

该命令用于设定设备的日期，适用于不依赖时间同步服务器的网络环境，所以如果需要设置设备日期为 2010 年 10 月 20 号，应该执行以下命令：

```
Demo(config)#system date 10 10 20
```

system time <hour> <minute> <second>

该命令用于设定设备的时间，适用于不依赖时间同步服务器的网络环境。设备采用 24 小时计时法，所以如果需要设置设备时间为晚上 11:33:51，应该执行以下命令：

```
Demo(config)#system time 23 33 51
```

system timezone

该命令用于设置系统时区。系统默认的时区值为“GMT”。设备通过三个步骤设置时区：

1. 选择大陆。
2. 选择国家。

3. 选择时间区域。



注意：在时区设置过程中，可以通过输入 0，退到上一步。例如，输入 0，可以从国家清单页退到第一步选择大陆。

show system timezone

该命令用于显示当前的系统时区设置。

clear system timezone

该命令用于将当前的系统时区设置恢复为默认值。

show date

该命令用于显示当前设备的日期和时间。

ntp on [index]

该命令用于启用 NTP（Network Time Protocol，时间同步协议）功能，并设置通过哪种程序进行时间同步。启用该功能前，必须先使用命令“**ntp server**”配置 NTP 服务器。启用该功能后，系统将与使用命令“**ntp server**”配置的 NTP 服务器进行时间同步。该功能默认设置为禁用。

index 可选，该参数指定时间同步程序的索引，取值必须为：

- 0：表示使用 ntpd 程序同步时间。
- 1：表示使用 ntpdate 程序同步时间。

默认值为“0”。



注意：

- 当 NTP 服务器的数量超过 1024 时，使用 ntpd 程序同步时间可能会失败，这种情况下，建议切换到 ntpdate 程序。
- 在切换 NTP 使用的时间同步程序前，例如从 ntpd 切换到 ntpdate，必须先禁用 NTP 功能。否则，切换不生效。

ntp off

该命令用于禁用 NTP 功能。

ntp server <ip_address> [version]

该命令用于配置 NTP 服务器。

ip_address 该参数指定 NTP 服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

version 该参数指定 NTP 版本号。取值必须为 1 到 4 之间的整数。

默认值为 4。

no ntp server <ip_address> [version]

该命令用于删除指定的 NTP 服务器。如不指定参数“version”，将删除 NTP 版本号为 4 的 NTP 服务器。

show ntp

该命令用于显示 NTP 功能相关信息，当 NTP 功能采用 ntpd 同步时间时，该命令显示 NTP 配置，包括当前服务器的时间同步状况和连接状况。当 NTP 功能采用 ntpdate 同步时间时，该命令会显示 NTP 服务器的 IP 地址。NTP 功能的开启状态以及 ntpdate 程序的执行结果。

clear ntp

该命令用于清除 NTP 配置。

hostname <host_name>

该命令用于设置设备的主机名称。默认的主机名为“AN”

host_name	该参数指定设备的主机名称，取值必须为长度不超过 64 个字符的字符串，支持字母、数字、特殊字符。当取值由纯数字组成或者包含特殊字符时，名称必须置于双引号内。以下特殊符号在命名时被禁止使用：“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“ ”、“`”和空格。

no hostname

该命令用于将设备的主机名称恢复为默认值。

show hostname

该命令用于显示设备的主机名称。

system mail external {on|off}

该命令用于启用或禁用外部 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）邮件服务器功能。在启用该功能前，请先使用命令“**system mail external server**”配置一个外部 SMTP 邮件服务器。启用该功能后，系统将作为邮件客户端，通过外部 SMTP 邮件服务器发送报警邮件。如果禁用该功能，系统将作为邮件客户端，通过内置的本地邮件服务器发送报警邮件。目前系统只支持外部 SMTP 邮件服务器。该功能默认设置为禁用。

system mail external server <server_address> [server_port] [ssl_flag]

该命令用于配置外部 SMTP 邮件服务器。系统只允许配置一台外部 SMTP 邮件服务器。

当系统已经存在 SMTP 邮件服务器时，该命令可以用于修改 SMTP 邮件服务器的配置。

server_address	该参数指定外部 SMTP 邮件服务器的域名或 IPv4 地址，取值必须为 IPv4 地址或长度不大于 64 个字节的字符串，支持字母、数字、特殊字符，必须置于双引号内。
server_port	可选，该参数指定外部 SMTP 邮件服务器的端口号。取值必须为 0 到 65,535 之间的整数。 默认值为 25。
ssl_flag	可选，该参数指定系统与外部 SMTP 邮件服务器的通信是否使用 SSL 或 TLS 协议加密。取值必须为： • 0：表示不使用 SSL 或 TLS 协议。 • 1：表示使用 SSL 或 TLS 协议。 默认值为 0。

no system mail external server

该命令用于删除外部 SMTP 邮件服务器。

system mail external user <username> <password>

该命令用于配置通过外部 SMTP 邮件服务器发送报警邮件的发件人 email 账户。外部 SMTP 邮件服务器在发送报警邮件前，会先对发件人 email 账户进行验证。只有发件人的 email 账户合法，外部 SMTP 邮件服务器才会发出来自发件人的邮件。

当系统已经存在 email 账户设置时，该命令可以用于修改已有账户的用户名和密码。

username	该参数指定发件人的 email 地址。取值必须为长度不大于 32 个字节的字符串，支持字母、数字、特殊字符，用户名必须置于双引号内。
password	该参数指定发件人的账户密码。取值必须为长度不大于 64 个字节的字符串，置于双引号内。

no system mail external user

该命令用于删除通过外部 SMTP 邮件服务器发送报警邮件的发件人 email 账户。

system mail from <from_string>

该命令用于修改通过本地邮件服务器发送报警邮件的发件人 email 账户。默认为“%h<alert@log.domain>”。

from_string 该参数指定发送报警邮件的发件人 email 账户。取值必须置于双引号内。参数支持配置以下转义字符串：

- %h: 表示通过命令“hostname”定义的主机名称。
- %q: 表示英文双引号。例如，如果要使用“an”，则需要输入“%qan%q”。
- %: 表示百分号。

注意：在以上转义字符串中，第一个字符“%”为转义字符，不能单独使用。

示例：

```
Demo(config)#system mail from "admin@abc.com"
```

配置以上命令后，管理员接收到的报警邮件的发件人为“admin@abc.com”。

no system mail from

该命令用于将通过本地邮件服务器发送报警邮件的发件人恢复为默认设置。

system mail hostname <host_string> [option]

该命令用于配置通过本地邮件服务器发送报警邮件的主机名称。默认为“%l.alert_pseudo_domain”。

host_string 该参数指定发送报警邮件的主机名称。取值必须为全称域名，置于双引号内，例如“abc.com”。以下特殊符号被禁止使用：“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“\”。

参数支持配置以下转义字符串：

- %h: 表示通过命令“hostname”定义的主机名称。
- %l: 表示主机名称中第一个“.”位置之前的部分。

注意：在以上转义字符串中，第一个字符“%”为转义字符，不能单独使用。

option 可选。该参数指定当主机名称和邮箱服务器域名相同时是否停止发送报警邮件。取值必须为：

- 1: 表示当主机名称和邮箱服务器域名相同时仍将发送报警邮件。
- 0: 表示当主机名称和邮箱服务器域名相同时停止发送报警邮件。

默认值为 0。

no system mail hostname

该命令用于将通过本地邮件服务器发送的报警邮件的主机名称恢复为默认设置。

show system mail

该命令用于显示本地邮件服务器和外部 SMTP 邮件服务器配置。

clear system mail

该命令用于将本地邮件服务器和外部 SMTP 邮件服务器恢复为默认配置，同时将删除外部 SMTP 邮件服务器和通过外部 SMTP 邮件服务器发送报警邮件的发件人 email 账户。

system mail relay {on|off}

该命令用于启用或禁用系统邮件中继功能。启用该功能后，当向指定域名的 email 地址发送报警邮件时，系统先将报警邮件发给邮件中继服务器再进行转发。启用该功能前，必须先使用命令“system mail relay server”配置邮件中继服务器。该功能默认设置为禁用。

system mail relay server <host_name> <relay_server>

该命令用于为指定域名的邮件服务器配置邮件中继服务器。

host_name 该参数指定邮件服务器的域名。

relay_server 该参数指定邮件中继服务器的域名或者 IPv4 地址。如果参数取值为 IPv4 地址，必须置于双引号内。如果参数取值为邮箱域名，请确保该域名能够被设备的 DNS 服务器解析。

示例：

```
Demo(config)#system mail relay server "mailserver.com" "relay.com"
Demo(config)#system mail relay on
```

配置以上命令后，当系统向包含域名“mailserver.com”的 email 地址发送报警邮件时，将报警邮件发给邮件中继服务器“relay.com”进行转发。

no system mail relay server <host_name>

该命令用于删除为指定邮件服务器配置的邮件中继服务器。

show system relay

该命令用于显示系统邮件中继功能的配置及状态信息。

clear system relay

该命令用于将系统邮件中继功能恢复为默认配置。

system interactive {on|off}

该命令用于启用或禁用 CLI 命令交互模式。启用该功能后，系统将会显示更多的命令细节信息。该功能默认设置为禁用。

show system interactive

该命令用于显示 CLI 命令交互模式的设置。

system command timeout <timeout>

该命令用于设置系统执行“**config file**”或“**config memory**”命令时的超时时间。系统默认执行上述命令的超时时间为 120 秒。

timeout 该参数指定系统执行“**config file**”或“**config memory**”命令时的超时时间，单位为秒。取值必须为 0 或者 30 至 65,535 之间的整数。取值为 0 表示没有超时时间。

show system command timeout

该命令用于查看系统执行“**config file**”或“**config memory**”命令的超时时间设置。

system command override on

该命令用于启用命令覆盖功能。启用该功能后，如果对类型和名称相同的虚拟服务或后台服务重复执行命令，之前的命令配置将被覆盖。该功能默认设置为启用。



注意：二层 IP 类型虚拟服务不支持覆盖已有配置。

system command override off

该命令用于禁用命令覆盖功能。

show system command override

该命令用于显示命令覆盖功能的配置。

switch weblink <url>

该命令用于配置设备内置交换机的管理地址。管理员可以通过该地址在设备的 WebUI 中对交换机进行管理和配置。

url 该参数指定内置交换机的 URL 地址。

2.1 网站分类

webclassify license <license_key>

该命令用于导入网站分类功能的许可密钥。该许可密钥允许设备使用 Webroot BrightCloud 威胁情报服务提供的网站分类功能。Webroot 为该功能提供 30 天的免费试用许可，试用许可证到期后，Webroot 服务器会拒绝系统的在线访问，同时系统会停止向 Webroot 服务器发送网站类别查询请求。

license_key 该参数指定许可密钥。请联系公司客户支持并提供设备型号和序列号获取网站分类功能的许可密钥。

show webclassify license

该命令用于显示网站分类功能许可证的相关信息，包括 OEM、设备 ID、序列号和许可类型（试用许可证或正式许可证）以及许可密钥的发布信息和有效期。

webclassify {on|off}

该命令用于启用或禁用全局网站分类功能。该功能的默认设置为禁用。

webclassify cloud {on|off}

该功能用于启用或禁用网站分类在线查询功能。该功能仅在全局网站分类功能启用后（“**webclassify on**”）才可以启用。网站分类在线查询功能默认设置为禁用。禁用该功能时，系统在收到访问指定网站的流量时只进行本地查询。启用该功能后，如果本地查询失败或本地缓存的条目超时，系统会连接到 Webroot BrightCloud 服务器进行在线查询。



注意：在禁用网站分类在线查询功能的短暂时间内，由于异步通信导致的时间间隔，系统仍会连接到 Webroot BrightCloud 服务器进行在线查询。

show webclassify settings

该命令用于显示全局网站分类功能和网站分类在线查询功能的配置。

show webclassify status

该命令用于显示网站分类功能相关的全局配置，例如 WebRoot BrightCloud 服务的域名、License 状态、网址分类在线查询功能的开启状态、数据库版本等等。

show webclassify url categories

该命令用于显示系统支持查询的所有网站类别。

show webclassify url category <website_name>

该命令用于查询指定网址的网站类别。如果系统从本地缓存或数据库可以查询到网址的网站类别，则会快速返回查询结果，否则会有一定延迟，最大延迟为 20 秒。

website_name 该参数指定网址的域名，取值必须为长度不大于 256 个字节的字符串，例如 “google.com”。

2.2 网桥

bridge name <bridge_name>

该命令用于创建一个网桥。系统支持配置最多 16 个网桥。

bridge_name 该参数指定网桥的名称，取值必须为长度不大于 31 个字节的字符串。

no bridge name <bridge_name>

该命令用于删除指定的网桥。

bridge member <bridge_name> <system_ifname> [broadcast_option]

该命令用于将一个系统接口加入指定的网桥。每个网桥最多可添加 32 个系统接口作为成员接口。

bridge_name 该参数指定网桥的名称，取值必须为长度不大于 31 个字节的字符串。

system_ifname 该参数指定系统接口的名称，默认为 port1、port2、port3、port4……。 (管理员可以通过 “**interface name**” 命令来自定义系统接口名称。)

broadcast_option 可选。该参数指定成员接口是否可以发送广播和多播报文。取值必须为：

- **yes**: 表示允许成员接口发送广播和多播报文。
- **no**: 表示禁止成员接口发送广播和多播报文。

默认值为 “yes”。

no bridge member <bridge_name> <system_ifname>

该命令用于从指定的网桥中删除一个成员接口。

bridge vlan <bridge_name> <system_ifname> <vlan_id>

该命令用于为指定网桥的指定成员接口添加一个 VLAN 标签，携带该 VLAN 标签的报文可以通过该接口转发。每个成员接口可以添加最多 4094 个 VLAN 标签。

bridge_name	该参数指定网桥的名称。
system_ifname	该参数指定系统接口的名称, 默认为 port1、port2、port3、port4……。 (管理员可以通过 “ interface name ” 命令来自定义系统接口名称。)
vlan_id	该参数指定 VLAN 接口的标识 ID, 取值必须为 1 至 4094 之间的整数。

no bridge vlan <bridge_name> <system_ifname> <vlan_ID>

该命令用于将指定网桥中的一个成员接口上的 VLAN 接口删除。

clear bridge vlan <bridge_name>

该命令用于清除指定网桥的所有 VLAN 接口。

bridge apprule <bridge_name> <src_ip> <src_port> <dst_ip> <dst_port>
<protocol>

该命令用于为指定的网桥配置一条流量过滤规则, 命中该规则的流量将被转发至上层协议, 例如 HTTP、DNS、HTTPS、FTP 等, 其他流量将被直接转发。

bridge_name	该参数指定网桥的名称。
src_ip	该参数指定需要过滤的流量的源 IP 地址。取值为 0.0.0.0 时表示所有 IP 地址。
src_port	该参数指定需要过滤的流量的源端口号, 取值必须为 0 至 65535 之间的整数。取值为 0 时表示所有端口号。
dst_ip	该参数指定需要过滤的流量的目的 IP 地址。取值为 0.0.0.0 时表示所有 IP 地址。
dst_port	该参数指定需要过滤的流量的目的端口号, 取值必须为 0 至 65535 之间的整数。取值为 0 时表示所有端口号。
protocol	该参数指定需要过滤的流量的传输层协议类型, 取值必须为 “tcp” 或 “udp”。

no bridge apprule <bridge_name> <src_ip> <src_port> <dst_ip> <dst_port>

该命令用于删除指定的网桥的一条流量过滤规则。

clear bridge apprule [bridge_name]

该命令用于清除指定网桥的所有流量过滤规则。如不指定参数“bridge_name”，则清除所有网桥的所有流量过滤规则。

show bridge config [bridge_name]

该命令用于显示指定网桥相关的所有配置。如不指定参数“bridge_name”，则显示所有网桥相关的所有配置。

clear bridge config [bridge_name]

该命令用于清除指定网桥相关的所有配置。如不指定参数“bridge_name”，则清除所有网桥相关的所有配置。

show bridge mactable [bridge_name|filter_string]

该命令用于显示指定网桥或符合指定过滤字符串的 MAC 表项信息。

bridge_name|filter_string 可选。该参数指定网桥的名称或用于匹配 MAC 表项的字符串。网桥名称和过滤字符串不能同时配置。当不配置该参数时，会显示所有网桥的 MAC 表项信息。

show bridge appflowtable

该命令用于显示网桥的流量表项信息。

show bridge status [bridge_name]

该命令用于显示指定网桥的状态信息。如不指定参数“bridge_name”，则显示所有网桥的状态信息。

show statistics bridge [bridge_name]

该命令用于显示指定网桥相关的所有统计数据。如不指定参数“bridge_name”，则显示所有网桥相关的统计数据。

2.3 端口镜像

spanport filterlist name <filterlist_name>

该命令用于配置一条过滤列表。系统支持配置最多 8 条过滤列表。

filterlist_name 该参数指定过滤列表的名称，取值必须为长度不大于 31 个字节的字符串。

no spanport filterlist name <filterlist_name>

该命令用于删除指定的过滤列表。

show spanport filterlist [filterlist_name]

该命令用于显示指定的过滤列表。如不指定参数“filterlist_name”，则显示所有的过滤列表。

clear spanport filterlist

该命令用于清除所有的过滤列表及其包含的过滤规则。

spanport filterlist member <filterlist_name> <interface_name> <src_ip>
<src_port> <dst_ip> <dst_port> <protocol> [direction]

该命令用于添加一条过滤规则到指定的过滤列表，系统会基于过滤规则过滤需要被复制的报文。每个过滤列表最多可添加 8 条过滤规则。建议过滤规则的各项匹配条件之间避免重叠，如果一个报文同时命中多条过滤规则，系统只会选择匹配其中的一条。

filterlist_name	该参数指定已存在的过滤列表的名称。
interface_name	该参数指定端口镜像的源端口，即通过该端口的报文将被复制，取值必须为系统接口的名称，例如“port1”、“port2”、“port3”等等。
src_ip	该参数指定需要复制的报文的源 IP 地址，取值必须为 IPv4 地址，取值为“0.0.0.0”时表示所有 IP 地址。
src_port	该参数指定需要复制的报文的源端口号，取值必须为 0 至 65,535 之间的整数。取值为 0 时表示所有端口号。
dst_ip	该参数指定需要复制的报文的目的 IP 地址，取值必须为 IPv4 地址，取值为“0.0.0.0”时表示所有 IP 地址。
dst_port	该参数指定需要复制的报文的目的端口号，取值必须为 0 至 65,535 之间的整数。取值为 0 时表示所有端口号。
protocol	该参数指定需要复制的报文所使用的传输层协议，取值必须为“tcp”、“udp”或“all”（TCP 和 UDP）。
direction	可选，该参数指定需要复制的报文的方向，取值必须为： • both: 表示双向（入向和出向）报文都复制。 • inbound: 表示只复制入向报文。 • outbound: 表示只复制出向报文。 默认值为 both。

no spanport filterlist member <filterlist_name> <interface_name> <src_ip>
<src_port> <dst_ip> <dst_port> <protocol> <direction>

该命令用于从指定的过滤列表中删除一条过滤规则。

spanport devicegroup name <group_name> <group_method>

该命令用于配置接收复制报文的安全设备服务组，并设置系统向该服务组发送复制报文的方式。系统支持配置最多 8 个安全设备服务组。

group_name	该参数指定安全设备服务组的名称，取值必须为长度不大于 31 个字节的字符串。
group_method	该参数指定系统向服务组发送复制报文的方式，取值必须为： • lb: 表示将复制的报文按照源 IP 和目的 IP 的哈希值负载均衡到服务组内的安全设备，源 IP 和目的 IP 哈希值相同的报文会被持续发送到同一个安全设备。 • dup: 表示服务组内的每个安全设备都会收到相同的复制报文。

no spanport devicegroup name <group_name>

该命令用于删除指定的安全设备服务组。

show spanport devicegroup [group_name]

该命令用于显示指定的安全设备服务组配置。如不指定参数“group_name”，则显示所有的安全设备服务组配置。

clear spanport devicegroup

该命令用于清除所有的安全设备服务组及其成员。

spanport devicegroup member <group_name> <interface_name> <mac> [sort_string]

该命令用于将一个安全设备作为成员添加到指定的安全设备服务组，每个服务组支持添加最多 8 个成员。

group_name	该参数指定已存在的安全设备服务组的名称。
interface_name	该参数指定端口镜像的目的端口，取值必须为系统接口的名称，例如“port1”、“port2”、“port3”等等。端口镜像的目的端口不能和源端口所在的系统接口相同。且不能同时用于其他业务。
mac	该参数指定安全设备的 MAC 地址。
sort_string	可选。该参数指定排序字符串。当需要从两台设备上复制报文，且复制的报文以负载均衡方式向两台或多台安全设备镜像时，该参数必须配置，且属于同一个服务组

的成员的排序字符串的值必须相同。

默认值为“abc”。



注意：用于端口镜像功能的目的端口不支持转发 VLAN 报文到安全设备，对于携带 VLAN 标签的复制报文，目的端口会在转发前剥离 VLAN 标签。

no spanport devicegroup member <group_name> <interface_name>
<mac>

该命令用于从指定的安全设备服务组里删除一个成员。

spanport policy <policy_name> <filterlist_name> <group_name>

该命令用于配置一条端口镜像策略来关联指定的过滤列表和指定的安全设备服务组，即将端口镜像的源端口和目的端口关联。每个过滤列表只能关联到一个安全设备服务组。系统支持配置最多 8 条端口镜像策略，建议通过策略关联的两个端口使用相同的网卡类型和 MTU 配置。

policy_name 该参数指定端口镜像策略的名称，取值必须为长度不大于 31 个字节的字符串。

filterlist_name 该参数指定已存在的过滤列表名称。

group_name 该参数指定已存在的安全设备服务组的名称。

no spanport policy <policy_name>

该命令用于删除指定的端口镜像策略。

show spanport policy [policy_name]

该命令用于显示指定的端口镜像策略。如不指定参数“policy_name”，则显示所有的端口镜像策略。

clear spanport policy

该命令用于清除所有的端口镜像策略。

clear spanport config

该命令用于清除端口镜像相关的所有配置。

show statistics spanport

该命令用于显示端口镜像的统计数据。

clear statistics spanport

该命令用于清除端口镜像的统计数据。

2.4 系统健康检查

本节介绍系统健康检查条件的配置命令。系统健康检查功能既适用于只有一台设备的场景，也可以应用于部署了两台或多台设备（HA）的场景。当配置了系统健康检查功能时，HA 功能可以使用系统健康检查作为 HA 节点的失效切换条件。

monitor system {on|off}

该命令用于启用或禁用系统健康检查功能。该功能的默认设置为启用。启用系统健康检查功能后，设备将基于以下默认配置进行健康检查：

- **monitor system cpu overheat 75 5000 3 3**
- **monitor system cpu utilization 60 5000 3 3**
- **monitor system ssl ae 60 5000 3 3**
- **monitor system ssl se 60 5000 3 3**
- **monitor system sslcard 10000 3 3**
- **monitor system memory utilization system 90 5000 3 3**
- **monitor system memory utilization network 90 5000 3 3**
- **monitor system memory utilization swap 20 5000 3 3**
- **monitor system memory utilization connection 95 5000 3 3**
- **monitor system ntp 5000 3 3**
- **monitor system disk system 60 60**
- **monitor system disk data 80 60**

管理员可以根据需要修改以上默认配置，也可以修改健康检查条件配置，配置命令如下。



注意：管理员修改健康检查条件后，系统会立即将相关状态标记为“Normal”。

monitor network gateway <unit_name> <gateway_ip> <condition_name>
[interval] [up_check_times] [down_check_times] [source_ip]

该命令用于为指定 HA 节点配置网关健康检查条件。

unit_name 该参数指定 HA 节点的名称。在非 HA 场景，该参数的取值应为空（用“”表示）。

gateway_ip 该参数指定 HA 节点的网关的 IP 地址，取值必须为 IPv4

	或 IPv6 地址。
condition_name	该参数指定该健康检查条件的名称，取值范围为 GATEWAY_1~GATEWAY_32。
interval	可选。该参数指定健康检查的时间间隔，单位为毫秒。取值必须为 1000 至 100,000 之间的整数。 默认值为 1000。
up_check_times	可选。该参数指定判断网关可用的连续健康检查成功次数。取值必须为 3 至 10 之间的整数。 默认值为 3。
down_check_times	可选。该参数指定判断网关不可用的连续健康检查失败次数。取值必须为 3 至 1000 之间的整数。 默认值为 15。
source_ip	可选。该参数指定对网关 ping 时使用的源 IP 地址，支持 IPv4 和 IPv6 地址。 默认值为空。

no monitor network gateway <unit_name> <gateway_ip>

该命令用于删除为指定 HA 节点的网关配置的健康检查条件。

clear monitor network gateway

该命令用于删除所有的网关健康检查条件。

monitor network imc tcp <imc_health_check_name> <ip> <port> [interval] [timeout] [max_retries]

该命令用于为集中管理平台 IMC 配置 TCP 健康检查条件。系统最多支持为 8 个集中管理平台 IMC 配置 TCP 健康检查条件。

imc_health_check_name	该参数指定 TCP 健康检查的名称，取值必须为长度不大于 128 个字节的字符串。
ip	该参数指定集中管理平台 IMC 的 IP 地址，取值必须为 IPv4 或 IPv6 地址。
port	该参数指定集中管理平台 IMC 的端口，取值必须为 1 到 65,535 之间的整数。
interval	可选。该参数指定 TCP 健康检查的时间间隔，单位为秒，取值必须为 3 至 86,400 之间的整数。默认值为 5。

timeout	可选, 该参数指定 TCP 健康检查的超时时间, 单位为秒, 取值必须为 3 到 86,400 之间的整数。默认值为 5。
max_retries	可选。该参数指定标识 TCP 健康检查的状态为 Up 或者 Down 需要的连续健康检查成功或失败的次数。取值必须为 1 至 10 之间的整数。 默认值为 3, 表示如果连续 3 次健康检查的结果都是 Up, 则系统将集中管理平台的状态设置为 Normal; 如果连续 3 次健康检查的结果都是 Down, 则系统将集中管理平台的状态设置为 Abnormal。

no monitor network imc tcp <imc_health_check_name>

该命令用于删除指定的集中管理平台 IMC 的 TCP 健康检查条件。

show monitor network imc tcp

该命令用于显示所有集中管理平台 IMC 的 TCP 健康检查条件。

clear monitor network imc tcp

该命令用于清除所有集中管理平台 IMC 的 TCP 健康检查条件。

show monitor network imc status

该命令用于显示所有集中管理平台 IMC 的 TCP 健康检查状态。

monitor system bond <bond_id> [threshold]

该命令用于为指定聚合接口配置健康检查条件。

bond_id	该参数指定已有的聚合接口的 ID。
threshold	可选。该参数指定聚合接口状态切换为 Down 的阈值, 单位为百分号 (%), 取值必须为 1 至 100 之间的整数。聚合接口中状态为 “Down” 的系统接口所占的比例小于设定的阈值时, 聚合接口的状态为 “Up”, 否则, 聚合接口的状态为 “Down”。 默认值为 50。



注意: 如果聚合接口健康检查状态显示为 “Down”, 不代表该聚合接口损坏, 仅表示聚合接口中系统接口的状态为 “Down” 的比例等于或超过设定的阈值。

no monitor system bond <bond_id>

该命令用于删除指定的聚合接口健康检查条件。

clear monitor system bond all

该命令用于将所有聚合接口健康检查条件恢复为默认配置。

monitor system cpu overheat *[temperature] [interval] [up_check_times]*
[down_check_times]

该命令用于配置 CPU 温度健康检查条件。

temperature	可选。该参数指定 CPU 温度的温度阈值，单位为摄氏度（℃）。取值必须为 1 至 100 之间的整数。 默认值为 75。
interval	可选。该参数指定健康检查的时间间隔，单位为毫秒。取值必须为 5000 至 1,000,000 之间的整数。 默认值为 5000。
up_check_times	可选。该参数指定连续检查出 CPU 温度未超过 CPU 温度阈值的次数。取值必须为 3 至 10 之间的整数。 默认值为 3。
down_check_times	可选。该参数指定连续检查出 CPU 温度超过 CPU 温度阈值的次数。取值必须为 3 至 10 之间的整数。 默认值为 3。

no monitor system cpu overheat

该命令用于删除 CPU 温度健康检查条件。

monitor system cpu utilization *[fatal_percent] [interval] [up_check_times]*
[down_check_times]

该命令用于配置 CPU 使用率健康检查条件。

fatal_percent	可选。该参数指定 CPU 使用率的阈值，单位为百分号（%）。取值必须为 1 至 100 之间的整数。 默认值为 60。
interval	可选。该参数指定健康检查的时间间隔，单位为毫秒。取值必须为 5000 至 1,000,000 之间的整数。 默认值为 5000。
up_check_times	可选。该参数指定连续检查出 CPU 使用率未超过阈值的次数。取值必须为 3 至 10 之间的整数。 默认值为 3。
down_check_times	可选。该参数指定连续检查出 CPU 使用率超过阈值的

次数。取值必须为 3 至 10 之间的整数。

默认值为 3。

no monitor system cpu utilization

该命令用于删除 CPU 使用率健康检查条件。

clear monitor system cpu all

该命令用于将 CPU 温度和使用率的健康检查条件恢复为默认设置。

monitor system sslcard [interval] [up_check_times] [down_check_times]

该命令用于配置 SSL 加速卡健康检查条件。

interval 可选。该参数指定健康检查的时间间隔，单位为毫秒。
取值必须为 10,000 至 3,600,000 之间的整数。

默认值为 10,000。

up_check_times 可选。该参数指定连续检查出 SSL 加速卡状态为 Up 的次数。取值必须为 1 至 10 之间的整数。

默认值为 3。

down_check_times 可选。该参数指定连续检查出 SSL 加速卡状态为 Down 的次数。取值必须为 1 至 10 之间的整数。

默认值为 3。



注意：SSL 加速卡健康检查的时间间隔必须大于 SSL 加速卡处理数据时的超时时间（通过“**system tune sslcardtimeout**”命令配置）。

no monitor system sslcard

该命令用于删除 SSL 加速卡健康检查条件。

monitor system ssl {ae|se} [fatal_percent] [interval] [up_check_times] [down_check_times]

该命令用于设置 SSL 加速卡（QAT 卡和 Nitrox V 系列加速卡）的 AE 或 SE 内核使用率健康检查条件。

默认情况下，设备将只为 Nitrox V 系列加速卡加载 AE 或 SE 内核使用率健康检查条件。

fatal_percent 可选。该参数指定 SSL 加速卡的 AE 或 SE 内核使用率的阈值，单位为百分号（%）。取值必须为 1 至 100 之间的整数。

	默认值为 60。
interval	可选。该参数指定健康检查的时间间隔，单位为毫秒。 取值必须为 5000 至 1,000,000 之间的整数。 默认值为 5000。
up_check_times	可选。该参数指定连续检查出 SSL 加速卡的 AE 或 SE 内核使用率未超过阈值的次数。取值必须为 3 至 10 之 间的整数。 默认值为 3。
down_check_times	可选。该参数指定连续检查出 SSL 加速卡的 AE 或 SE 内核使用率超过阈值的次数。取值必须为 3 至 10 之 间的整数。 默认值为 3。

no monitor system ssl {ae|se}

该命令用于删除 SSL 加速卡的 AE 或 SE 内核使用率健康检查条件。

clear monitor system ssl all

该命令用于删除 SSL 加速卡的 AE 和 SE 内核使用率健康检查条件。

monitor system memory utilization <memory_type> [fatal_percent] [interval] [up_check_times] [down_check_times]

该命令用于配置内存使用率健康检查条件，包括系统内存、网络内存、连接内存和 SWAP 内存。

memory_type	该参数指定需要检查的内存使用率类型，取值必须为： • system：表示系统内存使用率 • network：表示网络内存使用率 • connection：表示连接内存使用率 • swap：表示 SWAP 内存使用率
fatal_percent	可选。该参数指定内存使用率的阈值，单位为百分号（%）。取值必须为 1 至 100 之间的整数。 不同类型内存使用率的默认值不同，分别为： • 系统内存：90 • 网络内存：90

- 连接内存：20
- SWAP 内存：95

interval	可选。该参数指定健康检查的时间间隔，单位为毫秒。 取值必须为 5000 至 1,000,000 之间的整数。 默认值为 5000。
up_check_times	可选。该参数指定连续检查出内存使用率未超过阈值的次数。取值必须为 3 至 10 之间的整数。 默认值为 3。
down_check_times	可选。该参数指定连续检查出内存使用率超过阈值的次数。取值必须为 3 至 10 之间的整数。 默认值为 3。

no monitor system memory utilization <memory_type>

该命令用于删除指定类型的内存使用率健康检查条件。

monitor system disk system [fatal_percent] [interval]

该命令用于配置系统硬盘分区使用率健康检查条件。系统硬盘分区是指当前系统的根分区。

fatal_percent	可选。该参数指定系统硬盘分区使用率的阈值，单位为百分号（%）。取值必须为 1 至 100 之间的整数。 默认值为 60。
interval	可选。该参数指定健康检查的时间间隔，单位为分钟。 取值必须为 1 至 300 之间的整数。 默认值为 60。

no monitor system disk system

该命令用于删除系统硬盘分区使用率健康检查条件。

monitor system disk data [fatal_percent] [interval]

该命令用于配置数据硬盘分区使用率健康检查条件。数据硬盘分区是硬盘上存储业务数据的分区。

fatal_percent	可选。该参数指定数据硬盘分区使用率的阈值，单位为百分号（%）。取值必须为 1 至 100 之间的整数。 默认值为 80。

interval 可选。该参数指定健康检查的时间间隔，单位为分钟。
取值必须为 1 至 300 之间的整数。
默认值为 60。

no monitor system disk data

该命令用于删除数据硬盘分区使用率健康检查条件。

clear monitor system disk all

该命令用于将系统硬盘和数据硬盘分区使用率健康检查条件恢复为默认设置。

monitor powersupply [interval]

该命令用于配置电源状态、风扇转速和 CPU 温度的健康检查的时间间隔。

interval 可选。该参数指定电源状态、风扇转速和 CPU 温度的健康检查的时间间隔，单位为毫秒。取值必须为 500 至 600,000 之间的整数。
默认值为 15,000。

no monitor powersupply

该命令用于将电源状态、风扇转速和 CPU 温度的健康检查的时间间隔恢复为默认值。

show monitor powersupply

该命令用于显示电源状态、风扇转速和 CPU 温度的健康检查的时间间隔。

monitor system ntp [interval] [up_check_times] [down_check_times]

该命令用于配置 NTP 状态健康检查条件。

interval 可选。该参数指定健康检查的时间间隔，单位为毫秒。
取值必须为 5000 至 1,000,000 之间的整数。
默认值为 5000。

up_check_times 可选。该参数指定连续检查出 NTP 服务可用的次数。取值必须为 3 至 10 之间的整数。
默认值为 3。

down_check_times 可选。该参数指定连续检查出 NTP 服务不可用的次数。取值必须为 3 至 10 之间的整数。
默认值为 3。

no monitor system ntp

该命令用于删除 NTP 状态健康检查条件。

monitor vcondition name <vcondition_name> <condition_name> [logic]

该命令用于配置一个健康检查条件组（vcondition）。该 vcondition 可以嵌套多个子健康检查条件。子健康检查条件可以为真实健康检查条件也可以为其它的 vcondition，该 vcondition 仍可以嵌套其它子健康条件。

vcondition_name	该参数指定 vcondition 的名称。取值必须为最大长度不超过 128 个字节的字符串。
condition_name	该参数指定与该 vcondition 绑定的系统预定义条件的名称。取值范围为 VCONDITION_1~ VCONDITION_32。
logic	该参数指定该 vcondition 所嵌套的多个子健康检查条件之间的逻辑关系，可以为“AND”或“OR”。“AND”表示只有当所有子健康检查条件都“up”时，该 vcondition 才“up”。“OR”表示当任何一个子健康检查条件“up”时，该 vcondition 就“up”。

no monitor vcondition name <vcondition_name>

该命令用于删除指定的 vcondition 配置。



注意：当执行命令“**no monitor vcondition name**”删除指定的 vcondition 时，与该 vcondition 相关的配置也将被删除，包括子健康检查条件和 HA 失效切换规则配置。

clear monitor vcondition all

该命令用于删除所有的 vcondition 配置。

monitor vcondition member <vcondition_name> <subcondition_name>

该命令用于为指定的 vcondition 嵌套一个子健康检查条件。一个 vcondition 最多可以嵌套 16 个子健康检查条件。

vcondition_name	该参数指定 vcondition 的名称。
subcondition_name	该参数指定子健康检查条件的名称，可以为其它真实健康检查条件或者 vcondition。

no monitor vcondition member <vcondition_name> <subcondition_name>

该命令用于删除指定 vcondition 的一个子健康检查条件。

clear monitor vcondition member <vcondition_name>

该命令用于删除指定 vcondition 的所有子健康检查条件。

monitor import scp <username@remote_scp_ip>

该命令用于从远程 SCP 服务器导入自定义的健康检查脚本。如需使用自定义的健康检查脚本，请联系公司技术支持。

username@remote_scp_ip 该参数指定远程 SCP 服务器的用户名和 IP 地址，用户名和 IP 地址之间通过 “@” 符号分隔，IP 地址后必须指定存放健康检查脚本的路径和文件名称，路径和 IP 地址之间通过冒号分隔，整个取值置于双引号内，例如 “user@10.8.3.12:/usr/tool/scr.tar.gz”。IPv4 和 IPv6 地址的 SCP 服务器都支持。

monitor export scp <username@remote_scp_ip>

该命令用于将自定义的健康检查脚本导出到一个远程 SCP 服务器中。

username@remote_scp_ip 该参数指定远程 SCP 服务器的用户名和 IP 地址，用户名和 IP 地址之间通过 “@” 符号分隔，IP 地址后必须指定存放健康检查脚本的路径，路径和 IP 地址之间通过冒号分隔，整个取值置于双引号内，例如 “user@10.8.3.12:/usr/save”。IPv4 和 IPv6 地址的 SCP 服务器都支持。

monitor import tftp <remote_tftp_ip> <file_name>

该命令用于从远程 TFTP（Trivial File Transfer Protocol，简单文件传输协议）服务器导入自定义的健康检查脚本。如需使用自定义的健康检查脚本，请联系公司技术支持。

remote_tftp_ip 该参数指定远程 TFTP 服务器的 IP 地址。IPv4 和 IPv6 地址的 TFTP 服务器都支持。

file_name 该参数指定远程 TFTP 服务器上保存健康检查脚本的文件名称。

monitor export tftp <remote_tftp_ip>

该命令用于将自定义的健康检查脚本导出到一个远程 TFTP 服务器中。

remote_tftp_ip 该参数指定远程 TFTP 服务器的 IP 地址。IPv4 和 IPv6 地址的 TFTP 服务器都支持。

show monitor config

该命令用于显示系统健康检查功能的开启状态以及所有的系统健康检查条件配置。

clear monitor all

该命令用于删除系统中的所有健康检查条件配置，同时将以下配置恢复为默认设置：

- 系统健康检查功能
- CPU 温度健康检查条件
- CPU 使用率健康检查条件
- SSL 加速卡健康检查条件
- 内存使用率健康检查条件（包括系统内存、网络内存、连接内存、SWAP 内存）
- 硬盘分区使用率健康检查条件（包括系统分区和数据分区）
- NTP 健康检查条件

show statistics monitor

该命令用于显示所有系统健康检查相关的统计信息。

clear statistics monitor

该命令用于清除所有系统健康检查相关的统计信息。

show statistics cpu

该命令用于显示系统的当前 CPU 使用率。

show statistics system

该命令用于显示系统的当前 CPU 使用率、平均每秒新建连接数和平均每秒接收到的请求数。

clear system resource

该命令用于释放被占用的系统内存。



注意：该命令仅在网络流量较少或没有网络流量时可以使用，否则可能造成无法预知的错误。

ip license server <ip_address> <port> <admin_name> <admin_password>
<email>

该命令用于配置与授权服务器相关的信息。该功能目前只适用于 vAPV。vAPV 须与授权服务器保持通信，告知授权服务器注册信息并上报带宽。如果七天以上不与授权服务器通信，许可密钥将会失效。

ip_address 该参数指定授权服务器的 IP 地址。

port 该参数指定授权服务器的端口号，端口取值必须为 1025

到 65,000 之间的整数。

admin_name	该参数指定登录授权服务器的用户名，取值必须为长度不超过 16 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。
admin_password	该参数指定登录授权服务器的密码，取值必须为长度不超过 80 个字符的字符串，支持字母、数字、特殊字符，必须置于双引号内。
email	该参数指定接收报警邮件的邮箱地址，地址必须置于双引号内。

no ip license server

该命令用于删除与授权服务器相关的配置。

show ip license server

该命令用于显示与授权服务器相关的配置。

第3章 高级系统配置

本章介绍高级系统配置的相关命令。

mnet {system_ifname|bond_ifname|vlan_ifname} <user_interface_name>

该命令用于在指定的系统接口、聚合接口或 VLAN 接口上创建 MNET（多网段）接口。系统最多支持配置 4126 个 MNET 接口。

system_ifname	该参数指定系统接口名称，默认为 port1、port2、port3、port4……。 （管理员可以通过“ interface name ”命令来自定义系统接口名称。）
bond_ifname	该参数指定聚合接口的名称，默认的聚合接口名称为 bond1、bond2、bond3、bond4……。 （管理员可以通过“ bond name ”命令来自定义聚合接口名称。）
vlan_ifname	该参数指定 VLAN 接口名称。（管理员可以通过“ vlan ”命令来创建 VLAN 接口。）
user_interface_name	该参数指定 MNET 接口的名称。取值必须为长度不大于 31 个字符的字符串，支持字母、数字和特殊字符，字母不区分大小写。 支持的特殊字符：“@”、“!”、“~”、“_”、“:”、“-”、“.”。

no mnet <mnet_ifname>

该命令用于从系统中删除一个特定的 MNET 接口。

mnet_ifname 指定待删除的 MNET 接口名称。

[show|clear] mnet

该命令用于显示或者清除所有 MNET 接口的配置。

vlan {system_ifname|bond_ifname} <vlan_ifname> <vlan_tag>

该命令用于在指定的系统接口或聚合接口上创建虚拟局域网（VLAN，Virtual Local Area Network）接口。系统支持最多配置 4094 个 VLAN 接口。

system_ifname	该参数指定系统接口的名称，默认为 port1、port2、port3、port4……。 （管理员可以通过“ interface name ”命令来自定义系统接口名称。）
bond_ifname	该参数指定聚合接口的名称，默认的聚合接口名称为 bond1、bond2、bond3、bond4……。 （管理员可以通过

“**bond name**”命令来自定义聚合接口名称。)

vlan_ifname 该参数指定 VLAN 接口名称。取值必须为长度不大于 31 个字符的字符串，支持字母、数字和特殊字符，字母不区分大小写。

支持的特殊字符：“@”、“!”、“~”、“_”、“:”、“-”、“.”。

vlan_tag 该参数指定 VLAN 接口的标识 ID，可以配置为 1 至 4094 之间的任意整数。



注意：请不要在配置了聚合接口的接口上配置 VLAN 接口。

no vlan <vlan_ifname>

该命令用来从系统中删除一个特定的 VLAN 接口。

vlan_ifname 指定待删除的 VLAN 接口名称。

[show|clear] vlan

该命令用于显示或者清除系统中所有 VLAN 接口的配置。

fwd tcp <local_ip> <local_port> <remote_ip> <remote_port> [timeout]

使用者使用这条命令把访问设备的一组 IP 地址/端口映像到后台的一组 IP 地址/端口。任意访问设备的 IP 地址/端口的 TCP 数据流都会路由到后台指定的 IP 地址/端口。

local_ip 指定本地的 IP 地址。可以为 IPv4 地址或 IPv6 地址。

local_port 指定本地的端口。

remote_ip 指定远程的 IP 地址。可以为 IPv4 地址或 IPv6 地址。

remote_port 指定远程的端口。

timeout 指定超时时间（可选），单位为秒，默认值为 300。

设备上支持的“**fwd tcp|udp**”条目的最大数量取决于系统内存的大小，如下表所示。

表3 - 1 “fwd tcp|udp”条目最大数量

系统内存	“fwd tcp udp”条目最大数量
<=4 GB	200
8 GB	600
>=16 GB	1200

fwd udp <local_ip> <local_port> <remote_ip> <remote_port> [timeout]

使用者使用这条命令把设备的一组 IP 地址/端口映像到后台的一组 IP 地址/端口。任意访问设备的 IP 地址/端口的 UDP 数据流都会路由到后台指定的 IP 地址/端口。

local_ip	指定本地的 IP 地址。可以为 IPv4 地址或 IPv6 地址。
local_port	指定本地的端口。
remote_ip	指定远程的 IP 地址。可以为 IPv4 地址或 IPv6 地址。
remote_port	指定远程的端口。
timeout	指定超时时间（可选），单位为秒，默认值为 60。

设备上支持的“fwd tcp|udp”条目的最大数量取决于系统内存的大小，如下表所示。

表3 - 2 “fwd tcp|udp” 条目最大数量

系统内存	“fwd tcp udp” 条目最大数量
<=4 GB	200
8 GB	600
>=16 GB	1200

no fwd tcp <local_ip> <local_port>

删除一条已经设置“fwd tcp”配置。

no fwd udp <local_ip> <local_port>

删除一条已经设置“fwd udp”配置。

show fwd

显示“fwd”的工作模式。

clear fwd

清除所有“fwd”相关配置。

nat port {pool_name|vip} {source_ip|source_ip_group} {netmask|prefix} [timeout] [gateway] [description]

该命令用于启用网络地址转换（NAT）和端口转换功能。NAT 把内部网络设备或者服务器的 IP 地址转换为可以访问外部网络的 IP 地址。它也可以充当防火墙，使得外部看不见内部 IP 地址。多个网段或 IP 地址或 IP 地址组可以转换成同一个 VIP，也可以转换成预设的 IP 地址池中的地址。设备会在配置过程中自动检查 NAT 配置中的子网重迭和 IP 冲突。“nat port”支持由内网向外网主动发起的流量。只有满足以下两个条件，数据报才会被 NAT：

- 源 IP 地址在配置的 “source_ip|source_ip_group” 和 “netmask|prefix” 范围之内。
- 配置的 “gateway” 与路由网关相同。但是如果 “gateway” 配置为默认值 0.0.0.0，则配置的 “vip” 或 IP 地址池所对应的网段则必须与路由网关所在的网段相同。

设备最多支持 512 条 “nat port” 配置。

pool_name vip	能访问外部网络的 IP 地址，可以设置为一个虚拟 IP 地址，也可以使用预先配置的 IP 地址池名称。可以为 IPv4 或 IPv6 地址或地址池。 注意：若用于网络地址转换的 VIP 地址不与任一系统接口 IP 地址在同一个网段上，则该 IP 地址将默认绑定到接口 port1 上。因此，需要事先为接口 port1 配置一个 IP 地址。
source_ip source_ip_group	需要转换的 IP 地址或源 IP 地址组。IP 地址可以为 IPv4 或 IPv6 地址。
netmask prefix	需要转换的 IP 地址对应的子网掩码或前缀长度。 • “netmask” 用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。 • “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。 当参数 “source_ip source_ip_group” 取值为源 IP 地址组时，该参数无效。
timeout	网络地址转换条目超时时间（可选），默认值为 60 秒。
gateway	指定网关 IP 地址。默认值为 0.0.0.0。当 “vip” 或 “pool_name” 所对应的网段与设备的任一接口 IP 地址在同一网段时，设备会自动选择路由，不需要配置 “gateway”；当 “vip” 或 “pool_name” 所对应的网段与设备的任一接口 IP 地址不在同一网段时，需要配置 “gateway”。
description	为这条 “nat port” 配置增加描述信息，作为提示或注意信息。描述信息需要置于双引号内，且长度不大于 31 个字符。



注意：

- 对于 IPv6 地址，仅仅 ICMP、TCP（FTP 应用除外）和 UDP 类型的数据报可以进行转换。

- L2 SLB 配置与 “nat port” 配置不能一起工作。如果 “nat port” 配置绑定到配置了 L2 SLB 的系统接口，那么 “nat port” 配置将失效。

no nat port {pool_name|vip} {source_ip|source_ip_group} {netmask|prefix}

该命令用于删除一条 “nat port” 配置。

clear nat port

该命令用于清除所有的 “nat port” 配置。

nat portdst {pool_name|vip} {destination_ip|destination_ip_group}
{netmask|prefix} [timeout] [gateway] [description]

该命令用于启用基于目的 IP 或 IP 地址组的网络地址转换功能，对目的 IP 在指定的网段或与路由网关处于同一网段的报文的源 IP 将进行转换。若网关设为默认值 “0.0.0.0”，则需要进行转换的报文的目的 IP 或 IP 池应与路由网关处于同一网段中。

pool_name|vip 能访问外部网络的 IP 地址，可以设置为一个虚拟 IP 地址，也可以使用预先配置的 IP 地址池名称。可以为 IPv4 或 IPv6 地址（池）。

destination_ip|destination_ip_group 目的 IP 地址或目的 IP 地址组。可以为 IPv4 或 IPv6 地址。

netmask|prefix 需要转换的 IP 地址对应的子网掩码或前缀长度。

- “netmask” 用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。

当参数 “destination_ip|destination_ip_group” 取值为目的 IP 地址组时，该参数无效。

timeout 网络地址转换条目超时时间（可选），默认值为 60 秒。

gateway 指定网关 IP 地址，默认值为 0.0.0.0。当 “vip” 或 “pool_name” 所对应的网段与设备的任一接口 IP 地址在同一网段时，设备会自动选择路由，不需要配置 “gateway”；当 “vip” 或 “pool_name” 所对应的网段与设备的任一接口 IP 地址不在同一网段时，需要配置 “gateway”。

description 为这条 “nat portdst” 配置增加描述信息，作为提示或注意信息。描述信息需要置于双引号内，且长度不大于 31 个字符。



注意：对于 IPv6 地址，仅仅 ICMP、TCP（FTP 应用除外）和 UDP 类型的数据报可以进行转换。

no nat portdst {pool_name|vip} {destination_ip|destination_ip_group}
{netmask|prefix}

该命令用于删除一条“**nat portdst**”配置。

clear nat portdst

该命令用于清除所有的“**nat portdst**”配置。

show nat port

该命令用于显示所有的“**nat port**”和“**nat portdst**”配置。

nat static <vip> <network_ip> [timeout] [gateway] [description]

创建一条“**nat static**”配置。和“**nat port**”的区别是本条命令仅做地址转换，端口将保持不变。“**nat static**”支持由内网向外网主动发起的流量以及由外网向内网主动发起的流量。只有满足以下两个条件：

- 源 IP 地址在配置的“**network_ip**”范围之内中。
- 配置的“**gateway**”与路由网关相同（路由网关是通过“**ip route default**”命令配置的）。但是如果“**gateway**”配置为默认值 0.0.0.0，则配置的“**vip**”则必须与路由网关在同一个网段中。

设备才会对 IPv4 数据包执行地址转换。而只需要满足第一个条件，设备就会对 IPv6 数据包执行地址转换。

vip 能访问外部网络的 IP 地址。可以为 IPv4 地址或 IPv6 地址。

注意：若用于网络地址转换的 VIP 地址不与任一系统接口 IP 地址在同一个网段上，则该 IP 地址将默认绑定到接口 port1 上。因此，需要事先为接口 port1 配置一个 IP 地址。

network_ip 需要转换的 IP 地址。可以为 IPv4 地址或 IPv6 地址。

timeout 超时时间（可选），默认值为 60 秒。

gateway 指定网关 IP 地址，可以为 IPv4 地址或 IPv6 地址。对于 IPv4 地址，默认值为 0.0.0.0。对于 IPv6 地址，默认值为：：。当“**vip**”或“**pool_name**”所对应的网段与设备的任一接口 IP 地址在同一网段时，设备会自动选择路由，不需要配置“**gateway**”；当“**vip**”或“**pool_name**”所对应的网段与设备的任一接口 IP 地址不在同一网段

时，需要配置 “gateway”。

description 该 “**nat static**” 配置的用法解释、注释或标注，置于双引号内且长度不大于 31 个字符。



注意：L2 SLB 配置与 “**nat static**” 配置不能一起工作。如果 “**nat static**” 配置绑定到配置了 L2 SLB 的系统接口，那么 “**nat static**” 配置将失效。

no nat static <vip>

删除一条 “**nat static**” 配置。

show nat static

显示所有的 “**nat static**” 配置。

clear nat static

清除所有的 “**nat static**” 配置。

nat itcpopt on <tcp_option_kind>

该命令用于在静态 NAT、NAPT（基于网络地址端口的 NAT 转换）和 NAT64/NAT46 环境下启用通过指定的 TCP 选项将客户端 IP 地址转发给服务器的功能，服务器可以从 TCP 选项里获取真实的客户端 IP 地址用于记录或审计。指定的 TCP 选项将被插入到系统发送的第一个 SYN 包和 ACK 包里。该功能的默认设置为禁用。

tcp_option_kind 该参数指定 TCP 选项的类型，取值必须为 31 至 252 之间的整数。

nat itcpopt off

该命令用于在静态 NAT 和 NAPT 环境下禁用通过指定的 TCP 选项将客户端 IP 地址转发给服务器的功能。

show nat itcpopt

该命令用于显示在静态 NAT 和 NAPT 环境下通过指定的 TCP 选项将客户端 IP 地址转发给服务器的功能的启用状态。

clear nat itcpopt

该命令用于在静态 NAT 和 NAPT 环境下将通过指定的 TCP 选项将客户端 IP 地址转发给服务器的功能重置为默认设置。

nat protocol pptp [port] [direction]

该命令用于在入向或出向启用 PPTP 隧道的 NAT 穿越功能。默认情况下，系统禁用该功能。

port	可选，该参数指定 PPTP 服务器的端口号。默认值是 1723。
direction	可选，该参数指定在入向或出向启用 PPTP 隧道的 NAT 穿越功能。该参数的有效取值为 “inbound” 和 “outbound”，默认值为 “outbound”。

no nat protocol pptp [direction]

该命令用于在入向或出向禁用 PPTP 隧道的 NAT 穿越功能。

direction	可选，该参数指定在入向或出向禁用 PPTP 隧道的 NAT 穿越功能。该参数的有效取值为 “inbound” 和 “outbound”，默认值为 “outbound”。

clear statistics pptp

这条命令用于清除设备上的所有 PPTP 相关统计信息。

show nat protocol pptp

该命令用于显示 PPTP 隧道的 NAT 穿越功能的所有配置信息。

nat protocol ftp port <port_number>

该命令用于为 FTP 服务的 NAT 功能配置一个备选 FTP 端口。系统允许为 FTP 服务的 NAT 功能配置最多 10 个备选 FTP 端口。如果没有为 FTP 服务的 NAT 功能配置任何备选 FTP 端口，在 FTP 主动模式下，NAT 只能处理 FTP 端口号为“21”的数据包。

port_number	该参数指定 FTP 端口号。取值必须为 1 到 65,390 之间的整数。由于系统已支持默认 FTP 端口号 “21”，所以该参数不能被设置为 “21”。

no nat protocol ftp port <port_number>

该命令用于删除为 FTP 服务的 NAT 功能配置的备选 FTP 端口。

show nat protocol ftp port

该命令用于显示为 FTP 服务的 NAT 功能配置的备选 FTP 端口。

clear nat protocol ftp port

该命令用于清除为 FTP 服务的 NAT 功能配置的所有的备选 FTP 端口。

nat protocol dns [method]

该命令用于启用 DNS NAT 功能。该功能应用于内网服务器返回的 DNS 响应中的解析 IP 地址为不能从外部访问的内网 IP 地址的场景。启用 DNS NAT 功能后，

当收到来自内网 DNS 服务器的 DNS 响应时，设备将根据 NAT Static 条目（通过命令“**nat static**”配置），将 DNS 响应中的内网解析 IP 地址转换为公网 IP 地址，然后将改写后的 DNS 响应返回给客户端。当外网用户使用公网 IP 地址访问时，系统根据 NAT Static 条目再将公网 IP 地址转换为内网服务器的 IP 地址，这样外网用户就可以访问内网服务器。默认情况下，该功能是禁用的。

method 可选，该参数指定在多链路环境中转换 DNS 响应中解析 IP 地址的方式。取值必须为：

- **rr**：表示将 DNS 响应中的解析 IP 地址按照 Round Robin 方式转换为不同的链路对应的 NAT Static 条目中的公网 IP 地址。
- **proximity**：表示将 DNS 响应中的解析 IP 地址转换为最近的链路（即 DNS 响应发出的链路）对应的 NAT Static 条目中的公网 IP 地址。

默认值为 proximity。



注意：在多链路环境中开启 DNS NAT 功能后：

- 对于 rr 算法，如果设备选择的 NAT Static 条目对应的链路是可用的，则按照该 NAT Static 条目进行转换；否则按照 Round Robin 方式选择下一个 NAT Static 条目。如果所有 NAT Static 条目对应的链路都不可用，则不进行 NAT Static 转换。
- 对于 proximity 算法，如果设备选择了最近的链路，则按照该链路对应的 NAT Static 条目进行转换。如果该链路对应多个 NAT Static 条目，则优先选择先配置的 NAT Static 条目。如果最近的链路没有对应任何 NAT Static 条目，则根据 rr 算法重新进行选择。

no nat protocol dns

该命令用于禁用 DNS NAT 功能。

show nat protocol dns

该命令用于显示 DNS NAT 功能的配置。

clear nat protocol dns

该命令用于清除 DNS NAT 功能的配置。

show nat dns status <network_ip>

该命令用于为指定的网络 IP 地址显示 DNS NAT 的统计信息。

network_ip 该参数指定一个网络 IP 地址。该参数取值必须为已存在的 NAT Static 条目（使用命令“**nat static**”配置）中的“network_ip”值。

clear nat dns status

该命令用于清除 DNS NAT 的所有统计信息。

show nat table [ip_address]

该命令用于显示入向/出向流量的网络地址解析记录，以及 GRE 隧道的相关统计信息。该命令仅支持 TCP 协议，而不支持 ICMP 和 UDP 协议。

ip_address 指定用来过滤输出结果的 IP 地址。该 IP 地址的类型可以为源 IP 地址、目的 IP 地址或网络地址转换条目的虚拟 IP 地址。

show statistics nat

该命令用于显示所有 NAT 相关的统计信息。

```
Demo(config)#show statistics nat
nat static 10.8.1.194 10.3.188.189 60 0.0.0.0
    Outbound protocol(total connection/current connection): icmp(4/10) udp(5/1) tcp(9/2)
        IP packet(total packet in/total packet out):    933/933
        IP packet(total byte in/total byte out):        100764/100764

    Inbound  protocol(total connection/current connection): icmp(2/0) udp(6000/3338)
tcp(25/2)
        IP packet(total packet in/total packet out):    933/933
        IP packet(total byte in/total byte out):        100764/100764
nat static 2012:1081::10:8:1:194 2012:1030::10:3:188:189 60 ::
    Outbound protocol(total connection/current connection):icmp(0/0) udp(63/4) tcp(4/1)
    Inbound  protocol(total connection/current connection):icmp(0/0) udp(6000/3338)
tcp(3000/1499)
```



注意：对于 IPv6 地址，ICMP 报文不能被转换，因此 IPv6 的 ICMP 统计值为 0。

nat pureip {on|off}

该命令用于为非 TCP、UDP 或 ICMP 的 IP 数据包启用或禁用 NAT 穿越功能。该功能适用于只修改 IP 头部的信息就可以进行网络地址转换的协议。例如，隧道模式的 ESP（Encapsulating Security Payload，封装安全负载）协议。该功能只适用于 IPv4 的 IP 数据包，并且只适用于静态地址转换。默认情况下，该功能是禁用的。



注意：

- 对于某些协议的 IP 数据包，只修改 IP 头部的信息不能进行网络地址转换。因此，建议仅在需要时启用该功能。

- 对隧道模式的 ESP 协议的 IP 数据包使用 NAT 穿越功能时，由于可能存在 SPI（Security Parameters Index，安全参数索引）的冲突，所以该功能不支持将多个私有 IP 地址转换为一个 VIP 地址的情况。
- 当该功能被启用后，无论系统的转发模式是透明还是非透明，设备都会将客户端 IP 作为端口转发连接的源 IP 地址。

show nat pureip

该命令用于显示非 TCP、UDP 或 ICMP 的 IP 数据包的 NAT 穿越功能的运行状态信息。

rip {on|off}

该命令用于启用或禁用路由信息协议（Routing Information Protocol，RIP）。当启用该功能后，系统将会学习其他设备的动态路由信息。可以通过命令“**show ip route**”查看学习到的动态路由信息。该功能默认是禁用的。

要使该功能生效，需要通过命令“**rip network**”为路由信息协议添加直连路由。

rip version <rip_version>

该命令用于设置 RIP 的版本。

rip_version 该参数指定 RIP 的版本，取值必须为 1 或 2。

rip network <ip_address> <netmask>

该命令用于为 RIP 添加一条直连路由。系统将通过指定的直连路由去学习其他设备上的路由。

ip_address 该参数指定要添加到 RIP 的直连路由的 IP 地址。取值必须为 IPv4 地址。

netmask 该参数指定 IP 地址对应的子网掩码，取值必须为点分十进制格式。

no rip network <ip_address> <netmask>

该命令用于为 RIP 删除指定的直连路由。

show rip status

该命令用于显示 RIP 的运行状态信息。

show rip settings

该命令用于显示 RIP 当前的所有设置。

ripng {on|off}

该命令用于为 IPv6 网络启用或禁用下一代路由信息协议（RIP next generation, RIPng）。当启用该功能时，系统将会学习其他设备 IPv6 网络的动态路由，可以通过命令“**show ip route**”命令查看学习到的路由信息。该功能默认是禁用的。

要使该功能生效，需要通过命令“**ripng interface**”为指定接口启用 RIPng。

ripng interface <interface_name>

该命令用于为指定接口启用 RIPng。

interface_name 该参数指定要启用 RIPng 的接口。

no rip interface <interface_name>

该命令用于为指定接口禁用 RIPng。

show ripng status

该命令用于显示 RIPng 的运行状态信息。

show ripng settings

该命令用于显示 RIPng 当前的所有设置。

ospf {on|off}

该命令用于启用或禁用 OSPF 功能。当启用 OSPF 功能时，系统将会学习 OSPF 路由。学习到的 OSPF 路由不会立即生效，它们大约在 30s 内生效。OSPF 功能默认是禁用的。

ospf network <ip_address> <netmask> <area_id>

该命令用于为指定的网络启用 OSPF，同时设置网络的地区号。

ip_address 该参数指定网络 IP 地址，取值必须为 IPv4 地址。

netmask 该参数指定网络对应的子网掩码，取值必须为点分十进制格式。

area_id 该参数指定分配给 OSPF 网络的地区号，取值必须为 0 至 4,294,967,296 之间的整数。

no ospf network <ip_address> <netmask> <area_id>

该命令用于对指定的网络禁用 OSPF，同时删除 OSPF 网络的地区号设置。

ospf interface cost <interface_name> <cost>

该命令用于设置 OSPF 接口和接口开销。如不配置该命令，则按照接口速率计算开销。

interface_name	该参数指定接口名称，取值必须为系统接口、VLAN 接口或聚合接口的名称。
cost	该参数指定接口运行 OSPF 协议所需的开销，取值必须为 1 至 65,535 之间的整数。

no ospf interface cost <interface_name>

该命令用于删除指定的 OSPF 接口开销设置。

ospf router <router_id>

该命令用于设置 OSPF 路由器的 ID。如不配置该命令，则默认使用系统接口最大的 IP 地址作为路由器 ID。

router_id 该参数指定 OSPF 路由器的 ID，取值必须为 IPv4 地址。

no ospf router

该命令用于删除 OSPF 路由器 ID 设置。

show ospf status

该命令用于显示 OSPF 的运行状态信息。

show ospf settings

该命令用于显示 OSPF 当前的所有设置信息。

ipv6 ospf {on|off}

该命令用于启用或禁用 OSPFv3（IPv6 OSPF）功能。默认该功能是禁用的。

ipv6 ospf routerid <id>

该命令用于设置 OSPF 路由 ID，该路由 ID 为点分格式的 IPv4 地址。

ipv6 ospf drpriority <interface_name> <priority>

该命令用于为接口设置进行 OSPF 指定路由器（DR，designated router）选举时的优先级。

interface_name 指定接口名称。可以为系统接口、聚合接口、VLAN 接口或者 MNET 接口。

priority 指定接口优先级。其值范围在 0 到 255 之间，默认为 1。



注意：该命令不支持配置同步（通过命令“sysconfig from”和“synconfig to”）。

ipv6 ospf interface <interface_name> <area_id>

该命令用于在指定的接口上启用 OSPFv3，同时为该接口设置一个区域 ID。

Interface_name 指定接口名称。可以为系统接口、聚合接口、VLAN 接口或者 MNET 接口。

area_id 指定接口的区域 ID。其值范围在 0 到 4294967295 之间，默认为 0。

no ipv6 ospf interface <interface_name> <area_id>

该命令用于删除具有某个区域 ID 所指定的接口上的 OSPFv3 配置。

show ipv6 ospf settings

该命令用于显示 OSPFv3 当前的所有配置信息。

例如：

```
Demo#show ipv6 ospf settings
ipv6 ospf on
ipv6 ospf drpriority port2 2
ipv6 ospf drpriority port1 1
ipv6 ospf drpriority port4 1
ipv6 ospf routerid 1.1.1.1
ipv6 ospf interface port4 0
ipv6 ospf interface port1 2
```

show ipv6 ospf status

该命令用于显示 OSPFv3 的运行状态信息（on/off）。

ospf rhi {on|off}

该命令用于启用或禁用路由健康注入（Route Health Injection，RHI）功能。默认情况下，该功能是禁用的。

当 RHI 功能启用后：

- 若一个虚拟 IP 地址对应的任一后台服务的健康检查结果为 UP，则该虚拟 IP 地址将被置为激活（ACT）状态。系统将该虚拟 IP 地址的路由信息注入到路由表中。如果处于激活状态的虚拟 IP 所在的网段已经（通过“**ospf network**”命令）启用了 OSPF 功能，此虚拟 IP 地址的路由信息通过 OSPF 协议发布给网络中的其他设备。
- 若一个虚拟 IP 地址对应的所有后台服务的健康检查结果都为 DOWN，则该虚拟 IP 地址将被置为禁用（INACT）状态。系统将从路由表中移除该虚拟 IP 地址的路由信息。因此，该虚拟 IP 地址的路由信息将不会被发布给网络中的其他设备。

注：如果一个虚拟 IP 地址是某个虚拟集群的唯一虚拟 IP 地址，则在该虚拟 IP 地址被置为激活或禁用状态时，对应的虚拟集群也将被置为主或初始状态。如果一个虚拟 IP 地址不是某个虚拟集群的唯一虚拟 IP 地址，则该虚拟 IP 地址的激活和禁用状态不影响虚拟集群功能。

show ospf rhi status

该命令用于显示当前全部虚拟 IP 地址的激活和禁用状态。

show statistics rhi

该命令用于显示关于虚拟 IP 地址的激活和禁用的统计信息。

clear statistics rhi

该命令用于删除关于虚拟 IP 地址的激活和禁用的统计信息。

bgp {on|off}

该命令用于启用或禁用 BGP 功能。默认情况下，该功能是禁用的。启用 BGP 功能后，设备将变为一台 BGP 路由器。

bgp asn <as_number>

该命令用于指定本地 BGP 路由器的自治系统标识号（ASN）。

as_number	指定本地 BGP 路由器的自治系统标识号。其取值范围为 1 到 4,294,967,295 之间的整数。

no bgp asn <as_number>

该命令用于删除为本地 BGP 路由器指定的自治系统标识号。删除自治系统标识号后，相关配置如 BGP 邻居及 BGP 路由器的管理距离值等配置也将同时被删除。

bgp router <router_id>

该命令用于指定本地 BGP 路由器的 ID。如不配置该命令，则本地 BGP 路由器将默认使用其最大的 IPv4 接口地址作为路由器 ID。

router_id	指定本地 BGP 路由器的 ID，其取值为点分十进制格式的 IPv4 地址。

no bgp router <router_id>

该命令用于删除指定的路由器 ID。

bgp network <ip_address> {netmask|prefix}

该命令用于添加要通告的网络。只有为本地 BGP 路由器指定了自治系统标识号后，才可执行此命令。

ip_address	指定通告网络的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。
netmask prefix	指定通告网络对应的子网掩码或前缀长度。 “mask”用于配置 IPv4 地址对应的子网掩码，其取值可以是点分十进制地址格式或是一个 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其取值应是一个 0 到 128 之间的整数。

no bgp network <ip_address> {netmask|prefix}

该命令用于删除要通告的网络。

bgp neighbor <ip_address> <as_number>

该命令用于指定一个 BGP 邻居，并指定该邻居的自治系统标识号。只有为本地 BGP 路由器指定了自治系统标识号后，才可执行此命令。

ip_address	指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。注意：当使用 IPv6 Link-Local 地址建立 BGP 连接时，需要执行 “ bgp interface <ip_address> <interface_name> ” 命令指定本地 BGP 路由器使用的接口。
as_number	指定 BGP 邻居的自治系统标识号，其取值范围为 1 到 4,294,967,295 之间的整数。

no bgp neighbor <ip_address>

该命令用于删除指定的 BGP 邻居。

show ip bgp neighbors [ip_address]

该命令用于显示指定的 BGP 邻居的详细信息。如不指定参数 “ip_address”，则显示所有 BGP 邻居的详细信息。

bgp interface <ip_address> <interface_name>

该命令用于指定当使用 IPv6 Link-Local 地址建立 BGP 连接时本地 BGP 路由器使用的接口。只有为本地 BGP 路由器指定了 BGP 邻居后，才可执行此命令。

ip_address	指定本地 BGP 路由器接口的 IPv6 地址。
interface_name	指定本地 BGP 路由器接口的名称，可以为系统接口或聚合接口。

no bgp interface <ip_address>

该命令用于删除当使用 IPv6 Link-Local 地址建立 BGP 连接时本地 BGP 路由器使用的接口。

bgp distance <ext_distance> <int_distance> <loc_distance>

该命令用于指定本地 BGP 路由器的管理距离值。本地 BGP 路由器使用管理距离来选择最优路由。管理距离值越低，路由的优先级越高。只有为本地 BGP 路由器指定了自治系统标识号后，才可执行此命令。

ext_distance 指定外部路由的管理距离。外部路由是指通过 EBGp (External BGP) 学到的路由。其取值范围为 1 到 255 之间的整数。

int_distance 指定内部路由的管理距离。内部路由是指通过 IBGP (Internal BGP) 学到的路由。其取值范围为 1 到 255 之间的整数。

loc_distance 指定本地路由的管理距离。作用于已经配置的本地路由。其取值范围为 1 到 255 之间的整数。

show ip bgp route [ip_address/mask|prefix]

该命令用于显示指定的 BGP 路由的详细信息。

ip_address/netmask|prefix 指定具体的 IPv4 地址及子网掩码，或 IPv6 地址及前缀长度。如不指定该参数，将显示全部 BGP 路由的详细信息。

- “netmask” 用于配置 IPv4 地址对应的子网掩码，其取值可以是点分十进制格式的 IP 地址或是一个 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，其取值应是一个 0 到 128 之间的整数。

bgp capability <ip_address> <option>

该命令用于设置向指定的 BGP 邻居通告指定的 BGP 能力。

ip_address 指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

option 指定向 BGP 邻居通告的 BGP 能力。该参数的取值如下（区分大小写）：

- **dynamic**: 向指定的 BGP 邻居通告本地 BGP 路由器的动态更新能力。动态更新能力允许 BGP 邻居之间在不重置 BGP 连接的基础上动态地更新 BGP 能力。

- **both:** 与指定的 BGP 邻居交互出向路由过滤（Outbound Route Filter, ORF）前缀列表。
- **receive:** 从指定的 BGP 邻居接收 ORF 前缀列表。
- **send:** 向指定的 BGP 邻居通告 ORF 前缀列表。

no bgp capability <ip_address> <option>

该命令用于取消向指定的 BGP 邻居通告指定的 BGP 能力。

bgp passive <ip_address>

该命令用于指定不向其主动发送 Open 报文的 BGP 邻居。

ip_address 指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

bgp nexthopself <ip_address>

该命令用于将通告路由的下一跳地址设置为本地 BGP 路由器的 IP 地址。只有为本地 BGP 路由器指定了自治系统标识号后，才可执行此命令。

ip_address 该参数用于指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

bgp def_orig <ip_address>

该命令用于向指定的 BGP 邻居通告到达本地 BGP 路由器的默认路由。

ip_address 指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

bgp local_as <ip_address> <as_number>

该命令用于设置本地 BGP 路由器与指定的 EBGP 邻居通信时使用的替代自治系统标识号。

ip_address 指定 EBGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

as_number 指定本地 BGP 路由器的替代自治系统标识号，其取值范围为 1 到 4,294,967,295 之间的整数。



注意：替代自治系统标识号不能与 BGP 邻居的自治系统标识号相同。

no bgp local_as <ip_address> <as_number>

该命令用于删除本地 BGP 路由器与指定的 EBGP 邻居通信时使用的替换自治系统标识号。

bgp shutdown <ip_address>

该命令用于终止与指定的 BGP 邻居之间的通信。

ip_address 指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

no bgp shutdown <ip_address>

该命令用于恢复与指定的 BGP 邻居之间的通信。

bgp redistribute <option>

该命令用于设置将指定类型的路由动态地重分发到 BGP 协议中。

option 指定动态重分发到 BGP 协议中的路由类型。该参数的取值如下（区分大小写）：

- connected: 直连路由
- ospf: OSPF 路由
- rip: RIP 路由
- static: 静态路由

no bgp redistribute <option>

该命令用于设置取消将指定类型的路由重分发到 BGP 协议中。

show bgp settings

该命令用于显示所有的 BGP 配置。

clear bgp ip [ip_address]

该命令用于重置本地 BGP 路由器与指定的 BGP 邻居之间的连接。如不指定参数“ip_address”，则重置本地 BGP 路由器与所有 BGP 邻居之间的连接。在修改 BGP 配置如管理距离值后，必须重置本地 BGP 路由器与指定的 BGP 邻居之间的连接以使修改生效。

ip_address 指定 BGP 邻居的 IP 地址，其取值可以为 IPv4 或 IPv6 地址。

clear bgp asn <as_number>

该命令用于重置本地 BGP 路由器与位于指定的自治系统中所有 BGP 邻居之间的连接。在修改 BGP 配置如管理距离值后，必须重置本地 BGP 路由器与指定的 BGP 邻居之间的连接以使修改生效。

as_number 指定 BGP 邻居的自治系统标识号。

3.1 LLDP

lldp {on|off} <system_ifname>

该命令用于为指定的系统接口启用或禁用 LLDP（Link Layer Discovery Protocol，链路层发现）协议。启用该功能后，系统接口将能够发送和接收 LLDP 报文。默认情况下，LLDP 协议在所有系统接口上为禁用状态。

system_ifname 该参数指定系统接口的名称，可以通过“**interface name**”命令来自定义系统接口名称。

默认名称为 port1、port2、port3、port4……。

lldp sysname <system_name>

该命令用于设置设备作为 LLDP 邻居时的系统名称。

当不配置该命令时，默认使用通过“hostname”命令设置的设备主机名称作为系统名称。

system_name 该参数指定系统名称，取值必须为长度不超过 64 个字节的字符串，支持字母、数字和特殊字符。当参数取值包含特殊字符时，必须置于双引号内。

lldp transmit_delay <interval>

该命令用于定义 LLDP 报文的发送间隔。

当不配置该命令时，默认的发送间隔是 30 秒。

interval 该参数指定发送间隔，取值必须为 1 至 100 之间的整数，单位为秒。

lldp max_neighbors <number>

该参数指定每个启用 LLDP 功能的系统接口上允许的最大邻居数。

当不配置该命令时，默认值为 32。

number 该参数指定允许的最大邻居数，取值必须为 1 至 64 之间的整数。

show lldp config

该命令用于显示所有的 LLDP 配置。

show lldp neighbors

该命令用于显示所有的 LLDP 邻居信息。

clear lldp all

该命令用于将所有的 LLDP 配置恢复为默认设置。

ipv6 ndp <ipv6_address> <mac_address>

该命令用于配置一条静态 NDP 解析项。

ipv6_address 指定远程主机的 IPv6 地址。

mac_address 指定远程主机的 MAC 地址。

no ipv6 ndp <ipv6_address>

该命令用于删除指定 IPv6 地址的 NDP 解析项。

show ipv6 ndp

该命令用于显示系统中配置的静态和动态 NDP 解析项。

clear ipv6 ndp

该命令用于清除系统中配置的静态和动态 NDP 解析项。

ip pool <pool_name> <start_ip> [end_ip] [interface_name]

该命令用于创建一个 IP 地址池，并向该地址池中添加一个 IP 地址段。该命令也可以用于只添加 IP 地址段，一个 IP 地址池中可以添加多个 IP 地址段。如果输入的地址池名称不存在，设备将创建一个新的 IP 地址池。在设备中可以配置多个 IP 地址池，每个地址池最多能添加 256 个 IP 地址。

pool_name 该参数指定 IP 地址池的名称。取值必须为长度不大于 128 个字节的字符串。支持字母、数字、特殊字符，但必须以字母开头，包含特殊字符时，必须置于双引号内。

start_ip 该参数指定添加到地址池的 IP 地址段的起始 IP 地址。可以为 IPv4 或 IPv6 地址。

end_ip 可选参数。该参数指定添加到地址池的 IP 地址段的结束 IP 地址。可以为 IPv4 或 IPv6 地址。如果没有指定这个参数，则只有“start_ip”所指定的 IP 地址会被加入到地址池中。

interface_name 可选参数。指定接口名称，接口为已配置了 overlap 选

项的接口，比如系统接口，mnet 接口，bond 接口。只有当配置了 NUMA SLB（单一 VIP，反向代理模式下）时，才配置此参数。默认值为空，IP 地址池默认绑定在原始接口。



注意：

- 一个 IP 地址池只能与一个接口绑定。
- 通常情况下，多个 IP 地址池中的 IP 地址段可以重叠。但是如果一个 IP 地址池与配置了“overlap”的接口绑定后，该 IP 地址池中包含的 IP 地址不能被添加到其他 IP 地址池中。
- 设备可以支持多个 IP 地址池，每个地址池最多可以包含 256 个 IP 地址。根据设备内存大小的不同，所支持的 IP 地址池个数也不相同，具体如下表所示：

表3 - 1 最大 IP 地址池数

系统内存	最大 IP 地址池数
4GB	32
8GB	64
16GB	128
32GB	256

no ip pool <pool_name> [start_ip]

该命令用于从指定的 IP 地址池中删除 IP 地址段。

pool_name IP 地址池的名称。

start_ip 需要删除的 IP 地址段的起始 IP 地址。配置该参数后，该地址池中以“start_ip”开始的 IP 地址段将被删除。

该参数可选。如果没有配置起始 IP 地址，则删除该地址池。

clear ip pool [pool_name]

该命令用于删除指定的 IP 地址池。如果没有指定可选参数“pool_name”，则系统将删除所有的 IP 地址池。

show ip pool [pool_name]

该命令用于查看指定的 IP 地址池的配置信息。如果没有指定可选参数“pool_name”，则系统将显示所有 IP 地址池的信息。

3.2 IP 域表

3.2.1 IP 域表通用命令

show ipregion name

该命令用于显示系统中已经存在的 IP 域表的名称。

ipregion table import <ipregion_name> <url>

该命令用于从 HTTP 服务器或 FTP 服务器为系统导入自定义的 IP 域表。

ipregion_name 该参数指定需要加载的 IP 域表的名称。取值必须为最大长度不大于 24 个字节的字符串，区分大小写。参数取值不可以为预定义的 IP 域表的名称。

url 该参数指定加载的 IP 域表文件的 HTTP 或 FTP URL 地址，用于加载 IP 域表。

注意：FTP 类型 URL
(ftp://user:password@host:port/path) 中的“path”需使用相对路径。

自定义的 IP 域表需要包含以下信息项：

- IP subnet（IP 子网；采用 CIDR 格式）
- Country name（国家名称；可选，最长 7 个字节）
- Brief description（描述信息；可选，最长 63 个字节）

这些信息项必须用“Tab”键或空格分隔。

导入 IP 域表文件时，系统会对文件内容进行检查（不检查文件类型）。因此，为了确保可以成功导入 IP 域表文件，自定义的 IP 域表名需遵循以下格式：

IP subnet Country name Brief description

例如，定义一个文件名为“test.txt”的 IP 域表，包括以下内容：

27.8.0.0/13 CN China Unicom Chongqing Province network
27.36.0.0/14 CN China Unicom Guangdong Province network

导入该 IP 域表：

Demo(config)#ipregion table import test ftp://10.3.109.1/test.txt

如果 FTP 服务器要求提供登录用户名和密码，管理员需要在输入参数“url”时包含有效的用户名和密码信息，例如：

```
Demo(config)#ipregion table import test ftp://username:passwd@10.3.109.1/test.txt
```

ipregion table export <ipregion_name> <url>

该命令用于将 IP 域表从系统中导出到 FTP 服务器。

ipregion_name 该参数指定需要上传的 IP 域表的名称。

url 该参数指定 FTP URL。IP 域表文件将被上传到该地址。

注意：FTP 类型 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。

示例：

```
Demo(config)#ipregion table export test12 ftp://10.3.109.1/test
ipregion "test12" is successfully exported
```

如果 FTP 服务器要求提供登录用户名和密码，管理员需要在输入参数“url”时包含有效的用户名和密码信息，例如：

```
Demo(config)#ipregion table export test12 ftp://username:passwd@10.3.109.1/test
ipregion "test12" is successfully exported
```

no ipregion table <ipregion_name>

该命令用于删除指定的 IP 域表。

show ipregion table <ipregion_name>

该命令用于显示指定的 IP 域表的条目。

clear ipregion table [predefined]

该命令用于删除自定义或预定义的 IP 域表。

predefined 可选，该参数指定是否删除预定义的 IP 域表。取值必须为：

- predefined：表示删除预定义的 IP 域表。
- 空：表示删除自定义的 IP 域表。

默认值为空。

3.2.2 基于 GeoIP 的 IP 域表

系统支持基于 GeoIP 数据库生成 IP 域表，以下命令用于导入 GeoIP 数据库和生成国家级和中国省级 IP 域表。生成 IP 域表后，可以通过“IP 域表通用命令”小节的命令为系统导入 IP 域表或调整相关配置。

ipregion geoip import <region_level> <url>

该命令用于从指定的 URL 地址导入一个 GeoIP（Geolocation IP）数据库，用于生成 IP 域表。

导入国家级 GeoIP 数据库后，系统将生成以下三个 CSV 格式数据库（“YYYYMMDD”表示 GeoIP 数据库更新日期）：

- Country_IPv4_YYYYMMDD.csv：国家级 IPv4 地址数据库。
- Country_IPv6_YYYYMMDD.csv：国家级 IPv6 地址数据库。
- Country_Location_YYYYMMDD.csv：国家级区域数据库。

导入省级 GeoIP 数据库后，系统将生成以下三个 CSV 格式数据库（“YYYYMMDD”表示 GeoIP 数据库更新日期）：

- State_IPv4_YYYYMMDD.csv：省级 IPv4 地址数据库。
- State_IPv6_YYYYMMDD.csv：省级 IPv6 地址数据库。
- State_Location_YYYYMMDD.csv：省级区域数据库。

导入自定义 GeoIP 数据库后，系统将生成以下.signed.tar.gz 格式数据库（“YYYYMMDD”表示 GeoIP 数据库更新日期）：

- GeoIP_Custom_YYYYMMDD.signed.tar.gz：自定义 GeoIP 数据库。自定义的 GeoIP 数据库支持中国大陆以及港澳台。

注意：系统只支持导入 MaxMind 的 CSV 格式数据库的 ZIP 压缩文件，下载地址：<http://dev.maxmind.com/geoip/geoip2/geolite2/>。

region_level 该参数指定需要导入的 GeoIP 数据库的区域级别，取值必须为：

- country：表示导入一个国家级 GeoIP 数据库。
- state：表示导入一个省级 GeoIP 数据库。
- custom：表示导入一个自定义 GeoIP 数据库。导入自定义数据库后，管理员需要执行命令“**sdns ipregion proximity**”生成 SDNS IP 域就近性规则。

注意：

当取值为“custom”时，该命令仅支持运行时配置同步。

url 该参数指定需要导入的数据库文件的 URL 地址，必须置于双引号内，支持 FTP 和 HTTP 两种 URL 地址类型。请联系客户支持获取 URL 地址。

示例：

```
Demo(config)#ipregion geoip import state
“ftp://192.168.5.55/home/GeoLite2-City-CSV_20160503.zip”
```

show ipregion geoip

该命令用于显示系统内生成的所有格式的数据库。

ipregion geoip convert country <country_name>

该命令用于基于国家级 GeoIP 数据库生成指定国家的 IP 域表。执行该命令前，需使用“**ipregion geoip import**”命令导入国家级 GeoIP 数据库。

country_name 该参数指定国家名称，取值必须是国家级 GeoIP 数据库里“country_name”定义的国家名称。该参数也可以设置为“all”，表示生成所有国家的 IP 域表。

ipregion geoip convert state <country_name> <state_name>

该命令用于基于省级 GeoIP 数据库生成指定省的 IP 域表，系统目前仅支持生成中国省级或直辖市的 IP 域表。执行该命令前，需使用“**ipregion geoip import**”命令导入省级 GeoIP 数据库。

country_name 该参数指定国家名称，取值必须“china”。

state_name 该参数指定中国的省名称，取值必须为“hebei”等省名称或“shanghai”等直辖市名称。该参数也可以设置为“all”，表示生成所有中国省和直辖市的 IP 域表。

ipregion geoip custom network <geoip_network_ip> <country> <state> [city] [ISP][longitude] [latitude]

该命令用于将自定义的 IP 域表表项添加到导入的自定义 GeoIP 数据库中。

自定义的 GeoIP 数据库通过命令“**ipregion geoip import custom url**”导入。注意该命令添加的 IP 域表表项适用于生成 SDNS IP 域就近性规则。

geoip_network_ip 该参数指定待添加的 IP 域表表项的网段。
取值格式必须为“IP 地址/子网掩码”，其中 IP 地址可以为 IPv4 或 IPv6 地址。例如：“1.0.1.0/24”和

“2001:0218:6000:0005:0000:0000:0000:0000/64”。

取值为 IPv6 地址时，支持简写。

例如：“3ffb:0000:0000:0000:0000:0000:0000:0071/64”
可以简写为“3ffb::71/64”。

country	该参数指定待添加的 IP 域表表项的国家信息。 取值必须为“China”，不区分大小写。
state	该参数指定待添加的 IP 域表表项的省份信息。 例如“Hebei”，不区分大小写。
city	可选，该参数指定待添加的 IP 域表表项的市信息。 例如“Chengde”，不区分大小写。
ISP	可选，该参数指定待添加的 IP 域表表项的运营商信息。 取值必须为长度不大于 128 个字节的字符串。 当取值为 CMCC（中国移动）、CUCC（中国联通）、CTCC（中国电信）、CTT（中国铁通）或 CERNET（中国教育网）时，不区分大小写。 当取值为其他运营商时，原样保存到数据库中。
longitude	可选，该参数指定待添加的 IP 域表表项的经度。 取值支持整数和小数。整数部分取值必须为 0 到 180 之间，小数部分最多可以包含 6 位。若取值只包括整数，必须包含在双引号内。取值包含整数和小数的示例如 121.300999。
latitude	可选，该参数指定待添加的 IP 域表表项的纬度。 取值支持整数和小数。整数部分取值必须为 0 到 90 之间，小数部分最多可以包含 6 位。若取值只包括整数，必须包含在双引号内。取值包含整数和小数的示例如 24.993580。



注意：“`sdns ipregion proximity`”命令中的 ISP 只支持 CMCC（中国移动）、CUCC（中国联通）、CTCC（中国电信）、CTT（中国铁通）和 CERNET（中国教育网）。

no ipregion geoip custom network < geoip_network_ip >

该命令用于删除导入的自定义 GeoIP 数据库中的指定 IP 域表表项。

show ipregion custom log

该命令用于查看对 GeoIP 数据库进行修改（添加或删除自定义 IP 域表表项）的日志。需要注意的是只有成功添加或删除的 IP 域表表项才会记录到日志中。

示例：

```
2023/11/21 09:49:52 "ipregion geoip custom network 1.1.1.1/24 China Hebei"
2023/11/21 09:49:52 "no ipregion geoip custom network 2.2.2.2/24"
```

ipregion geoip custom rollback

该命令用于恢复 GeoIP 数据库到初始状态。执行该命令后，系统将删除所有向 GeoIP 数据库中添加的自定义 IP 域表表项。

restapi on [protocol] [port]

该命令用于启用 RESTful API 服务。该功能默认为禁用。

protocol 可选。该参数指定 RESTful API 服务使用的协议类型。
取值必须为“http”或“https”。

默认值为“https”。

port 可选。该参数指定基于 RESTful API 服务监听的端口号。
取值必须为 1025 至 65,000 之间的整数，但不能与其他服务使用的端口号相同。

默认值为 9997。

restapi off

该命令用于禁用 RESTful API 服务。

restapi ip <ip_address>

该命令用于设置 RESTful API 服务的监听 IP 地址。执行该命令后，管理员只能通过指定 IP 地址访问设备的 RESTful API 服务。

ip_address 该参数指定 RESTful API 服务监听的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

注意：

- 只有系统接口的 IP 地址和虚拟服务的 IP 地址可以配置为 RESTful API 的 IP 地址；
- 为了系统的安全，建议将管理接口的 IP 地址设置为 RESTful API 服务的监听 IP 地址。

clear restapi ip

该命令用于删除 RESTful API 服务的监听 IP 地址的设置。

clear restapi port

该命令用于将 RESTful API 服务的监听端口设置重置为默认值 9997。

restapi source <source_ip> <netmask|prefix> [action]

该命令用于添加一条 RESTful API 源 IP 地址限制规则。当参数 “source_ip” 与 “netmask|prefix” 的值与已配置规则的值相同时，该命令还可以修改该规则的动作。RESTful API 源 IP 地址限制规则的动作可以为 “permit” 或 “deny”。系统允许配置最多 100 条 RESTful API 源 IP 地址限制规则。

如果没有配置任何 RESTful API 源 IP 地址限制规则，系统对管理员通过 RESTful API 方式访问系统使用的源 IP 地址不受限制。如果配置了 RESTful API 源 IP 地址限制规则，当管理员通过 RESTful API 方式访问系统时：

- 当源 IP 地址匹配上一条 “permit” 规则，且没有匹配任何 “deny” 规则时，系统允许管理员通过 RESTful API 方式访问系统。
- 当源 IP 地址匹配上一条 “permit” 规则，但是也匹配上一条 “deny” 规则时，系统拒绝管理员通过 RESTful API 方式访问系统。
- 当源 IP 地址没有匹配上任何一条 “permit” 规则，系统拒绝管理员通过 RESTful API 方式访问系统。

source_ip 该参数指定通过 RESTful API 方式访问系统的源 IP 地址或网段。参数取值可以为 IPv4 或 IPv6。

注意：对于 IPv4 地址，参数取值不能为 “0.0.0.0”。对于 IPv6 地址，参数取值不能为 “：：”。

netmask|prefix 该参数指定源 IP 地址或网段对应的子网掩码或前缀长度。

- “netmask” 用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 1 到 128 之间的整数。

action 可选，该参数指定通过 RESTful API 方式访问系统的源 IP 地址匹配该规则时所采取的动作。参数取值可以为：

- **permit**: 允许指定的源 IP 地址或网段通过 RESTful API 方式访问系统。
- **deny**: 拒绝指定的源 IP 地址或网段通过 RESTful API 方式访问系统。

默认值为“permit”。



注意：如果只配置了“deny”规则，管理员不能从任何网段通过 RESTful API 方式访问系统。

no restapi source <source_ip> <netmask|prefix>

该命令用于删除指定的 RESTful API 源 IP 地址限制规则。

clear restapi source

该命令用于清除所有的 RESTful API 源 IP 地址限制规则。

show restapi settings

该命令用于显示 RESTful API 服务的配置（SSL 配置除外）。



注意：如果要访问 RESTful API 服务，需要使用拥有 API 权限级别的管理员账户，并使用 HTTP 基本认证方式进行认证。关于如何创建拥有 API 权限级别的管理员账户，请参见命令“**user <user_name> [password] [level]**”。

restapi ssl settings protocol <version>

该命令用于指定 RESTful API 服务支持的 SSL 协议版本。当不配置该命令时，默认的 SSL 协议版本为“TLSv12”。

version 该参数指定 RESTful API 服务支持的 SSL 协议版本。如果要配置多种版本，请使用冒号（:）来分隔协议版本。取值必须为：

- SSLv3: 表示支持 SSLv3 协议版本。
- TLSv1: 表示支持 TLSv1.0 协议版本。
- TLSv11: 表示支持 TLSv1.1 协议版本。
- TLSv12: 表示支持 TLSv1.2 协议版本。
- ALL: 表示支持以上全部协议版本。

restapi ssl settings ciphersuites <cipher_string>

该命令用于指定 RESTful API 服务支持的密码套件。

当不配置该命令时，默认的密码套件为

“ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:

ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AE
S128-GCM-SHA256:AES256-GCM-SHA384”。

cipher_string

该参数指定 RESTful API 服务支持的密码套件。取值不区分大小写。如果要配置两种或两种以上密码套件，请使用冒号 (:) 来分隔密码套件。目前，RESTful API 服务支持的密码套件如下：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES256-SHA256

restapi ssl import certificate [url]

该命令用于通过复制粘贴的方式或者从远端 FTP、TFTP 或 HTTP 服务器为 RESTful API 服务导入 PEM 格式的证书链文件。PEM 格式的证书链文件包括证书链和关联的私钥。

当未指定“url”参数时，可以通过将 PEM 格式的证书链复制粘贴到 CLI 的方式导入证书。证书内容的最后一行必须输入“...”用于标记导入结束。

如果不配置该命令，系统将使用默认的证书。

url

可选。该参数指定导入 PEM 格式的证书链文件的 FTP、TFTP 或 HTTP URL。如果没有指定该参数，可以通过复制粘贴的方式导入证书链文件。



注意：系统暂不支持导入 SM2 证书和 RSAPSS 证书。

show restapi ssl certificate

该命令用于显示为 RESTful API 服务所导入的证书链文件的内容。如果尚未导入证书链文件，该命令显示默认的证书。

clear restapi ssl certificate

该命令用于清除为 RESTful API 服务导入的证书链文件。

restapi ssl import clientca [url]

该命令用于通过复制粘贴的方式或者从远端 FTP、TFTP 或 HTTP 服务器为 RESTful API 服务导入用于 SSL 客户端认证的客户端 CA 证书。

当未指定“url”参数时，可以通过将 PEM 格式的证书复制粘贴到 CLI 的方式导入证书。证书内容的最后一行必须输入“...”用于标记导入结束。

url 可选，该参数指定导入证书的 FTP、TFTP 或 HTTP URL。如果没有指定该参数，可以通过复制粘贴的方式导入证书。

show restapi ssl clientca

该命令用于显示为 RESTful API 服务所导入的客户端 CA 证书。

clear restapi ssl clientca

该命令用于删除为 RESTful API 服务所导入的客户端 CA 证书。

restapi ssl settings clientauth enable

该命令用于为 RESTful API 服务启用 SSL 客户端认证功能，即 SSL 双向认证功能。启用该功能后，在登录 RESTful API 服务执行 SSL 握手时，客户端和服务端将执行 SSL 双向认证。该功能默认设置为禁用。启用该功能前，需要使用“**restapi ssl import clientca**”命令为 RESTful API 服务导入客户端 CA 证书。

restapi ssl settings clientauth disable

该命令用于为 RESTful API 服务禁用 SSL 客户端认证功能。

restapi ssl settings authmandatory enable

该命令用于为 RESTful API 服务启用 SSL 客户端认证强制模式。开启该模式后，RESTful API 服务的 SSL 客户端必须通过身份认证后才能正常登录设备，否则 SSL 连接请求将失败。该功能默认设置为启用。启用强制模式前，请先通过“**restapi ssl settings clientauth enable**”命令启用 SSL 客户端认证功能。

restapi ssl settings authmandatory disable

该命令用于为 RESTful API 服务禁用 SSL 客户端认证强制模式。

show restapi ssl settings

该命令用于显示所有 RESTful API 服务的 SSL 功能的配置信息。

例如：

```
Demo(config)#show restapi ssl settings
restapi ssl settings clientauth disable
restapi ssl settings authmandatory enable
restapi ssl settings ciphersuites
"ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384"
restapi ssl settings protocol "TLSv12"
```

clear restapi ssl settings

该命令用于将 RESTful API 服务的 SSL 配置恢复为默认值。

crontab {enable|disable}

该命令用于启用或禁用 Crontab 功能。如果启用 Crontab 功能，系统将在每小时的 0、10、20、30、40 和 50 这些时间点扫描 Crontab 文件，并执行命令启动时间早于或晚于这些时间点 5 分钟之内的 CLI 命令。例如，如果当前时间为 12:50，系统将执行启动时间在 12:45:00 到 12:54:59 之间的 CLI 命令。

在启用 Crontab 功能前，请先使用命令“crontab import”导入 Crontab 文件。该功能默认设置为禁用。

Crontab 文件中可以包含多个 Crontab 条目，每个 Crontab 条目由时间信息项和 CLI 命令组成，其中时间信息项指定 CLI 命令的启动时间。

Crontab 条目支持两种格式：

- 绝对日期：year-month-day hour:minute command
- 周期性：day-of-week hour:minute command

时间信息项中参数的取值范围如下表所示：

表3 - 2 时间信息项参数取值范围

时间信息项	参数取值范围
minute	00-59
hour	00-23
day	01-31
month	01-12
day-of-week	0 到 7：1 到 7 表示星期一到星期日；“0”表示星期日。
	Mon、Tue、Wed、Thu、Fri、Sat 或者 Sun。
	weekday：表示每周的星期一到星期五。
	weekend：表示每周的星期六和星期日。

	daily: 表示每周的星期一到星期日。

各个时间信息项必须通过“Tab”键或空格分隔。对于参数“day-of-week”，取值区分大小写。

示例：

- 定义一个文件名为“Eroute.txt”的 Crontab 文件，使得系统在周一到周五每天的 08:00 中增加一条 Eroute “p1”，在 22:00 删除 Eroute “p1”。其 Crontab 文件内容如下：

```
weekday 08:00 ip eroute "p1" 1300 0.0.0.0 0.0.0.0 0 2.1.1.0 255.255.255.0 0 any 1.1.1.1 1
weekday 22:00 no ip eroute "p1"
```

- 定义一个文件名为“Eroute.txt”的 Crontab 文件，使得系统在 2014 年 10 月 10 日的 08:00 中增加一条 Eroute “p2”，在 2014 年 10 月 15 日的 22:00 删除 Eroute “p2”。其 Crontab 文件内容如下：

```
2014-10-10 08:00 ip eroute "p2" 1300 0.0.0.0 0.0.0.0 0 3.1.1.0 255.255.255.0 0 any 1.1.1.1 1
2014-10-15 22:00 no ip eroute "p2"
```



注意：

- 建议管理员启用 Crontab 功能前，确保系统当前的配置和 Crontab 文件指定的配置不冲突，否则可能导致无法预知的错误。
- Crontab 功能不支持命令“ip address”、“ip route”、“ssh ip”、“bond”、“hostname”、“mnet”、“vlan”、“webwall”、“webui ip”、“cluster virtual priority”、“interface name”、“interface speed”、“interface mtu”、“interface mac”、“ha ssf peer”、“accesslist”和“accessgroup”。

crontab import <url>

该命令用于导入 Crontab 文件。系统只允许导入一个 Crontab 文件。

url 该参数指定用于导入 Crontab 文件的 HTTP 或 FTP URL 地址。取值必须为支持大小写字母、数字、特殊字符的字符串。仅支持以下特殊字符：“@”、“!”、“-”、“_”、“.”、“/”、“:”。

注意：FTP 类型 URL (ftp://user:password@host:port/path) 中的“path”需使用相对路径。

crontab export <url>

该命令用于导出系统中当前的 Crontab 文件。

url 该参数指定将 Crontab 文件导出到的 FTP URL 地址。

注意: FTP 类型 URL (ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

show crontab file

该命令用于显示已导入的 Crontab 文件的内容。

show crontab config

该命令用于显示当前 Crontab 的配置。

3.3 VXLAN

vxlan enable

该命令用于启用虚拟扩展局域网 (Virtual eXtensible Local Area Network, VXLAN) 功能。默认情况下, 该功能是禁用的。

vxlan disable

该命令用于禁用 VXLAN 功能。

vxlan mode <p2mp|multicast>

该命令用于设置 VXLAN 功能的工作模式。管理员应该在配置 VXLAN 隧道前指定 VXLAN 的工作模式。请注意如果修改了 VXLAN 功能的工作模式, 需要清除 VXLAN 隧道和接口的绑定关系, 否则 VXLAN 功能将无法正常工作。如果不配置该命令, 默认的工作模式为 p2mp。

p2mp|multicast

该参数指定 VXLAN 的工作模式。取值必须为:

- **p2mp:** 在该工作模式下, 在一个 VXLAN 中, 管理员需要手动为设备与所有的 VXLAN 隧道端点 (VXLAN Tunnel End Point, VTEP) 建立单播隧道。
- **multicast:** 在该工作模式下, 在一个 VXLAN 中, 管理员只需要为设备建立一个到该 VXLAN 的多播隧道。

show vxlan mode

该命令用于显示 VXLAN 功能的工作模式。

vxlan learn <on|off>

该命令用于启用或禁用 VXLAN 学习功能。启用该功能后, 设备将自动学习 VTEP IP 和 MAC 地址间的映射关系。请注意只有当所有 VTEP IP 地址和 MAC 地址间

的映射关系都为手动配置时，才能禁用该功能。否则，网络中将会存在大量 Flooding 报文。默认情况下，该功能是启用的。



注意：学习的转发表项的有效期为 20 分钟，超时后将被删除。

show vxlan learn

该命令用于显示 VXLAN 学习功能的状态。

vxlan port <vxlan_port>

该命令将用于设置 VXLAN 隧道的目的端口号。如果不配置该命令，默认目的端口号为 4789。

vxlan_port 该参数指定 VXLAN 隧道的目的端口号。取值必须为 1025 到 65,000 之间的整数。

show vxlan port

该命令用于显示 VXLAN 隧道的目的端口号。

vxlan interface <vxlan_ifname> <vni>

该命令用于创建一个 VXLAN 接口并指定其所属 VXLAN 网络。VXLAN 接口支持设置 IP 地址、IP 服务池和 WebWall 功能。系统允许配置最多 32,768 个 VXLAN。

每个创建的 VXLAN 接口将成为该 VXLAN 网络中的本地 VTEP。

vxlan_ifname 该参数指定 VXLAN 接口的名称。取值必须为长度不大于 32 个字符的字符串，支持字母、数字和特殊字符，字母不区分大小写。

支持的特殊字符：“@”、“!”、“~”、“_”、“:”、“-”、“.”。

vni 该参数指定用于标识 VXLAN 的 VNI 号。取值必须为 1 到 32,768 之间的整数。



注意：

- VXLAN 接口不支持配置 MTU。
- 在 HA 环境中，VXLAN 接口的配置可以同步到对端的 HA 节点。

no vxlan interface <vxlan_ifname>

该命令用于删除指定的 VXLAN 接口。

show vxlan interface

该命令用于显示所有的 VXLAN 接口。

clear vxlan interface

该命令用于清除所有的 VXLAN 接口。

vxlan tunnel < tunnel_name > < local_ip > < remote_ip >

该命令用于创建一条 VXLAN 隧道。设备支持两种类型的 VXLAN 隧道：单播和多播。系统支持创建最多 64 条 VXLAN 单播和多播隧道。

当 VXLAN 工作模式为 p2mp 时，针对每个 VXLAN 网络，管理员需要创建到每个 VTEP 的单播隧道，并将与这些隧道与相应的 VXLAN 接口绑定。

当 VXLAN 工作模式为 multicast 时，管理员需要创建一条到该 VXLAN 的多播隧道，并将该隧道与相应的 VXLAN 接口绑定。

tunnel_name 该参数指定 VXLAN 隧道的名称。取值必须为长度不大于 32 个字节的字符串。

local_ip 该参数指定本地 VTEP IP 地址。取值必须为 IPv4 或 IPv6 地址。取值可以为设备上的接口 IP 地址，也可以为集群虚拟 IP 地址和 HA 浮动 IP 地址。当本地 VTEP IP 地址为集群虚拟 IP 地址或 HA 浮动 IP 地址时，隧道的配置可以被同步到对端节点。

remote_ip 该参数指定远端 VTEP IP 地址。取值必须为 IPv4 或 IPv6 地址。如果要创建单播隧道，参数取值应设为单播 IP 地址；如果要创建多播隧道，参数取值应为多播 IP 地址。

注意： 推荐为不同的多播隧道配置不同的多播组地址。

no vxlan tunnel < tunnel_name >

该命令用于删除指定的 VXLAN 隧道。

show vxlan tunnel [tunnel_name]

该命令用于显示指定的 VXLAN 隧道的配置。如果不指定参数 “tunnel_name”，将显示所有 VXLAN 隧道的配置。

clear vxlan tunnel

该命令用于清除所有的 VXLAN 隧道的配置。

vxlan bind < vxlan_ifname > < tunnel_name >

该命令用于将 VXLAN 接口与 VXLAN 隧道绑定。一个 VXLAN 接口可以绑定最多 12 条单播 VXLAN 隧道(p2mp 工作模式下)或一条多播 VXLAN 隧道(multicast 工作模式下)。

vxlan_ifname 该参数指定已存在的 VXLAN 接口的名称。

tunnel_name 该参数指定已存在的 VXLAN 隧道的名称。

no vxlan bind <vxlan_ifname> <tunnel_name>

该命令用于删除 VXLAN 接口和 VXLAN 隧道间的绑定关系。

show vxlan bind [vxlan_ifname]

该命令用于显示指定的 VXLAN 接口上绑定的隧道配置。如果不指定参数“vxlan_ifname”，所有 VXLAN 接口上绑定的配置都将被显示。

clear vxlan bind [vxlan_ifname]

该命令用于清除指定的 VXLAN 接口上绑定的隧道配置。如果不指定参数“vxlan_ifname”，所有 VXLAN 接口上的绑定配置都将被清除。

vxlan associate <vxlan_ifname> <vlan_ifname>

该命令通过将 VXLAN 接口与 VLAN 接口关联。该命令在设备作为 VXLAN 二层网关的场景下才需要配置。一个 VXLAN 接口只可以与一个 VLAN 接口关联。

vxlan_ifname 该参数指定 VXLAN 接口的名称。

vlan_ifname 该参数指定 VLAN 接口的名称。

no vxlan associate <vxlan_ifname>

该命令通过删除 VXLAN 接口与 VLAN 接口之间的关联关系。

show vxlan associate [vxlan_ifname]

该命令用于显示指定的 VXLAN 接口关联的 VLAN 接口。如果不指定参数“vxlan_ifname”，将显示所有 VXLAN 接口关联的 VLAN 接口。

clear vxlan associate

该命令用于清除所有的 VXLAN 接口与 VLAN 接口的关联关系。

vxlan forwarding remote <vni> <mac_address> <vtep_ip>

该命令用于为指定的 VXLAN 网络的远端 VTEP 添加一个静态 VXLAN 转发表项。

vni 该参数指定用于标识 VXLAN 的 VNI 号。

mac_address 该参数指定目的 MAC 地址。

vtep_ip 该参数指定远端 VTEP IP 地址。



注意：系统支持为每个 VXLAN 网络配置 2000 个静态 VXLAN 转发表项。（包括远端 VTEP 和 L2 接口的转发表项）

no vxlan forwarding remote <vni> <mac_address>

该命令用于删除指定的 VXLAN 网络的远端 VTEP 的一个静态 VXLAN 转发表项。

vxlan forwarding local <vni> <mac_address>

该命令用于为指定的 VXLAN 网络的 L2 接口添加一个静态 VXLAN 转发表项。

vni 该参数指定用于标识 VXLAN 的 VNI 号。

mac_address 该参数指定目的 MAC 地址。



注意：系统支持为每个 VXLAN 网络配置 2000 个静态 VXLAN 转发表项。（包括远端 VTEP 和 L2 接口的转发表项）

no vxlan forwarding local <vni> <mac_address>

该命令用于删除指定的 VXLAN 网络的 L2 接口的一个静态 VXLAN 转发表项。



注意：在删除 VXLAN 接口与 VLAN 接口之间的关联关系后，需要手动删除 L2 接口的静态转发表。

show vxlan forwarding <vni> [mac_address]

该命令用于显示指定 VXLAN 网络的所有 VXLAN 转发表项。

vni 该参数指定用于标识 VXLAN 的 VNI 号。

mac_address 可选，该参数指定 MAC 地址。如果指定该参数，与该 MAC 地址相关的 VXLAN 转发表项将被显示。默认值为空，表示所有 VXLAN 转发表项都将被显示。

clear vxlan forwarding dynamic <vni>

该命令用于清除指定 VXLAN 网络的所有动态 VXLAN 转发表项。

clear vxlan forwarding static <vni>

该命令用于清除指定 VXLAN 网络的所有静态 VXLAN 转发表项。

show vxlan all

该命令用于显示 VXLAN 功能的所有配置。

clear vxlan all

该命令用于清除 VXLAN 功能的所有配置。

第4章 链路聚合

本章介绍链路聚合（Link Aggregation）功能的相关配置命令。

bond name <bond_id> <bond_name>

该命令用于配置指定聚合接口的名称。系统最多支持 8 个聚合接口。

bond_id 该参数指定设备上聚合接口的默认接口 ID（bond1、bond2、bond3、bond4……）。

bond_name 该参数指定聚合接口名称。取值必须为长度不超过 31 个字符的字符串，支持字母、数字和特殊字符，字母不区分大小写。默认的聚合接口名称为 bond1、bond2、bond3、bond4……。

支持的特殊字符：“@”、“!”、“~”、“_”、“:”、“-”、“.”。

bond interface <bond_name> <interface_name> [1|0]

这条命令允许用户把某个网络接口绑定到指定的聚合接口上。一个聚合接口最多可以绑定 12 个网络接口。

参数“1|0”用于将网络接口设置为聚合接口上的主接口（1）或备用接口（0）。每个聚合接口上可以设置多个主接口或备用接口。当所有主接口都无法工作时，备用接口将接替主接口开始工作。

bond_name 聚合接口名称，由字母和数字组成。默认的聚合接口名称为 bond1、bond2、bond3、bond4……。

interface_name 系统接口名称，由字母和数字组成；默认值为 port1、port2、port3、port4……。系统接口名称通过命令“**interface name**”来设置。

1|0 1：表示将网络接口设置为聚合接口上的主接口。默认情况下，设置为主接口（1）。

0：表示将网络接口设置为聚合接口上的备用接口。

no bond interface <bond_name> <interface_name>

这条命令允许用户从指定的聚合接口上删除已经绑定的接口。

show bond [bond_name]

这条命令显示所有当前系统聚合接口的信息。如果指定了接口名称，则只显示该接口的信息。

clear bond [bond_name]

这条命令把聚合接口配置重置成默认值。如果不指定接口名称，则清除所有聚合接口的配置。

**bond health <bond_name> <destination_ip> [interval] [timeout]
[up_check_times] [down_check_times] [gateway_ip]**

该命令用于为聚合接口配置并启用健康检查。设备通过聚合接口的每个子接口向目的地址发送 ICMP echo 请求，并检查是否收到相应的 ICMP echo 响应。如果连续收到的 ICMP echo 响应的次数达到参数“up_check_times”指定的值，则该子接口标记为“up”；如果连续未收到 ICMP echo 响应的次数达到参数

“down_check_times”指定的值，则该子接口标记为“down”。默认情况下健康检查是禁用的。

bond_name	指定聚合接口的名称。由字母和数字组成，最多支持 32 个字符。默认的聚合接口名称为 bond1、bond2、bond3、bond4……。
destination_ip	指定目的 IP 地址。可以为 IPv4 地址或 IPv6 地址。
interval	可选参数。指定发送 ICMP echo 请求的时间间隔。取值范围为 1~65535。默认值为 5。单位为秒。
timeout	可选参数。该参数用于指定从发送 ICMP echo 请求到收到 ICMP echo 响应的的时间间隔，即超时时间。取值范围为 1~65535。默认值为 3。单位为秒。
up_check_times	可选参数。指定连续收到 ICMP echo 响应的次数。如果连续收到的 ICMP echo 响应的次数达到参数“up_check_times”指定的值，则标记为“up”。取值范围为 1~65535。默认值为 3。
down_check_times	可选参数。指定连续未收到 ICMP echo 响应的次数。如果连续未收到的 ICMP echo 响应的次数达到参数“down_check_times”指定的值，则标记为“down”。取值范围为 1~65535。默认值为 3。
gateway_ip	可选参数。指定网关的 IP 地址。可以为 IPv4 地址或 IPv6 地址。对于 IPv4 地址，默认值为 0.0.0.0；对于 IPv6 地址，默认值为：：。注意：如果参数“destination_ip”的值与聚合接口不在同一网段，必须配置参数“gateway_ip”。

no bond health <bond_name>

该命令用于删除指定聚合接口的健康检查。

第5章 集群

本章介绍集群功能的相关配置命令。

show cluster virtual status [*interface_name*]

这条命令用于显示所有接口上的虚拟集群的运行状态信息。如果指定了某个接口名称，则只显示与该接口相关的集群运行信息。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。

例如：

```
Demo(config)#show cluster virtual status
ffo cable status: remote no power
discreet mode enabled

ifname= port1
vcid      off/on   vc state
1         on      master

ifname= port2
vcid      off/on   vc state
1         on      master

ifname= mnet1
vcid      off/on   vc state
1         on      master
```

cluster virtual {on|off} [*cluster_id|0*] [*interface_name*]

这条命令用于启用或者禁用设备的虚拟集群功能。虚拟集群 ID 的取值范围为 1~255。使用这条命令时用户必须指定正确的接口名称。如果没有在命令中指定集群 ID 或接口名称，所有的集群会被启用。

cluster virtual ffo {on|off}

这条命令用于启用或者禁用快速失效切换功能。默认值是禁用该功能。

cluster virtual ffo interface carrier loss timeout <*interface_timeout*>

这条命令用于设置在快速失效切换之前网卡载波丢失的超时时间(单位为毫秒)。如果在超时时间范围内重新获得网卡载波，设备不会进行快速失效切换。超时时间的取值范围为 0~65535，0 表示立即切换，65535 表示不进行快速失效切换。

system test failover port [*on/off*]

这条命令用于检测快速失效切换端口是否正常。设备提供基于 USB 的 FFO 端口。



注意：在运行这条命令之前，请确认已经使用“**cluster virtual ffo off**”命令禁用 FFO 功能。

管理员可以执行如下步骤检查 USB 端口的状态：

1. 把 USB FFO 线一段插入设备的 USB 端口，另外一段插在 PC 机上。
2. 在 PC 机上安装 USB 驱动，确保 PC 机能够识别设备。
3. 在 PC 机上，打开终端软件，连接 USB-COM 端口。
4. 运行“**system test failover port on**”命令启用 testing 模式。
5. 按键盘上任意键，查看输入的字符是否在终端软件上显示。

显示：USB 类型 FFO 端口正常。

不显示：USB 类型 FFO 端口故障。

6. 运行“**system test failover port off**”命令禁用 testing 模式。

show cluster virtual config [interface_name]

这条命令用于显示所有接口上的虚拟集群配置信息。如果指定了某个接口名称，则只显示与该接口相关的集群配置信息。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。默认值为 all。

例如：

```
Demo(config)#show cluster virtual config port2
cluster virtual ifname "port2" 1
cluster virtual vip "port2" 1 10.30.0.30
cluster virtual auth "port2" 1 1 "myString"
cluster virtual interval "port2" 1 10
cluster virtual preempt "port2" 1 0
cluster virtual priority "port2" 1 200
```

show cluster virtual ffo

这条命令用于显示当前快速失效切换功能的所有配置。

cluster virtual ifname <interface_name> <cluster_id>

这条命令用于为一个网络接口创建一个虚拟集群 ID。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接

口或 MNET 接口。

cluster_id 虚拟集群 ID，取值范围为 1~255。



注意：

- 如果系统中配置的虚拟集群 ID（VCID）的数量太多,可能会引起不必要的系统超载。因此，建议不要配置过多的 VCID。如果需要配置多个虚拟 IP 地址，可以在同一个 VCID 中配置多个虚拟 IP 地址，而不是为每个虚拟 IP 地址配置一个 VCID。
- 如果本地节点上指定的接口只配置了 IPv6 地址，且对端节点上指定的接口也配置了 IPv6 地址，那么两节点间使用 IPv6 链路发送 VRRP 报文。如果两个节点上指定的接口既配置了 IPv4 地址又配置了 IPv6 地址，那么两节点间使用 IPv4 链路发送 VRRP 报文。

show cluster virtual interface

这条命令用于查看用户通过“**cluster virtual ifname**”命令配置的所有接口上的集群。

clear cluster virtual ifname <interface_name> <cluster_id>

这条命令用于删除指定接口上的虚拟集群。

interface_name 该参数指定接口名称，取值必须为系统接口、聚合接口、VLAN 接口、MNET 接口名称或“all”（所有接口）

cluster_id 该参数指定虚拟集群的 ID，取值必须为 0 至 255 之间的整数。取值 0 表示所有虚拟集群。

cluster virtual vip <interface_name> <cluster_id> <vip>

这条命令用于为指定接口上的虚拟集群设置虚拟 IP 地址。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。

cluster_id 虚拟集群 ID，取值范围为 1~255。每个集群 ID 最多可以配置 255 条 IP 地址，不同接口上相同的集群 ID 数值将被当作不同的虚拟 ID。一个虚拟 ID 上所有的虚拟 IP 地址具有同样的状态（Master 或 Backup）。

vip 虚拟 IP 地址，不能设置为 0.0.0.0 以及 255.255.255.255，也不能设置为环回地址、多播地址等专用地址。每个虚拟 IP 地址可以是 IPv4 或者 IPv6 地址，且必须是唯一的。



注意：当同一业务通过多个虚拟 IP 提供服务时（无论使用的接口是否相同），所有虚拟 IP 关联的 VCID 必须相同。否则该业务会被划分到不同集群中，可能出现集群

状态不一致的情况。

cluster virtual auth <interface_name> <cluster_id> {0|1} [password]

该命令用于启用及配置虚拟集群身份认证功能。

interface_name	指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。
cluster_id	指定虚拟集群 ID，取值范围为 1~255。
0 1	指定身份认证类型。0 表示不使用密码；1 表示使用明文密码。
password	当身份认证类型设置为 1 时，需要指定身份认证所需的密码，最多由 8 位字符组成。如果密码字符串为数值，需要将其置于双引号内。

cluster virtual preempt <interface_name> <cluster_id> <mode>

这条命令用于配置集群抢占模式。（注意：集群的优先级被配置成 255 除外。）

interface_name	指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。
cluster_id	已配置的虚拟集群 ID。
mode	指定虚拟集群抢占模式，其值可以为 1 或者 0，默认值为 1。 1：允许集群中高优先级的主机抢占网络地址。 0：禁用集群中高优先级的主机抢占网络地址。 其中，缺省值为 1。

cluster virtual interval <interface_name> <cluster_id> <seconds>

该命令用于设置虚拟集群广播的时间间隔。

interface_name	指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。
cluster_id	指定已配置的虚拟集群 ID。
seconds	指定虚拟集群广播的时间间隔，单位为秒。该参数的取值为 3 到 255 之间的整数，默认值为 5。虚拟集群的状态切换花费的时间大约为该时间间隔的二至三倍。



注意：集群中主机与备机上的相同接口的同一个虚拟集群 ID，其广播时间间隔应设置为相同的值。否则，集群中会出现两个设备的状态同时为“MAST”的情况，从而导致集群不能正常工作。

cluster virtual priority <interface_name> <cluster_id> <priority>
[synconfig_peer_name]

该命令用于设置虚拟集群的优先级。如果不配置该命令，虚拟集群的默认优先级为 100。每个接口支持定义最多 64 个节点的优先级。

interface_name	指定接口的名称。可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。
cluster_id	指定虚拟集群的 ID。
priority	指定虚拟集群的优先级。数值越大，优先级越高。取值范围为 1~255。
synconfig_peer_name	可选参数。指定本地节点或对端节点的名称。参数值可以为“Primary”或命令“ synconfig peer <peer_name> <peer_ip>”定义的任何节点的名称。当参数值为“Primary”时，该命令配置本地节点。当参数值为命令“ synconfig peer <peer_name> <peer_ip>”定义的节点的名称时，该命令配置相应的节点。默认值为“Primary”。



注意：为了将虚拟集群的优先级同步到对端节点，需要在本地节点上配置命令“**synconfig peer** <peer_name> <peer_ip>”定义的本地节点和对端节点的虚拟集群优先级。

no cluster virtual vip <interface_name> <cluster_id> <vip>

删除指定集群 ID 和接口上的虚拟 IP。



注意：

- 如果删除了集群中主机或备机上的虚拟集群的 VIP，设备状态会立即切换为“INIT”，同时，集群将会执行主备切换动作。
- 若主机和备机上的虚拟集群配置信息不一致，可能会出现两个设备的状态同时为“MAST”，从而引起 IP 冲突。因此，在更改集群的主机配置之前，建议首先关闭备机的集群功能，然后在主机配置更改完成之后，将主机上的配置同步至备机。

no cluster virtual auth <interface_name> <cluster_id>

该命令用于恢复集群身份认证功能为缺省值，即禁用集群身份认证功能。

no cluster virtual interval <interface_name> <cluster_id>

恢复发包时间间隔为缺省值（5 秒）。

no cluster virtual preempt <interface_name> <cluster_id>

该命令用于恢复集群抢占模式为缺省值，即启用抢占模式。

no cluster virtual priority <interface_name> <cluster_id>
[synconfig_peer_name]

该命令用于恢复集群优先级为缺省值（100）或从本机上删除参数“synconfig_peer_name”指定的节点的集群优先级信息。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。

cluster_id 指定已配置的虚拟集群 ID。

synconfig_peer_name 可选参数，默认值是“Primary”。除默认值以外，参数“synconfig_peer_name”的值可以是任何一个由命令“**synconfig peer** <peer_name> <peer_ip>”定义的同步配置节点的名称。当参数“synconfig_peer_name”的值为“Primary”或本地节点的同步配置节点名称时，该命令将本地节点的集群优先级恢复为默认值（100）。当参数“synconfig_peer_name”的值为其他同步配置节点名称时，该命令仅从本机上删除该名称对应的节点的集群优先级信息。

cluster virtual discreet {on|off}

该命令用于启用或禁用集群的谨慎备份模式（Discreet Backup）。在该模式下，系统通过主设备和从设备之间的一条心跳线（Heartbeat cable）收集主从设备的状态信息，从而确定主从设备的状态，最终正确判断是否需要切换设备的主从状态。在该模式下，设备之间的状态切换更加稳妥，不会因为 VRRP 包的丢失造成双主机状态。缺省情况下，该模式是禁用的。



注意：谨慎备份模式需要通过心跳线来确定主设备和从设备的状态，因此首先必须保证主从设备之间通过心跳线连接，并且使用“**cluster virtual ffo on**”命令将心跳线启用（心跳线与 FFO cable 是同一条线）。

show cluster virtual discreet

该命令用于显示谨慎备份模式的配置

show cluster virtual transition [interface_name]

该命令用于显示指定接口的最近 100 条集群状态转换日志。如果没有指定接口，则显示所有接口的最近 100 条集群状态转换日志。集群状态包括初始状态

(INIT)、备份状态 (BACK)、谨慎备份状态 (DISCREET)、快速失效切换状态 (FFO) 以及主状态 (MAST)。

interface_name 指定接口名称，可以为系统接口、聚合接口、VLAN 接口或 MNET 接口。默认值是 “all”。

例如：

```
Demo(config)#show cluster virtual transition
ifname = port1, vcid = 1
Sep 25 17:36:22 (+0000) [BACK -> MAST] Timeout.
Sep 25 17:36:17 (+0000) [DISCREET -> BACK] Receive a VRRP advertisement of priority 0.
Sep 25 17:34:58 (+0000) [BACK -> DISCREET] Entering discreet mode.
Sep 25 17:34:58 (+0000) [FFO -> BACK] FFO cable is OK. Cluster is ready to work.
Sep 25 17:34:58 (+0000) [INIT -> FFO] FFO is enabled.
Sep 25 17:34:56 (+0000) [BACK -> INIT] Stop running.
Sep 25 17:34:56 (+0000) [FFO -> BACK] FFO cable is OK. Cluster is ready to work.
Sep 25 17:34:56 (+0000) [INIT -> FFO] FFO is enabled.
```

clear cluster virtual transition [interface_name] [cluster_id]

这条命令用于删除指定虚拟集群或者所有虚拟集群的接口上的集群状态转换日志。缺省情况下，参数 “interface_name” 值为 “all”，表示删除所有接口的集群状态转换日志。参数 “cluster_id” 的缺省值为 “0”，表示删除所有虚拟集群的接口上的集群状态转换日志。

show statistics cluster virtual [interface]

这条命令用于显示指定接口的虚拟集群统计信息。如果没有指定接口，则显示所有接口上的虚拟集群统计信息。

例如：

```
Demo(config)#show statistics cluster virtual
ifname = port1, vcid = 1
transition to master: 1
（转换为主状态，获得 VIP）
quit master: 0
（退出主状态，释放 VIP）
VRRP loss: 0
（可能丢失 VRRP 包：设备在备份状态时，两个时间间隔内没有收到任何来自主设备 VRRP 通告（advertisement），但是在超时（三个时间间隔）之前却收到了一个有效的 VRRP 通告。）
quick transition: 2
（收到优先级为 0 的 VRRP 通告：被用于快速状态转换）
inconsistency: 0
```

（检测与同一 VCID 的其他接口状态不一致的状态，丢掉优先级比自身优先级低的 VRRP 包。）

提示：以上括号里的内容是对各项输出信息的解释。

clear statistics cluster virtual [interface_name] [cluster_id]

该命令用于删除指定虚拟集群或者所有虚拟集群的接口的统计信息。缺省情况下，参数“interface_name”值为“all”，表示删除所有接口的集群统计信息。参数“cluster_id”的缺省值为“0”，表示删除所有虚拟集群接口上的集群统计信息。

cluster virtual arp interval [seconds]

这条命令用于设置主设备免费 ARP 广播包的时间间隔。

seconds 可以为 0，或 30 到 65535 之间的任意整数，单位为秒，默认值为 60 秒。0 表示设备只有在转换为主设备的那一瞬间才主动发送 ARP 包。

第6章 高可用性 (HA)

本章介绍 HA 功能的相关配置命令。



注意：HA 和集群功能是互斥的，二者的配置不能同时存在。

6.1 HA 节点

ha unit <unit_name> <ip_address> [port]

该命令用于为 HA 域添加一个 HA 节点。一个 HA 域中最多允许添加 32 个节点。为 HA 域添加了多个 HA 节点后，系统会自动在每两个 HA 节点之间建立主链路连接。

unit_name	该参数指定 HA 节点的名称，取值必须为最大长度不超过 8 个字节的字符串，区分大小写。每个节点的名称在 HA 域中应是唯一的。
ip_address	该参数指定 HA 节点的 IP 地址，即用于与其它节点进行主链路通信的 IP 地址。取值必须为 IPv4 或 IPv6 地址。同一个 HA 域中节点的 IP 地址必须同时为 IPv4 地址或 IPv6 地址。
port	可选。该参数指定 HA 节点用于与其它节点进行主链路通信的端口。 默认值为 65521。



注意：

- 配置本节点前，本节点的接口 IP 地址必须已经配置，否则 HA 域不能够识别本节点。
- HA 节点的端口不能与 SDNS 数据中心（通过“sdns dc”命令配置）的端口相同，否则 HA 节点的状态会出现异常。

no ha unit <unit_name>

该命令用于删除一个配置的 HA 节点。



注意：对于在“segment ip address”命令中被引用的 HA 节点，需要先通过“no segment ip address”命令解除引用后再删除该节点。

show ha unit

该命令用于显示所有配置的 HA 节点。

clear ha unit

该命令用于清除所有配置的 HA 节点。

6.2 HA 链路

ha link network secondary <unit_name> <link_id> <ip_address> [port]

该命令用于在一个 HA 节点上配置一条备用链路。两个 HA 节点之间可以配置最多 31 条备用链路。

unit_name	指该参数定 HA 节点的名称。
link_id	该参数指定备用链路的 ID。取值必须为 1 至 31 之间的整数。两个 HA 节点之间备用链路的 ID 是唯一的。
ip_address	该参数指定 HA 节点上用于备用链路通信的 IP 地址。取值必须为 IPv4 或 IPv6 地址。一条备用链路两端的 IP 地址必须同时使用 IPv4 或者 IPv6 地址。
port	可选。该参数指定了 HA 节点用于备用链路通信的端口。默认值为 65521。



注意：在两个 HA 节点之间建立一条备用链路，需要分别在两个节点上配置一个 ID 相同的备用链路。

例如，两个 HA 节点“u1”和“u2”的备用链路的 IP 地址分别为 192.168.1.1 和 192.168.1.2，如果为两个 HA 节点创建一条备用链路，分别在每个 HA 节点上做如下配置：

```
Demo(config)#ha link network secondary u1 1 192.168.1.1 65521
Demo(config)#ha link network secondary u2 1 192.168.1.2 65521
```

这样，HA 节点“u1”和“u2”之间就建立了 ID 为“1”的备用链路。

no ha link network secondary <unit_name> <link_id>

该命令用于删除与指定 HA 节点之间的备用链路。

clear ha link network secondary

该命令用于删除本节点上的所有备用链路配置。

ha link network {on|off}

该命令用于启用或禁用本节点与对端节点之间的网络链路，包括主链路和备用链路。默认情况下，系统启用网络链路。

ha link ffo {on|off}

该命令用于为 HA 功能启用或禁用 FFO 链路 (FFO link)。FFO 链路只能应用于 HA 域只包含两个节点的场景中。默认情况下，系统禁用 FFO 链路。



注意：FFO 链路必须配合网络链路一起使用，如果网络链路为禁用状态，FFO 链路和 HA 功能不生效。

ha link ffo heartbeat {on|off}

该命令用于为 HA 功能启用或禁用发送 FFO 链路心跳包的功能。只有在 HA 的 FFO 链路功能启用的情况下，该功能才能生效。该功能默认设置为禁用。

show ha link

该命令用于显示网络链路和 FFO 链路的开启状态以及备用链路的配置。

6.3 浮动 IP 分组和浮动 MAC

ha group id <group_id>

该命令用于在 HA 节点上定义一个浮动 IP 分组。每个节点上最多可定义 1024 个分组，包括系统浮动 IP 分组和分区浮动 IP 分组。

group_id 该参数指定浮动 IP 分组的 ID，取值必须为 0 至 1023 之间的整数。

no ha group id <group_id>

该命令用于删除本节点上指定的浮动 IP 分组。

show ha group id [group_id]

该命令用于显示本节点上指定浮动 IP 分组相关的所有配置。如不指定参数“group_id”，则显示所有浮动 IP 分组相关的配置。

clear ha group id

该命令用于清除本节点上全部的浮动 IP 分组。

ha group fip <group_id> <floating_ip> [interface_name] [floating_mac]

该命令用于为指定浮动 IP 分组配置一个浮动 IP 地址，将这一 IP 地址与指定的接口进行绑定，并配置浮动 MAC 功能。

group_id 该参数指定已存在的浮动 IP 分组的 ID。

floating_ip 该参数指定浮动 IP 地址，取值必须为 IPv4 或 IPv6 地址。

interface_name 可选，该参数指定绑定浮动 IP 地址的接口名称，取值必须为系统接口、聚合接口、MNET 接口、VLAN 接口的名称或者“auto”。“auto”表示将自动选择一个接口。

注意：不建议将该参数设置为主链路所在接口。当需要绑定浮动 MAC 地址时，该参数不能设置为聚合接口的成员接口。

默认值为“auto”。

当需要配置“floating_mac”参数，又需要设置该参数为默认值时，必须指定“auto”。当不需要配置

“floating_mac”参数时，可以不指定取值来表示使用默认值。

floating_mac

可选，该参数指定一个浮动 MAC 地址，格式为 xx:xx:xx:xx:xx:xx。该 MAC 地址不能为任何系统接口的 MAC 地址，不能和同一浮动 IP 分组其他系统接口或者聚合接口绑定的 MAC 地址相同，不能和其他浮动 IP 分组建定的 MAC 地址相同，也不能和网桥使用的系统接口 MAC 地址相同。

默认值为空，表示不使用浮动 MAC 功能。

no ha group fip <group_id> <floating_ip>

该命令用于删除指定浮动 IP 分组的一个浮动 IP 地址。

clear ha group fip <group_id>

该命令用于清除指定浮动 IP 分组的所有浮动 IP 地址。

ha group fiprange <group_id> <start_floating_ip> <end_floating_ip>
[interface_name] [floating_mac]

该命令用于为指定浮动 IP 分组配置一个浮动 IP 地址段，将这一 IP 地址段与指定的接口进行绑定，并配置浮动 MAC 功能。每个浮动 IP 地址段中最多包含 256 个 IP 地址。

group_id

该参数指定已存在的浮动 IP 分组的 ID。

start_floating_ip

该参数指定起始浮动 IP 地址段的起始 IP，取值必须为 IPv4 或 IPv6 地址。

end_floating_ip

该参数指定结束浮动 IP 地址段的结束 IP，取值必须为 IPv4 或 IPv6 地址。

interface_name

可选，该参数指定绑定浮动 IP 地址的接口名称，取值必须为系统接口、聚合接口、MNET 接口、VLAN 接口的名称或“auto”。“auto”表示系统将自动选择一个接口。注意：不建议将该参数设置为主链路所在接口。当需要绑定浮动 MAC 地址时，该参数不能设置为聚合接口的成员接口。

默认值为“auto”。

当需要配置“floating_mac”参数，又需要设置该参数为默认值时，必须指定“auto”。当不需要配置

“floating_mac”参数时，可以不指定取值来表示使用默认值。

floating_mac

可选，该参数指定一个浮动 MAC 地址，格式为 xx:xx:xx:xx:xx:xx。该 MAC 地址不能为任何系统接口的 MAC 地址，不能和同一浮动 IP 分组其他系统接口或者聚合接口绑定的 MAC 地址相同，不能和其他浮动 IP 分组绑定的 MAC 地址相同，也不能和网桥使用的系统接口 MAC 地址相同。

默认值为空，表示不使用浮动 MAC 功能。

设备上支持的浮动 IP 地址、浮动 IP 地址段、分区浮动 IP 分组和分区浮动 IP 地址段共有的最大数量取决于系统内存的大小，如下表所示。

表6 - 1 IP 地址段共有的最大数量

系统内存	最大数量
<= 8 GB	2000
16 GB	4000
24 GB	4000
>= 32 GB	8000



注意：浮动 IP 地址段中包含的所有 IP 地址（包括起始 IP 和结束 IP）不能配置为已通过命令“ip address”绑定到特定接口上的 IP 地址。

no ha group fiprange <group_id> <start_floating_ip> <end_floating_ip>

该命令用于删除指定浮动 IP 分组的一个浮动 IP 地址段。

clear ha group fiprange <group_id>

该命令用于清除指定浮动 IP 分组的所有浮动 IP 地址段。

ha floatmac {on|off}

该命令用于启用或禁用 HA 浮动 MAC 功能。浮动 MAC 功能是指当分组状态发生切换时，浮动 MAC 地址将浮动到当前分组状态为“Active”的节点上。这样，分组状态切换发生后，即使提供应用服务的设备发生了变化，但是由于使用的 MAC 地址没有发生改变，所以客户端感知不到提供服务的设备发生了变化。

默认情况下，系统禁用该功能。在启用浮动 MAC 功能之前，必须先执行“ha off”命令禁用 HA 功能。

ha arp interval <interval>

该命令用于为 HA 节点设置发送 ARP 广播包的时间间隔。

interval 该参数指定 HA 节点发送 ARP 广播包的时间间隔, 单位为秒。取值必须为 0 或 30 至 65535 之间的整数, 如果该参数的取值为 0, 则表示只在本地 HA 节点的浮动 IP 分组状态切换为 “Active” 时才发送 ARP 广播包。

默认值为 30。

ha group priority <unit_name|ssi> <group_id> <priority>

该命令用于配置指定浮动 IP 分组在指定 HA 节点上的优先级。

unit_name|ssi 该参数指定 HA 节点的名称, 取值必须为本地 HA 节点或者对端 HA 节点的名称, 表示浮动 IP 分组的优先级设置将用于 HA 功能。

参数“ssi”仅用于 SSI 功能, 具体请参见单系统映像 (SSI) 里关于该命令的介绍。

group_id 该参数指定浮动 IP 分组的 ID。

priority 该参数指定浮动 IP 分组在指定节点上的优先级, 取值必须为 0 至 255 之间的整数。取值越大, 优先级越高。



注意: 如果不为浮动 IP 分组配置在指定 HA 节点上的优先级, 或者删除其优先级配置, 则该分组无法在该 HA 节点上生效 (执行 “show ha status” 命令后该分组在指定 HA 节点上的状态始终显示为 “-”)。

no ha group priority <unit_name|ssi> <group_id>

该命令用于删除指定浮动 IP 分组在指定节点上的优先级配置。

ha group preempt {on|off} <group_id>

该命令用于为指定浮动 IP 分组启用或禁用抢占模式。抢占模式能够确保浮动 IP 分组在优先级最高的可用节点上的状态始终为 “Active”。默认情况下, 系统禁用浮动 IP 分组的抢占模式。

group_id 该参数指定已存在的浮动 IP 分组的 ID, 取值必须为 0 至 1024 之间的整数。“1024” 表示为所有浮动 IP 分组启用或禁用抢占模式。



注意: 为了保证抢占模式对指定的浮动 IP 分组生效, 请确保在所有启用该分组的节点上已启用抢占模式。

ha group {enable|disable} <group_id>

该命令用于在本节点上启用或禁用指定的浮动 IP 分组。默认情况下，系统禁用所有浮动 IP 分组。当一个浮动 IP 分组在多个 HA 节点上被启用，仅由浮动 IP 分组状态为“Active”的 HA 节点提供该浮动 IP 分组所对应的应用服务。浮动 IP 分组与应用服务通过“ha group fip”或“ha group fiprange”命令的配置关联起来。

group_id 该参数指定已存在的浮动 IP 分组的 ID，取值必须为 0 至 1024 之间的整数。“1024”表示在本地 HA 节点上启用或禁用所有的浮动 IP 分组。

ha heartbeat [interval] [down_check_times]

该命令用于设置 HA 节点向 HA 域中其它 HA 节点发送心跳包的间隔。HA 节点会按照设置的发送间隔，通过主链路、备用链路和 FFO 链路向其它 HA 节点发送心跳包。如果连续多次（由参数“down_check_times”确定）都没从这些链路收到对端 HA 节点的心跳响应，则认为该对端 HA 节点的状态为“Down”。否则，认为该对端 HA 节点的状态为“Up”。

interval 可选。该参数指定 HA 节点发送心跳包的时间间隔，单位为毫秒。取值必须为 100 至 10,000 之间的整数。

默认值为 1000。

down_check_times 可选。该参数指定连续没有收到对端 HA 节点的心跳响应的次数。取值必须为 3 至 1000 之间的整数。

默认值为 15。

当对端节点发生故障时，对端节点在某一浮动 IP 分组中的状态将从“Active”切换到“Init”时。同时，在该分组中最高优先级的可用 HA 节点的状态将会从“Standby”切换到“Active”，开始提供该分组对应的应用服务。



注意：请确保 HA 节点上的“ha heartbeat”配置相同；否则，可能会发生 HA 状态反复切换。

ha group switch <unit_name> <group_id>

该命令用于将指定的浮动 IP 分组切换到指定的 HA 节点。切换后，该分组在当前节点上的状态会从主用变为备用，在目标节点上的状态将从备用变为主用。该命令只对禁用了抢占功能（通过“ha group preempt”命令配置）的分组生效。

unit_name 该参数指定已存在的 HA 节点名称。

group_id 该参数指定已存在的浮动 IP 分组的 ID，取值为 1024 时将切换所有处于主用状态的浮动 IP 分组。

注意：如果该参数指定的浮动 IP 分组配置的浮动 IP 地址的数量较多时,通过该命令将指定的浮动 IP 分组切换到指定的 HA 节点时,可能会切换失败。推荐不要为一个浮动 IP 分组配置过多的浮动 IP 地址。如果浮动 IP 地址数量较多,推荐管理员将其配置到多个浮动 IP 分组。

6.4 HA 健康检查和失效切换

HA 功能支持以下健康检查类型：

- 系统健康检查：设备支持直接使用系统健康检查作为 HA 节点的失效切换条件，具体请参考第二章内系统健康检查的配置命令。
- 预定义健康检查：HA 功能预定义了网络接口健康检查条件（PORT_1~PORT_32）。默认情况下，当发生网络接口故障时，HA 节点会执行 Group_Failover 切换。管理员可以根据需要通过“**ha decision rule**”命令修改基于网络接口健康检查条件的失效切换动作。当浮动 IP 地址或浮动 IP 地址段绑定的系统接口出现故障时，该接口对应的预定义失效切换规则会在向对端节点发送心跳包的时间间隔（即 1000~10,000 毫秒）内生效。
- 自定义健康检查：管理员可以根据需要自定义健康检查脚本，然后通过 SCP 或 TFTP 导入到设备中，配置命令请参考第二章“系统健康检查”小节。

show monitor condition [unit_name]

该命令用于显示指定 HA 节点的健康状态。

unit_name 该参数指定 HA 节点的名称。如不指定该参数，则显示所有 HA 节点的健康状态。



注意：该命令不显示状态为“Init”的健康检查条件。

ha decision rule <condition_name> <action_name> <group_id>

该命令用于为指定浮动 IP 分组配置一条失效切换规则，规定当指定的健康检查条件为由 Up 状态变为 Down 时所执行失效切换动作。同一个健康检查条件最多可以用于 1024 个失效切换规则的配置中。

condition_name 该参数指定健康检查条件的名称，取值必须为真实健康检查条件或者 vcondition 的名称。系统支持如下名称：

- （预定义）PORT_1~PORT_32：端口健康检查条件
- GATEWAY_1~GATEWAY_32：网关健康检查条件
- CPU_UTIL：CPU 使用率健康检查条件

- CPU_TEMP: CPU 温度健康检查条件
- SSL_CARD: SSL 加速卡健康检查条件
- SSL_AE_UTIL: SSL 加速卡 AE 内核使用率健康检查条件
- SSL_SE_UTIL: SSL 加速卡 SE 内核使用率健康检查条件
- SYSTEM_MEM_UTIL: 系统内存使用率健康检查条件
- NETWORK_MEM_UTIL: 网络内存使用率健康检查条件
- SWAP_MEM_UTIL: SWAP 内存使用率健康检查条件
- CONN_MEM_UTIL: 连接内存使用率健康检查条件
- SYSTEM_DISK_UTIL: 系统硬盘分区使用率健康检查条件
- DATA_DISK_UTIL: 数据硬盘分区使用率健康检查条件
- BOND_1~BOND_8: 聚合接口状态健康检查条件
- SCRIPT: 自定义脚本健康检查条件
- 自定义的健康检查条件组 (vcondition) 的名称

action_name 该参数指定当健康检查条件为 Down 时, 要执行的切换动作。取值必须为 “Unit_Failover”, “Group_Failover” 或 “Reboot”。

group_id 该参数指定切换规则生效的浮动 IP 分组的 ID。只有当 “action_name” 参数设置为 “Group_Failover” 时, 该参数才可用。



注意:

- 对于 HA 域中为同一浮动 IP 分组提供失效切换支持的各节点, 需要为该浮动 IP 分组配置相同的失效切换规则, 包括切换规则中健康检查条件的名称。
- 对于 HA 域中为 “Unit_Failover” 提供失效切换支持的各节点, 需要为 “Unit_Failover” 配置相同的失效切换规则, 包括切换规则中健康检查条件的名称。
- 系统预定义了失效切换规则, 管理员可以通过执行命令 “show ha decision” 查看这些预定义规则。管理员可以通过执行命令 “ha decision rule” 修改预定义规则中

的切换动作。当浮动 IP 地址或浮动 IP 地址段绑定的系统接口出现故障时，该接口对应的预定义失效切换规则会在向对端节点发送心跳包的时间间隔（即 1000~10,000 毫秒）内生效。

- 为了实现根据接口状态的灵活失效切换，可以将网络接口健康检查条件（PORT_1~PORT_32）添加进健康检查条件组，并使用健康检查条件组作为切换条件。例如，通过把两个网络接口健康检查条件添加进一个健康检查条件组，并把两个预定义条件之间的关系配置为“OR”，用户可以定义如下切换规则：在两个接口同时故障时才执行分组切换（Group_Failover）。网络接口健康检查条件添加进健康检查条件组后，对应的预定义切换规则将失效。

no ha decision rule <condition_name> <action_name> <group_id>

该命令用于删除指定浮动 IP 分组的一条失效切换规则。



注意：当参数“condition_name”设置为 PORT_1~PORT_32 时，系统将把切换动作重置为默认值“Group_Failover”。

clear ha decision rule

该命令用于清除所有浮动 IP 分组的失效切换规则。



注意：执行该命令不会删除系统预定义的失效切换规则，而是将其切换动作重置为默认值“Group_Failover”。

show ha decision

该命令用于显示本地 HA 节点上所有浮动 IP 分组的失效切换规则，包括预定义规则和自定义规则。

例如：

Demo(config)#show ha decision			
ID	Condition_Name	Action_Name	Group_ID
0	PORT_1	Group_Failover	-
1	PORT_2	Group_Failover	-
2	PORT_3	Group_Failover	-
3	PORT_4	Group_Failover	-
4	CPU_UTIL	Unit_Failover	-

show ha failover [group_id]

该命令用于显示指定浮动 IP 分组的失效切换日志。如不指定参数“group_id”，则显示所有浮动 IP 分组的失效切换日志。

6.5 对端节点 HA 分组状态检查

ha checkpeer {on|off}

该命令用于启用或禁用对端节点 HA 分组状态检查功能。

启用该功能后，在处于活动状态的 HA 节点上，当检查健康的结果为 Down 时，该节点会检查对端 HA 节点上的 HA 分组的状态，如果对端节点上的 HA 分组也处于 Down 的状态，该 HA 节点会继续保持活动状态，而不是直接切换为 Down。

禁用该功能后，处于活动状态的 HA 节点在健康检查结果为 Down 时，不会检查对端 HA 节点上的 HA 分组的状态，而是直接切换为 Down。

该功能的默认设置为启用。

clear ha checkpeer

该命令用于将对端节点 HA 分组状态检查功能恢复为默认设置。执行该命令后，该功能将处于启用状态。

6.6 配置同步

ha synconfig bootup {on|off}

该命令用于启用或禁用 HA 功能的启动时配置同步功能，将对端 HA 节点的配置信息同步到本地 HA 节点，该功能默认设置为禁用。

该功能不会同步的配置项列表如下：

```
show config consistency
ip address
ip route
ip dhcp
ssh ip
bond
hostname
mnet
vlan
access
webui ip
webwall
ip redundant
cluster virtual priority, with "synconfig_peer_name" being "primary"
llb dns local
sdns listener
sdns member local
```

```
sdns dps localdetector
interface
no interface
clear interface
interface name
interface speed
interface mtu
interface mac
interface management
ha ssf peer
user
admin mode separation on
admin mode separation off
admin test factor
no admin test factor
```



注意：

- 该功能通过 FFO 链路同步 HA 节点和链路相关配置，通过主链路同步 “**write memory**” 保存的配置。
- 如果通过命令 “**synconfig secure on**” 启用了配置同步的安全模式，启用该功能前，需先使用 “**synconfig peer**” 在本地和对端 HA 节点上分别配置同步节点，指定的同步节点名称必须和 HA 节点名称相同。
- 启用该功能后，本地节点上的所有 SLB 统计信息将被系统清除。
- 在启动时配置同步过程中，不允许手动添加、修改或者删除配置。
- 在 HA 功能开启的环境下执行 “**synconfig from**”、“**synconfig to**”、“**synconfig rollback peer**”、“**synconfig rollback local**”、“**config memory**”和 “**config file**” 中的任何一个命令前，必须确认启动时配置同步功能为禁用状态，否则可能出现配置异常。

ha synconfig runtime {on|off}

该命令用于启用或禁用 HA 功能的运行时配置同步功能，该功能默认是禁用的。只有在本地对端 HA 节点上都启用该功能时，才能在两个 HA 节点之间进行实时的配置同步。对于不需要同步的配置项，系统通过一个黑名单管理。启用运行时配置同步功能后，除黑名单以外的所有配置项都会被同步。下表列出了黑名单里的所有配置项：

```
show
show config consistency
ip address
no ip address
ip route
no ip route
ssh ip
```

```
no ssh ip
bond
no bond
clear bond
hostname
no hostname
mnet
no mnet
clear mnet
vlan
no vlan
clear vlan
webui ip
clear webui ip
xmlrpc ip
clear xmlrpc ip
webwall
cluster virtual priority
sdns listener
no sdns listener
clear sdns listener
sdns dps localdetector
sdns dnssec keygen
interface
no interface
clear interface
ha on
ha off
ha unit
no ha unit
clear ha unit
ha synconfig runtime on
ha synconfig runtime off
ha group enable
ha group disable
ha group switch
ha ssf peer
no ha ssf peer
clear ha ssf peer
ha link ffo
ha link network on
ha link network off
```

clear ha all
write net
write all
write file
log alert
system serialnumber
system fallback
system update
system license
system portmap
no system portmap
system rescue
ntp on
clear http import error
clear http error
qos enable
role
clear role name
no role user
clear role user
user
no user
clear users
passwd
system tune route numaaccel on
clear system resource
config
no config
health import request
health import response
no health import request
no health import response
clear health import request
clear health import response
no http error
synconfig
no synconfig
quit
exit
engineering
config terminal
enable

```
disable
pager
no pager
debug
no debug
ssl export key
ipregion table export
crontab export
ping
no segment name
clear segment name
ip dhcp
accessgroup
no accessgroup
clear accessgroup
accesslist
no accesslist
clear accesslist
slb sip callnum list export
sdns dc
no sdns dc
show sdns dc name

show sdns dc status

clear sdns dc
ssl restore certificate
sdns config
no sdns config
clear sdns config
sdns dps write proximity
admin mode separation on
admin mode separation off
admin test factor
no admin test factor
```

**注意：**

- HA 运行时配置同步功能只对系统模式下的配置项生效，对分区模式内的配置项不生效。
- 通过 HA 运行时配置同步功能同步配置到对端节点时，对端节点不会执行 SDNS 运行时配置同步命令。
- 在同时配置 HA 功能与 SDNS 功能的情景下，备机上执行命令，主机不会通过 SDNS 运行时配置同步功能将配置同步到其他 SDNS 设备上。

- 不建议两台 SDNS 主机之间配置 HA 功能。

show ha synconfig

该命令用于显示启动时配置同步和运行时配置同步功能的启用状态。

show ha status [group|domain|link|login]

该命令用于显示浮动 IP 分组状态、HA 节点状态、链路状态、配置同步状态和 HA 本地节点的登录状态信息。

group|domain|link|login 可选，该参数指定需要显示的具体状态信息，取值必须为：

- group: 显示浮动 IP 分组状态。
- domain: 显示所有 HA 节点的状态。
- link: 显示主用和备用链路的状态。
- login: 显示 HA 本地节点的登录状态和配置同步状态。

默认值为“group”。

6.7 SSF

ha ssf peer <peer_ip>

该命令用于为 SSF 功能设置对端节点。

peer_ip 该参数指定对端节点的 IP 地址。

no ha ssf peer <peer_ip>

该命令用于删除指定的 SSF 对端节点。

clear ha ssf peer

该命令用于清除所有的 SSF 对端节点。

ha ssf {on|off} [virtual_service]

该命令用于为指定的虚拟服务启用或禁用 SSF (Session Stateful Failover, 连接同步) 功能。默认情况下，系统为所有单个虚拟服务启用 SSF 功能，但是禁用全局 SSF 功能。如果要使 SSF 功能对单个的虚拟服务生效，包括在分区模式下启用 SSF 功能时，必须先启用全局 SSF 功能。

virtual_service 可选，该参数指定虚拟服务名称。SSF 功能只对 TCP、UDP、FTP、IP、TCPS、HTTP 和 HTTPS 类型的虚拟服

务生效。

如不指定该参数，则启用或禁用全局 SSF 功能。

在分区模式下配置该命令时，该参数为必选。



注意：

- SSF 功能支持最多三个 HA 节点。
- 启用 SSF 功能前需确认 SLB 和 NAT 虚拟 IP 地址已经设置为浮动 IP 地址，否则可能发生意外错误。
- 如果为虚拟服务配置了 DoH 策略，则 SSF 功能对该虚拟服务不生效。如果要使用 SSF 功能，请先删除为其配置的 DoH 策略。
- 启用了 SSF 功能的 TCPS 和 HTTPS 类型的虚拟服务不支持 SM2 和 TLS1.3 协议。
- 启用了 SSF 功能的 TCPS 和 HTTPS 类型的虚拟服务不支持 SSL 后台主机。
- SSF 功能目前只支持局域网部署场景。
- SSF 链路上接口的 MTU 应大于等于业务链路接口 MTU 值与 500 的和。
- SSF 链路的带宽应大于业务链路的带宽。
- 为保证 SSF 功能正常工作，主备设备需满足如下条件：
 - 主备设备的 SLB 配置应相同且配置顺序一致
 - 主备设备的时间差应小于 60 秒。
 - 主备设备上后台服务的健康检查状态一致。
- 启用了 SSF 功能的 HTTP 和 HTTPS 类型的虚拟服务不支持 Via 头部插入、压缩、缓存、HTTP/2 和 ePolicy 功能。
- 启用了 SSF 功能的虚拟服务不支持 TCP 选择性确认 (SACK) 功能。
- 同时启用 HA 功能和 SSF 功能才会进行连接同步。

假设两个 HA 节点的 IP 地址分别为 198.162.1.1 和 198.162.1.2。如果要为两个 HA 节点启用 SSF 功能，需要如下配置：

HA 节点 1 上：

```
AN1(config)#ha ssf peer 192.168.1.2
AN1(config)#ha ssf on
```

HA 节点 2 上：

```
AN2(config)#ha ssf peer 192.168.1.1
AN2(config)#ha ssf on
```


ha ssf {on|off} nat

该命令用于为 NAT 启用或禁用 SSF 功能，该功能默认是禁用的。

当该功能启用并且配置了“**nat static**”命令时，系统支持对经过“**nat static**”规则转换的出向流量进行失效切换，不支持对其转换的入向流量进行失效切换。

show ha ssf session

该命令用于显示所有 SSF 相关的会话信息。

show ha ssf settings

该命令用于显示所有 SSF 相关的设置。

例如：

```
Demo(config)#show ha ssf settings
ha ssf peer 192.168.1.1
ha ssf on
ha ssf off nat
ha ssf on v2
ha ssf on vsudp
```

show statistics ssf

该命令用于显示所有 SSF 相关的统计信息。

clear statistics ssf

该命令用于清除所有 SSF 相关的统计信息。

ha ssf timeout <timeout>

该命令用于设置 SSF 会话超时时间。当没有配置该命令时，默认的 SSF 会话超时时间为 300 秒。

timeout 该参数指定超时时间，单位为秒。其值范围在 60 到 7200 之间。

no ha ssf timeout

该命令用于将 SSF 会话超时时间设置恢复为默认值。

6.8 HA 一致性检查

ha consistency {on|off}

该命令用于启用或禁用 HA 一致性检查功能。启用该功能后，当管理员执行“**ha on**”命令时，HA 节点之间将对软件版本、设备型号和授权特性的一致性进行检查，如果 HA 节点之间的软件版本、设备型号或授权特性中的任何一项不一致，

HA 功能将无法启用。检查软件版本的一致性时，只要版本号的前两位相同，即认为版本号一致。禁用该功能后，当管理员执行“**ha on**”命令时，HA 节点之间将不进行设备型号和授权特性的一致性检查，只要软件版本前两位相同，HA 功能即可生效。

该功能仅在 SSF 功能和运行时配置同步功能禁用时才能禁用，默认设置为启用。当该功能为禁用状态时，不能启用 SSF 功能和运行时配置同步功能。该功能在所有 HA 节点上的配置状态必须一致。

clear ha consistency

该命令用于将 HA 一致性检查功能恢复为默认设置。执行该命令后，HA 一致性检查功能将被启用。

6.9 HA 日志

ha log {on|off}

该命令用于启用或禁用 HA 的日志功能。默认情况下，系统禁用该功能。若启用了 HA 功能，则日志功能也相应被启用；若禁用了 HA 功能，则日志功能也将被禁用。

ha log level <level>

该命令用于设置系统生成的 HA 日志的级别。

level 该参数指定 HA 日志的级别。设备上有八个 HA 日志级别，分别是：emerg、alert、crit、err、warning、notice、info 和 debug。HA 日志级别默认为 info。一旦设定了 HA 日志级别，低于这个级别的消息将被忽略。

show ha log [line_number]

该命令用于显示 HA 相关的日志信息。

line_number 可选。该参数指定显示 HA 日志的行数。
默认值为 100，表示系统将显示最新产生的 100 行 HA 日志信息。

clear ha log

该命令用于清除所有 HA 相关的日志信息。

6.10 通用配置

ha on

该命令用于启用 HA 功能。

**注意：**

- HA 功能和集群功能不能同时启用。
- HA 使用的 IP 地址池必须在启用 HA 功能前配置。如果在启用 HA 功能后配置 IP 地址池，需要重启 HA 功能。

ha off [force]

该命令用于禁用 HA 功能，默认情况下 HA 功能是被禁用的。

force 该参数用于在节点加入 HA 域的过程中，当节点 HA 状态发生异常时，强制关闭 HA 功能。

show ha config

该命令用于显示 HA 功能相关的所有配置。

例如：

```
Demo(config)#show ha config
ha off
ha log off
ha log level info
ha arp interval 30
ha link ffo off
ha link network on
show ha ssf settings
ha checkpeer on
ha synconfig bootup on
ha synconfig runtime off
ha heartbeat 1000 3
ha ssf off
ha ssf off nat
ha ssf on vs1
```

clear ha all

该命令用于清除 HA 功能相关的所有配置。

show statistics ha

该命令用于显示所有 HA 相关的统计数据，包括 HA 事件统计、HA 分组状态统计和失效切换统计。

clear statistics ha

该命令用于清除所有 HA 相关的统计数据。

第7章 单系统映像 (SSI)

SSI 功能通过使多台设备构成同一 SSI 域来共同提供同一虚拟服务，从而大大提高性能。由于 SSI 功能构建于 HA 功能的基本框架，SSI 功能复用 HA 功能的命令。

ha ssi on/off

启用/禁用单系统映像功能。

ha group port <group_id> <bond_ifname|l2_vip_interface> [system_ifname]

该命令用于将聚合接口中的系统接口或二层虚拟服务关联的系统接口加入到 HA 浮动 IP 分组中。当 HA 浮动 IP 分组的状态为“Active”时，该组内的聚合接口的系统接口或二层虚拟服务关联的系统接口为激活状态，可以转发数据包；当 HA 浮动 IP 分组的状态为“Init”或者“Standby”时，该组内的聚合接口的系统接口或二层虚拟服务关联的系统接口为关闭状态，不能转发数据包。

group_id	该参数指定已存在的浮动 IP 分组的 ID。
bond_ifname l2_vip_interface	该参数指定聚合接口或二层虚拟服务关联的系统接口的名称。默认的聚合接口的名称为 bond1、bond2、bond3、bond4……。 (管理员可以通过“ bond name ”命令来自定义聚合接口名称。)
system_ifname	可选，该参数指定聚合接口中系统接口的名称，默认为 port1、port2、port3、port4……。 (管理员可以通过“ interface name ”命令来自定义系统接口的名称。)

注意：当参数“bond_ifname|l2_vip_interface”设置为聚合接口的名称时，必须配置该参数。

no ha group port <group_id> <bond_ifname> <system_ifname>

该命令用于将聚合链路接口的子接口从 HA 浮动分组中删除。

clear ha group port <group_id>

该命令用于清除指定浮动 IP 分组与所有接口的绑定关系。

ha group backup <group_id1> <group_id2>

将同一个节点上两个不同的 HA 分组进行相互备份，从而实现交换机失效切换。

ha group priority <unit_name|ssi> <group_id> <priority>

该命令用于配置或修改指定浮动 IP 分组在 SSI 域中所有节点上的优先级。如果不配置浮动 IP 分组在 SSI 域中的优先级，该浮动 IP 分组不生效。

unit_name ssi	该参数指定 SSI 域，取值必须为“ssi”，表示浮动 IP 分组的优先级配置将用于 SSI 功能。 参数“unit_name”仅用于 HA 功能，具体请参见高可用性（HA）里对该命令的介绍。
group_id	该参数指定浮动 IP 分组的 ID。
priority	该参数指定浮动 IP 分组在指定节点上的优先级。取值必须为 0 至 255 之间的整数。取值越大，优先级越高。

第8章 分区管理

8.1 系统模式

segment name <segment_name>

该命令用于创建一个分区并指定分区的名称。

segment_name 该参数指定分区的名称，取值必须为长度不大于 128 个字节的字符串。

支持“a~z”、“A~Z”、“0~9”、“@”、“-”、“_”和“!”。不支持“@@”，也不能以“@”开头和结尾。

取值由纯数字组成或者包含特殊字符时，必须置于双引号内。



注意：在分区内配置 SSL 功能时，分区名称的长度、虚拟主机或后台主机名称的长度和相应的 SNI 域名长度的总和不能超过 220 个字符。

设备上支持的“**segment name**”分区的最大数量取决于系统内存的大小，如下表所示。

表8 - 1 分区最大数量

系统内存	分区最大数量
1 GB ≤ 系统内存 ≤ 24 GB	8
系统内存 = 32 GB	64
64 GB ≤ 系统内存 ≤ 384 GB	1024

no segment name <segment_name>

该命令用于删除指定的分区以及该分区相关的所有配置。

show segment name [segment_user]

该命令用于显示指定的分区管理员账户关联的分区。如不指定参数“segment_user”，系统将按照分区字典顺序排列显示所有已创建的分区。

分区下支持：

show segment name

该命令用于按照分区字典顺序排列显示当前分区管理员账户关联的分区。

clear segment name

该命令用于清除所有已创建的分区以及相关的所有配置。

segment user <segment_user> <segment_name> <password> [level]

该命令用于创建一个分区管理员账户，并指定分区管理员账户的名称、密码和权限级别，同时将该分区管理员账户与指定的分区绑定。系统支持最多创建 2048 个分区管理员账户。

一个分区可以绑定多个分区管理员账户。通过该命令，一个分区管理员账户只能和一个分区绑定，如果一个分区管理员账户需要和多个分区绑定，请执行命令“**segment access**”。

对于已存在的分区管理员账户，如需修改权限级别，需删除账号后重新创建。

segment_user 该参数指定分区管理员账户的名称，取值必须为不大于 32 字节的字符串。

支持字母和数字，区分大小写，不支持特殊字符，但是允许“\$”出现在参数值的结尾。

当“\$”出现在取值的结尾时或取值由纯数字组成时，必须置于双引号内。

segment_name 该参数指定已存在的分区名称。取值支持配置为空，表示不指定分区，此时参数“level”可配置，但是不生效。当只需配置分区管理员账户，但是不绑定分区时，可以配置取值为空。

password 该参数指定密码。

在强制密码模式关闭时，取值必须为 1 至 116 个字节的字符串，区分大小写。当参数取值包含数字或特殊字符时，必须置于双引号内。

在强制密码模式开启时，取值必须满足强制密码模式的密码复杂度要求（参考“**passwd forcemode**”命令）。

level 可选。该参数指定分区管理员账户的权限级别。取值必须为：

- **enable**: 拥有该权限级别的分区管理员账户可以运行分区内所有“enable”级别下的 CLI 命令。
- **config**: 拥有该权限级别的分区管理员账户可以运行分区内所有的全部 CLI 配置命令。
- **api**: 拥有该权限级别的分区管理员账户可以访问分区内基于 API 的 Web 服务，但是不能运行任何 CLI 命令。

默认值为“config”。

segment access <segment_user> <segment_name> [level]

该命令用于绑定指定的分区管理员账户和指定的分区，并指定该分区管理员账户对分区的权限级别。一个分区管理员账户可以和不同的分区进行绑定，一个分区也可以和不同的分区管理员账户进行绑定。具体支持的绑定数量和分区管理员账户以及分区个数一致。

segment_user	该参数指定需要绑定的已存在的分区管理员账户的用户名。
segment_name	该参数指定需要绑定的已存在的分区的名称。
level	可选。该参数指定分区管理员账户的权限级别。取值必须为： • enable: 拥有该权限级别的分区管理员账户可以运行分区内所有“enable”级别下的 CLI 命令。 • config: 拥有该权限级别的分区管理员账户可以运行分区内所有的全部 CLI 配置命令。 • api: 拥有该权限级别的分区管理员账户可以访问分区内基于 API 的 Web 服务，但是不能运行任何 CLI 命令。 默认值为“config”。

no segment access <segment_user> <segment_name>

该命令用于将指定的分区管理员账户和指定的分区进行解绑。

show segment access [segment_user]

该命令用于显示指定分区管理员账户绑定的所有分区。如果不指定“segment_user”，则显示所有分区管理员账户绑定的所有分区。

clear segment access [segment_user]

该命令用于清除指定分区管理员账户绑定的所有分区。如果不指定“segment_user”，则清除所有分区管理员账户绑定的所有分区。

segment passwd <segment_user> <password>

该命令用于修改指定分区管理员账户的密码。

segment_user	该参数指定已存在的分区管理员账户的名称。
password	该参数指定新密码。 在强制密码模式关闭时，取值必须为 1 至 116 个字节的字符串，区分大小写。当参数取值包含数字或特殊字符

时，必须置于双引号内。

在强制密码模式开启时，取值必须满足强制密码模式的密码复杂度要求（参考“**passwd forcemode**”命令）。

no segment user <segment_user>

该命令用于删除指定的分区管理员账户。

show segment user [segment_name]

该命令用于显示指定分区的所有管理员账户配置。如不指定参数“segment_name”，则显示所有的分区管理员账户配置。

clear segment users [segment_name]

该命令用于清除指定分区的所有管理员账户。如不指定参数“segment_name”，则清除所有的分区管理员账户。

segment interface <segment_name> {system_ifname|bond_ifname|vlan_ifname}

该命令用于将指定的系统接口、聚合接口或 VLAN 接口加入指定的分区。

segment_name	该参数指定已存在的分区名称。
system_ifname	该参数指定系统接口的名称,可以通过“ interface name ”命令来自定义系统接口名称。 默认名称为 port1、port2、port3、port4.....。
bond_ifname	该参数指定聚合接口的名称。 默认名称为 bond1、bond2、bond3、bond4.....。
vlan_ifname	该参数指定 VLAN 接口的名称，可以通过“ segment vlan ”命令来自定义 VLAN 接口名称。



注意：每个分区都只能使用已经添加到该分区的接口，如果在某些特殊情况下需要为一个分区使用不属于该分区的接口，请联系公司技术支持。

no segment interface <segment_name> {system_ifname|bond_ifname|vlan_ifname}

该命令用于删除指定分区的一条接口配置。

show segment interface [segment_name]

该命令用于显示指定分区的所有接口配置。如不指定参数“segment_name”，则显示所有分区的接口配置。

clear segment interface [*segment_name*]

该命令用于从清除指定分区的所有接口配置。如不指定参数“segment_name”，则清除所有分区的接口配置。

segment ip address {*system_ifname*|*bond_ifname*|*vlan_ifname*|*mnet_ifname*}
<*segment_ip*> {*netmask*|*prefix*} [*nat_mode*] [*unit_name*]

该命令用于设置分区中系统接口、聚合接口、VLAN 接口或 MNET 接口的 IP 地址和子网掩码或前缀长度，并为接口配置地址转换规则。

<i>system_ifname</i>	该参数指定系统接口的名称。
<i>bond_ifname</i>	该参数指定聚合接口的名称。
<i>vlan_ifname</i>	该参数指定 VLAN 接口的名称。
<i>mnet_ifname</i>	该参数指定 MNET 接口的名称。
<i>segment_ip</i>	该参数指定需要转换的 IP 地址，可以为 IPv4 或 IPv6 地址。
<i>netmask</i> <i>prefix</i>	该参数指定需要转换的 IP 地址对应的子网掩码或前缀长度。 “mask”用于配置 IPv4 地址对应的子网掩码，取值可以为点分地址格式或 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，取值为 0 到 128 之间的整数。
<i>nat_mod</i>	可选，该参数指定 NAT 转换分区 IP 地址的模式。取值必须为： “internal_ip”：在该模式下，系统将分区 IP 地址静态转换为该 IP 地址。当参数“segment_ip”和后台服务 IP 地址不在同一网段时，需要为后台服务配置 NAT 地址转换（即“segment nat”）。 注意：此时参数取值不可以为以下网段的 IP： “7.0.0.0/8”、“8.0.0.0/8”、“9.0.0.0/8”、“1237::/64”、“1238::/64”、“1239::/64”。 “auto”：在该模式下，系统自动将分区 IP 地址转换为从“system tune segment iprange”命令配置的 IP 网段中选择的 IP 地址。并且，系统将自动为后台服务生成一条地址转换规则。 “空”：系统不进行 NAT 地址转换。

默认值为空。

unit_name

可选，该参数指定 HA 节点名称。

如不指定该参数，则表示为本地节点配置该命令。



注意：

- 在 HA 环境下，执行配置同步操作前，请先确认该命令配置了“unit_name”选项，否则该命令的配置不会被同步。
- 在 HA 环境下，同一个 MNET 接口中的不同 HA 节点的 internal IP 必须相同。其他情况下，internal IP 不能相同。
- 在分区内，当参数“internal_ip|auto”取值为 auto 时，须在分区内先配置后台服务，后配置静态路由，删除后台服务配置时，须先删除对应的静态路由配置。
- 指定参数“internal_ip|auto”时，全局配置 SLB 中的虚拟服务 IP 不能与 NAT 转换后的地址处在同一网段。未指定参数“internal_ip|auto”时，全局配置 SLB 中的虚拟服务 IP 不能与分区 IP 地址处在同一网段。
- 在分区模式下配置 SLB 和 SSL 相关功能前，需先在系统模式下配置“segment ip address”等相关网络功能。
- 在分区内，当参数“internal_ip|auto”取值为 auto，且后台服务的地址为域名时，需要为该后台服务手动配置 NAT 转换规则（通过命令“segment nat”）。
- 在实际使用中，不允许将“internal_ip”配置为系统自动分配的 IP 网段。
- 在分区内，当配置的后台服务 IP 地址与分区 IP 地址不在同一网段时，需为该后台服务添加静态路由，且静态路由目的网络为后台服务 IP 地址，子网掩码为 32 位（IPv4）或 128 位（IPv6）。
- 如果为后台服务配置了附加健康检查，且附加健康的目的 IP 地址与后台服务的 IP 地址不在同一网段，需要为附加健康检查的目的 IP 地址配置 NAT 转换规则（通过命令“segment nat”）。

no segment ip address <segment_interface_name> [ip_type] [auto]
[unit_name]

该命令用于删除指定的分区接口的 IP 地址设置。

segment_interface_name 该参数指定分区接口的名称。

ip_type 该参数指定接口的 IP 地址类型：

- 4：表示 IPv4 地址。
- 6：表示 IPv6 地址。

默认值为 4。

auto 可选，该参数取值为“auto”时，系统将删除在 NAT 转换时自动分配的 IP 网段。

unit_name 可选，该参数指定节点名称。

如不指定该参数，则表示为本地节点配置该命令。

show segment ip address

该命令用于显示所有的分区接口 IP 地址设置。

clear segment ip address

该命令用于清除所有的分区接口 IP 地址配置。

segment mnet {system_ifname|bond_ifname|vlan_ifname}
<mnet_interface_name>

该命令用于为分区中指定的系统接口、聚合接口或 VLAN 接口创建 MNET（多网段）接口。系统最多支持配置 4126 个 MNET 接口。

system_ifname	该参数指定系统接口名称，默认为 port1、port2、port3、port4……。 （管理员可以通过“ interface name ”命令来自定义系统接口名称。）
bond_ifname	该参数指定聚合接口的名称，默认的聚合接口名称为 bond1、bond2、bond3、bond4……。 （管理员可以通过“ bond name ”命令来自定义聚合接口名称。）
vlan_ifname	该参数指定 VLAN 接口名称。（管理员可以通过“ vlan ”命令来创建 VLAN 接口。）
mnet_interface_name	该参数指定 MNET 接口的名称。取值必须为长度不大于 31 个字符的字符串。支持数字、字母和特殊字符（特殊字符包括‘@’、‘!’、‘~’、‘.’、‘_’、‘:’、‘-’）。参数取值不能包含空格，参数名称不能与已存在的接口名称相同。

no segment mnet <mnet_interface_name>

该命令用于从分区中删除一个特定的 MNET 接口。

mnet_interface_name 该参数指定待删除的 MNET 接口名称。

show segment mnet

该命令用于显示分区中所有 MNET 接口的配置。

clear segment mnet

该命令用于清除分区中所有 MNET 接口的配置。

segment vlan {system_ifname|bond_ifname} <vlan_ifname> <vlan_tag>

该命令用于在指定的系统接口或聚合接口上创建用于分区的虚拟局域网（VLAN，Virtual Local Area Network）接口。系统支持最多配置 4094 个 VLAN 接口，包括系统 VLAN 接口和分区 VLAN 接口。

系统 VLAN 接口和分区 VLAN 接口不能拥有相同的接口名称和标识 ID。

system_ifname	该参数指定系统接口的名称，默认为 port1、port2、port3、port4……。 （管理员可以通过“ interface name ”命令来自定义系统接口名称。）
bond_ifname	该参数指定聚合接口的名称，默认的聚合接口名称为 bond1、bond2、bond3、bond4……。 （管理员可以通过“ bond name ”命令来自定义聚合接口名称。）
vlan_ifname	该参数指定 VLAN 接口的名称，由字母和数字组成，最多支持 31 个字符。
vlan_tag	该参数指定 VLAN 接口的标识 ID，可以配置为 1 至 4094 之间的任意整数。



注意：请不要在配置了聚合接口的接口上配置 VLAN 接口。

no segment vlan <vlan_ifname>

该命令用于删除指定的分区 VLAN 接口。

show segment vlan

该命令用于显示所有分区 VLAN 接口的配置。

clear segment vlan

该命令用于清除所有分区 VLAN 接口的配置。

segment {enable|disable}

该命令用于启用或者禁用分区 NAT 功能。分区 NAT 功能默认设置为禁用。

segment nat <segment_name> <segment_ip> <internal_ip> {netmask|prefix}

该命令用于为指定的分区配置一条地址转换规则，每个分区最多配置 4096 条地址转换规则。

segment_name	该参数指定已存在的分区名称。
segment_ip	该参数指定需要转换的 IP 地址，可以为 IPv4 或 IPv6 地址。
internal_ip	该参数指定转换后的 IP 地址。

netmask prefix	该参数指定需要转换的 IP 地址对应的子网掩码或前缀长度。
	“mask”用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。



注意：

- 在 SLB 反向代理模式中，如果不通过命令 “segment nat” 为分区的后台服务的 IP 地址配置地址转换规则，后台服务将会使用系统路由。
- 若管理员需要为不同分区配置到相同目的网络的静态路由，需要先通过 “segment nat” 命令为每个分区配置 NAT 转换规则。
- 在实际使用中，不允许将 “internal_ip” 配置为系统自动分配的 IP 网段。

no segment nat <segment_name> <segment_ip> <internal_ip>
{netmask|prefix}

该命令用于删除指定分区的一条地址转换规则配置。

show segment nat [segment_name]

该命令用于显示指定分区的所有地址转换规则配置。如不指定参数 “segment_name”，则显示所有分区的地址转换规则配置。

clear segment nat [segment_name]

该命令用于清除指定分区的所有地址转换规则配置。如不指定参数 “segment_name”，则清除所有分区的地址转换规则配置。

segment ha group id <group_id>

该命令用于定义一个分区浮动 IP 分组。每个节点最多定义 1024 个浮动 IP 分组，包括系统浮动 IP 分组和分区浮动 IP 分组。

group_id 该参数指定浮动 IP 分组的 ID，取值必须为 0 至 1023 之间的整数。

no segment ha group id <group_id>

该命令用于删除指定的分区浮动 IP 分组。

segment ha group {enable|disable} <group_id>

该命令用于启用或禁用指定的分区浮动 IP 分组。默认情况下，系统禁用所有的分区浮动 IP 分组。当一个分区浮动 IP 分组在多个 HA 节点上被启用时，仅由分区浮动 IP 分组状态为 “Active” 的 HA 节点提供该分区浮动 IP 分组所对应的应

用服务。分区浮动 IP 分组需要通过“**segment ha group fip**”或“**segment ha group fiprange**”命令与应用服务关联起来。

group_id 该参数指定已存在的分区浮动 IP 分组的 ID，取值必须为 0 至 1024 之间的整数，取值为 1024 时表示启用或禁用所有的分区浮动 IP 分组。

segment ha group preempt {on|off} <group_id>

该命令用于为指定分区浮动 IP 分组启用或禁用抢占模式。抢占模式能够确保分区浮动 IP 分组在优先级最高的可用节点上的状态始终为“Active”。默认情况下，系统禁用分区浮动 IP 分组的抢占模式。

group_id 该参数指定已存在的分区浮动 IP 分组的 ID，取值必须为 0 至 1024 之间的整数，取值为 1024 时表示为所有的分区浮动 IP 分组启用或禁用抢占模式。

segment ha group priority <unit_name> <group_id> <priority>

该命令用于配置指定分区浮动 IP 分组在指定 HA 节点上的优先级。

unit_name 该参数指定 HA 节点的名称，可以为本地节点或对端节点。

group_id 该参数指定已存在的浮动 IP 分组的 ID。

priority 该参数指定优先级，取值必须为 0 至 255 之间的整数，取值越大，优先级越高。

no segment ha group priority <unit_name> <group_id>

该命令用于删除指定分区浮动 IP 分组在指定 HA 节点上的优先级配置。

segment ha group fip <group_id> <floating_ip> <segment_name> [<interface_name>] [<floating_mac>]

该命令用于将指定的分区浮动 IP 分组与指定分区绑定，并为该分区浮动 IP 分组配置一个浮动 IP 地址。

group_id 该参数指定已存在的浮动 IP 分组的 ID。

floating_ip 该参数指定浮动 IP 地址，可以为 IPv4 或 IPv6 地址。

segment_name 该参数指定已存在的分区名称。

interface_name 可选，该参数指定绑定浮动 IP 地址的接口名称，取值必须为系统接口、聚合接口、MNET 接口、VLAN 接口的名称或“auto”。“auto”表示系统将自动选择一个接口。注意：不建议将该参数设置为主链路所在接口。

当需要绑定浮动 MAC 地址时，该参数不能设置为聚合接口的成员接口。

默认值为“auto”。

当需要配置“floating_mac”参数，又需要设置该参数为默认值时，必须指定“auto”。当不需要配置“floating_mac”参数时，可以不指定取值来表示使用默认值。

floating_mac 可选，该参数指定一个浮动 MAC 地址，格式为 `xx:xx:xx:xx:xx:xx`。该 MAC 地址不能为任何系统接口的 MAC 地址，不能和同一浮动 IP 分组其他系统接口或者聚合接口绑定的 MAC 地址相同，不能和其他浮动 IP 分组绑定的 MAC 地址相同，也不能和网桥使用的系统接口 MAC 地址相同。

默认值为空，表示不使用浮动 MAC 功能。

no segment ha group fip <group_id> <floating_ip> <segment_name>

该命令用于删除指定分区的一条浮动 IP 地址配置。

segment ha group fiprange <group_id> <start_floating_ip> <end_floating_ip> <segment_name> [interface_name] [floating_mac]

该命令用于将指定分区浮动 IP 分组与指定分区绑定，并为该分区浮动 IP 分组配置一个浮动 IP 地址段。

每个分区浮动 IP 地址段中最多包含 256 个 IP 地址。

group_id	该参数指定已存在的分区浮动 IP 分组的 ID。
start_floating_ip	该参数指定浮动 IP 地址段的起始 IP，可以为 IPv4 或 IPv6 地址。
end_floating_ip	该参数指定浮动 IP 地址段的结束 IP，可以为 IPv4 或 IPv6 地址。
segment_name	该参数指定已存在的分区名称。
interface_name	可选，该参数指定绑定浮动 IP 地址的接口名称，取值必须为系统接口、聚合接口、MNET 接口、VLAN 接口的名称或“auto”。“auto”表示系统将自动选择一个接口。注意：不建议将该参数设置为主链路所在接口。当需要绑定浮动 MAC 地址时，该参数不能设置为聚合接口的成员接口。

默认值为“auto”。

当需要配置“floating_mac”参数，又需要设置该参数为默认值时，必须指定“auto”。当不需要配置“floating_mac”参数时，可以不指定取值来表示使用默认值。

floating_mac

可选，该参数指定一个浮动 MAC 地址，格式为 xx:xx:xx:xx:xx:xx。该 MAC 地址不能为任何系统接口的 MAC 地址，不能和同一浮动 IP 分组其他系统接口或者聚合接口绑定的 MAC 地址相同，不能和其他浮动 IP 分组绑定的 MAC 地址相同，也不能和网桥使用的系统接口 MAC 地址相同。

默认值为空，表示不使用浮动 MAC 功能。

设备上支持的浮动 IP 地址、浮动 IP 地址段、分区浮动 IP 分组和分区浮动 IP 地址段共有的最大数量取决于系统内存的大小，如下表所示。

表8 - 2 地址段共有的最大数量

系统内存	最大数量
<= 8 GB	2000
16 GB	4000
24 GB	4000
>= 32 GB	8000

no segment ha group fiprange <group_id> <start_floating_ip>
<end_floating_ip> <segment_name>

该命令用于删除指定分区的一条浮动 IP 地址段配置。

clear segment ha group all

该命令用于清除所有浮动 IP 分组及相关配置。

segment ha decision rule <condition_name> <action_name> [group_id]

该命令用于为指定的分区浮动 IP 分组配置一条失效切换规则，规定当指定的健康检查条件由 Up 状态变为 Down 时，执行指定的失效切换动作。同一个健康检查条件最多可以用于 1024 个失效切换规则的配置中。

condition_name

该参数指定健康检查条件的名称，取值必须为预定义的健康检查条件或自定义的健康检查条件组的（vcondition）名称：

系统支持的健康检查包括：

- （预定义）PORT_1~PORT_32：端口健康检查条件
- GATEWAY_1~GATEWAY_32：网关健康检查条件

- CPU_UTIL: CPU 使用率健康检查条件
- CPU_TEMP: CPU 温度健康检查条件
- SSL_CARD: SSL 加速卡健康检查条件
- SSL_AE_UTIL: SSL 加速卡 AE 内核使用率健康检查条件
- SSL_SE_UTIL: SSL 加速卡 SE 内核使用率健康检查条件
- SYSTEM_MEM_UTIL: 系统内存使用率健康检查条件
- NETWORK_MEM_UTIL: 网络内存使用率健康检查条件
- SWAP_MEM_UTIL: SWAP 内存使用率健康检查条件
- CONN_MEM_UTIL: 连接内存使用率健康检查条件
- SYSTEM_DISK_UTIL: 系统硬盘分区使用率健康检查条件
- DATA_DISK_UTIL: 数据硬盘分区使用率健康检查条件
- SCRIPT: 自定义脚本健康检查条件
- 自定义的健康检查条件组 (vcondition) 名称, 可以通过 “monitor vcondition name” 命令配置。

action_name

该参数指定当健康检查条件的状态变为 Down 时, 需要执行的切换动作, 取值可以为:

- Unit_Failover: 表示对节点上所有的分区浮动 IP 分组执行状态切换动作。
- Group_Failover: 表示对指定的分区浮动 IP 分组执行状态切换动作, 系统会基于 HA 节点的健康状况和分组优先级重新选择接管服务的节点, 并将节点上的分区浮动 IP 分组置为 “Active” 状态。
- Reboot: 表示对节点上所有的分区浮动 IP 分组执行状态切换动作后, 再执行重启设备操作。

group_id

可选, 该参数指定需要执行切换规则的分区浮动 IP 分组的 ID, 该参数仅在 “action_name” 参数设置为

“Group_Failover”时才需要配置。

no segment ha decision rule <condition_name> <action_name> [group_id]

该命令用于删除指定分区浮动 IP 分组的一条失效切换规则。

clear segment ha decision rule

该命令用于清除所有分区的失效切换规则。

show segment ha config

该命令用于显示所有分区的 HA 功能相关的所有配置。

show segment ip eroute <segment_name>

该命令用于显示系统为指定分区生成的 Eroute 路由。

show segment config [segment_name]

该命令用于显示指定分区相关的所有配置。如不指定参数“segment_name”，则显示所有分区相关的所有配置。

show segment summary [segment_name]

该命令用于显示指定分区的主要配置信息。如不指定参数“segment_name”，则显示所有分区的主要配置信息。

write segment file

该命令用于将所有分区内当前的运行配置保存到备份文件。

config segment file

该命令用于加载通过“write segment file”命令保存的所有配置。

write segment memory [segment_name]

该命令用于将指定分区内的所有配置保存到硬盘中作为下次的启动配置。如不指定参数“segment_name”，则保存所有分区内的配置。执行该命令后，建议执行“write memory”命令。

show current segment

该命令用于显示当前所处的分区。该命令在系统模式和分区模式下均可执行。在系统模式下执行时，系统会提示当前属于全局用户，不显示分区。

8.2 分区模式

分区拥有独立的用于配置 SLB、SSL 和 SDNS 的 CLI 命令，所有分区支持的 CLI 命令相同。对于 Config 级别的分区管理员账号，在 Config 模式下输入“?”可

查看分区内支持的所有 CLI 命令。命令功能请参考其他章节内对应命令的描述，以下命令仅在分区模式下可用。

**注意：**

- 对于 SDNS 模块，系统模式和分区模式下，参数“host_name”、“service_name”、“pool_name”、“monitor_name”、“oid_name”和“expression”命名需要全局唯一，不同的分区下也不能相同。分区模式下，参数“host_name”不支持泛域名，即不能配置“*”。
- 对于 SDNS 模块，全局指全局账户，并非所有分区管理员账户。

password <password>

该命令用于修改分区管理员账号的密码。

password

该参数指定新密码。

在强制密码模式关闭时，取值必须为 1 至 116 个字节的字符串，区分大小写。当参数取值包含数字或特殊字符时，必须置于双引号内。

在强制密码模式开启时，取值必须满足强制密码模式的密码复杂度要求（参考“**passwd forcemode**”命令）。

第9章 SSL 加速

本章介绍 SSL（Secure Sockets Layer，安全套接层）特性的相关配置命令。

SSL 协议在应用层协议（例如 HTTP 和 FTP）和 TCP/IP 协议之间建立数据安全层，为 TCP/IP 连接上的服务提供保密性、认证和信息完整性。

通常情况下，当 SLB 后台服务与客户端进行 SSL 安全通信时，需要消耗大量的系统资源来处理 SSL 加解密工作。设备采用 SSL 代理技术将 SSL 加解密工作移交至具有高 SSL 处理性能的设备上，在满足 SLB 虚拟服务与客户端、后台应用服务之间加密通信需求的同时，大大提高服务器性能，从而提升用户体验。

9.1 SSL 主机配置

ssl host {virtual|real} <host_name> [slb_service]

该命令用于创建一个 SSL 主机，并将它与一个指定 SLB 服务相关联。在关联 SSL 主机到 SLB 服务之前，需要先创建该 SLB 服务。可将多个不同的 SLB 服务关联到同一个 SSL 主机以节省 SSL 资源。目前一个 SSL 主机可以关联最多 2000 个 SLB 服务。

virtual|real

该参数指定 SSL 主机所关联的 SLB 服务的类型：

- **virtual**：表示 SSL 主机关联到 SLB 虚拟服务。此时 SSL 主机充当一个 SSL 服务器，称为 SSL 虚拟主机。
- **real**：表示 SSL 主机关联到 SLB 后台服务。此时 SSL 主机充当一个 SSL 客户端，称为 SSL 后台主机。

SSL 虚拟主机和 SSL 后台主机是两个不同的实体，具有不同的配置参数。

host_name

该参数指定 SSL 主机的名称。取值必须为长度不大于 240 个字节的字符串。支持数字、字母和下划线，但不能以下划线开头。不支持特殊字符和空格符。

在分区模式下配置该命令时，该参数的取值长度上限为 100 个字节。

slb_service

可选，该参数指定该 SSL 主机所要绑定的 SLB 服务名称。SSL 虚拟主机绑定的 SLB 虚拟服务必须是 HTTPS、TCPS 或 FTPS 类型。SSL 后台主机绑定的 SLB 后台服务必须是 HTTPS 或 TCPS 类型。如果不指定该参数，系统将只创建 SSL 主机，不关联 SLB 服务。



注意：SSL 虚拟主机不能和虚拟 IP 为“0.0.0.0”的 SLB 虚拟服务关联，除非该 SSL 虚拟主机已经启用了 SSL 侦听功能。

no ssl host {virtual|real} <host_name> <slb_service>

该命令用于删除 SSL 主机和指定 SLB 服务的关联关系。

show ssl host

该命令用于显示当前配置的 SSL 主机及其关联的 SLB 服务。

clear ssl host <host_name>

该命令用于删除指定 SSL 虚拟或后台主机，并清除其配置，包括私钥和证书等。使用本命令后，若想重新配置该 SSL 主机，需重新创建私钥，购买新的证书。

show ssl session <host_name> [num_of_conn]

该命令用于显示指定 SSL 虚拟或后台主机上的 SSL 连接的相关信息，包括客户端 IP 地址、服务端 IP 地址，会话 ID 和密码套件。

host_name 该参数指定 SSL 虚拟或后台主机的名称。

num_of_conn 可选，该参数指定 SSL 虚拟或后台主机显示的连接的数量。取值必须为 1 到 1000 之间的整数，默认值为 100。

ssl sni <host_name> <domain_name>

该命令用于将一个域名和一个 SSL 虚拟主机或后台主机关联。一个 SSL 虚拟主机最多能和 64 个域名关联，一个 SSL 后台主机只能关联一个域名。

支持在 SSL 主机处于启用状态时进行配置。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

domain_name 该参数指定域名的名称。取值必须为长度不大于 255 个字节的字符串。如果参数名称不是以字符开头，参数必须置于双引号内。

当“host_name”的取值为虚拟主机名称时，该参数支持使用通配符“*”，用于匹配 0 个或多个在它之前的字符，取值格式必须为“*.domain.com”，不支持“a*.domain.com”、“*a.domain.com”等格式。

举例：

当设置该参数为“*.domain.com”时，所有以“.domain.com”结尾的域名都会被关联到指定的虚拟主机，例如“www.domain.com”、“blog.domain.com”。如果同时配置了“www.domain.com”和“*.domain.com”，前者将优先被匹配。



注意：虚拟主机或后台主机名称的长度和关联的 SNI 域名长度的总和不能超过 220 个字符。

show ssl sni <host_name>

该命令用于显示与指定的 SSL 主机关联的域名。

clear ssl sni <host_name> <domain_name>

该命令用于删除域名和指定的 SSL 主机的关联关系。



注意：执行该命令后，所有与指定域名的 SSL 主机关联的 SSL 配置（包括密钥）都将被删除。一旦密钥被删除，管理员可能需要购买一个新的证书。

ssl settings autosni <real_host_name>

该命令用于为指定 SSL 后台主机启用自动获取 SNI 的功能。启用该功能后，在连接后台服务前，SSL 后台主机会从 SSL 虚拟主机获取 SNI 后发送给后台服务。该功能的默认设置为启用。

real_host_name 该参数指定 SSL 后台主机的名称。

ssl snmp oid vhost <virtual_host_name> <index>

该命令用于为指定的虚拟主机配置一个静态 SNMP OID。虚拟主机的静态 SNMP OID 由系统已定义的 SNMP OID 前缀和在该命令的“index”参数中配置的 SNMP OID 索引号组成。例如，虚拟主机的 SNMP OID 前缀是

“1.3.6.1.4.1.7564.20.2.4.1.4”，SNMP OID 索引号是“4000”，则完整的 SNMP OID 为“1.3.6.1.4.1.7564.20.2.4.1.4.4000”。静态 SNMP OID 配置完成后将不会改变，优先级高于自动生成的动态 SNMP OID。如果没有配置静态 SNMP OID，系统将使用动态 SNMP OID。动态 SNMP OID 可能会在使用中发生变化。

virtual_host 该参数指定一个已存在的虚拟主机名称。

index 该参数指定 SNMP OID 的索引号，即 SNMP OID 中的最后一个数字。取值必须为 4000 到 7999 之间的整数。

no ssl snmp oid vhost <virtual_host_name>

该命令用于删除指定虚拟主机的静态 SNMP OID。当静态 SNMP OID 删除后，虚拟主机将使用动态 SNMP OID。

show ssl snmp oid vhost [virtual_host_name]

该命令用于显示指定虚拟主机的静态 SNMP OID。如不指定参数“virtual_host_name”，则显示所有虚拟主机的静态 SNMP OID。

clear ssl snmp oid vhost

该命令用于清除所有虚拟主机的静态 SNMP OID。

9.2 SSL 证书管理

**ssl csr <host_name> [key_length] [certificate_index]
[signature_algorithm_index] [domain_name] [csr_type_index]**

该命令用于为指定 SSL 虚拟或后台主机生成一个 CSR（Certificate Signing Request，证书签发请求）文件和密钥对。在此过程中系统将提示输入生成 CSR 所需的信息。可以选择将私钥设置为可导出的，并设置私钥的加密密码保护该私钥。此外，该命令也为 SSL 虚拟主机生成了一个测试证书，该证书只能用于测试，不能用于实际运行环境。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
key_length	可选，该参数指定生成的密钥对的长度，单位为比特（bit）。取值必须为 1024、2048 或者 4096。 默认值为 2048。
certificate_index	可选，该参数指定生成的测试证书的索引。取值必须为 1、2 或者 3。默认值为 1。
signature_algorithm_index	可选，该参数指定 CSR 文件签名算法的索引。 • 对于装备了 FIPS HSM 的设备，取值必须为 1，对应的签名算法为 sha1RSA。 • 对于未装备 FIPS HSM 的设备，如果要生成 PKCSv1.5 RSA 类型的 CSR，取值必须为 1、2、3 或者 4，对应的签名算法分别为 sha256RSA、sha384RSA、sha512RSA 和 sha1RSA；如果要生成 RSASSA-PSS 类型的 CSR，取值必须为 1、2 或 3。 无论设备是否装备 FIPS HSM，默认值均为 1。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。 • 如果指定参数“domain_name”，将会为与指定的 SSL 虚拟主机关联的指定的域名生成一个 CSR。 • 如果没有指定参数“domain_name”，将会为指定

的 SSL 虚拟或后台主机生成一个 CSR。

csr_type_index 可选，该参数指定 CSR 类型的索引，取值必须为：

- 0：表示生成 PKCSv1.5 RSA CSR。
- 1：表示生成 RSASSA-PSS CSR。

默认值为 0。



注意：

- 测试证书的签名算法使用参数 “signature_algorithm_index” 的设置。
- 私钥的 Passphrase 支持所有类型字符，对长度没有限制。但是 Passphrase 长度不能为 0。
- 支持在证书已激活时，对其索引生成 CSR。

**ssl ecc csr <host_name> [curve_name] [certificate_index]
[signature_algorithm_index] [domain_name]**

该命令用于为指定的 SSL 虚拟或后台主机生成一个基于 ECC（Elliptic Curve Cryptography，椭圆曲线密码体制）算法的 CSR 文件和密钥对。在此过程中系统将提示输入生成 CSR 所需的信息。可以选择将私钥设置为可导出的，并设置私钥的加密密码保护该私钥。此外，该命令也为 SSL 虚拟主机生成了一个测试证书，该证书只能用于测试，不能用于实际运行环境。

host_name 该参数指定 SSL 虚拟或后台主机的名称。

curve_name 可选，该参数指定椭圆曲线名称，取值必须为 “prime256v1”、“secp384r1” 或 “secp521r1”。

默认值为 “prime256v1”。

certificate_index 可选，该参数指定生成的测试证书的索引。取值必须为 1、2 或者 3。

默认值为 1。

signature_algorithm_index 可选，该参数指定 CSR 文件签名算法的索引。取值必须为 1、2、3 或者 4，对应的签名算法分别为 sha256ECDSA、sha384ECDSA、sha512ECDSA 和 sha1ECDSA。

默认值为 1。

domain_name 可选，该参数指定域名的名称。

- 如果指定参数 “domain_name”，将会为与指定的 SSL 虚拟主机关联的指定的域名生成一个 CSR。
- 如果没有指定参数 “domain_name”，将会为指定

的 SSL 主机生成一个 CSR。

以生成一个 SSL CSR 文件和密钥对为例，如果没有指定域名，系统要求输入的信息如下：

```
Demo(config)#ssl csr "ssl_vhost"
We will now gather some required information about your ssl virtual host,
This information is encoded into your certificate
Two character country code for your organization (eg. US):
State or province []:
Location or local city []:
Organization Name:
Organizational Unit:
Organizational Unit []:
Organizational Unit []:
Do you want to use the virtual host name "ssl_vhost" as the Common Name
(recommended)?(Y/N):
Email address of administrator []:
Do you want the private key to be exportable [Yes/(No)]:
Enter passphrase for the private key:
Confirm passphrase for the private key:
```

如果指定域名，系统要求输入的信息如下：

```
Demo(config)#ssl csr "ssl_vhost" 2048 1 1 www.foo.com
We will now gather some required information about your ssl virtual host,
This information is encoded into your certificate
Two character country code for your organization (eg. US):
State or province []:
Location or local city []:
Organization Name:
Organizational Unit:
Organizational Unit []:
Organizational Unit []:
Do you want to use the SNI domain-name "www.foo.com" (of virtual host "ssl_vhost ")
as the Common Name? (recommended) [Y/N]:
Email address of administrator []:
Do you want the private key to be exportable [Yes/(No)]:
Enter passphrase for the private key:
Confirm passphrase for the private key:
```

上述信息中，主题字段“State or province”、“Location or local city”和“Email address of administrator”为可选项。可以为“Organizational Unit”主题字段指定最多 3 个值。CSR 中各主题字段的最大长度必须遵守以下限制：

- Two Character Country Code: 2 个字节
- Common Name: 64 个字节
- State or Province: 64 个字节
- Location or Local City: 64 个字节
- Organization Name: 64 个字节
- Organizational Unit: 64 个字节
- Email Address of Administrator: 80 个字节

如果指定了域名，将会提示字段“Subject Alternate Name”。该字段是可选的，取值支持使用通配符“*”。该字段的最大长度如下：

- Subject Alternate Name: 256 个字节

当输入上述信息后，系统会产生 CSR，可以将其复制到 Email 中发送给 CA（Certificate Authority，证书授权中心）进行证书签发。



注意：

- 测试证书的签名算法使用参数“signature_algorithm_index”的设置。
- 私钥的 Passphrase 支持所有类型字符，对长度没有限制。但是 Passphrase 长度不能为 0。
- 当一个证书索引对应的证书为启动状态时，不能对该索引进行生成 CSR 操作。

ssl sm2 csr <host_name> [curve_name] [certificate_index] [format_index]

该命令用于为指定虚拟或后台主机生成 SM2 签名证书的 CSR 文件和签名密钥对。在此过程中系统将提示输入生成 CSR 所需的信息。可以选择将私钥设置为可导出的，并设置私钥的加密密码保护该私钥，密码长度不超过 1024 个字符。此外，该命令也为 SSL 虚拟或后台主机生成了一个测试证书，该证书只能用于测试，不能用于实际运行环境。

host_name	该参数指定 SSL 虚拟或后台主机的名称。
curve_name	可选，该参数指定椭圆曲线名称，取值必须为“sm2”。 默认值为“sm2”。
certificate_index	可选，该参数指定生成的测试证书的索引。取值必须为 1、2 或者 3。 默认值为 1。
format_index	可选，该参数指定数字信封格式的索引。取值必须为 1 或者 2，对应的数字信封格式分别为 SCCA（State Commercial Cryptography Administration，国家商用密码

管理局) 和 CFCA (China Financial Certification Authority, 中国金融认证中心) 格式。

默认值为 1。

注意: 当生成 CFCA 格式的 CSR 时, 可以选择是否导出 Challenge 密钥, 导出的 Challenge key 会被加密。



注意: 当一个证书索引对应的证书为激活状态时, 不能对该索引进行生成 CSR 操作。

ssl sm2 import challengekey <host_name> [key_index] [tftp_ip|url]
[file_name]

该命令用于为指定 SSL 虚拟主机或后台主机导入一个 Challenge 密钥。用于解密导入的 CFCA 格式的数字信封, 并将 Challenge 密钥与指定密钥索引相关联。系统支持为同一 SSL 主机导入最多三个私钥。

host_name	该参数指定 SSL 虚拟或后台主机的名称。
key_index	可选, 该参数指定待导入的 Challenge 密钥的索引。取值必须为 1、2 或者 3。分别对应为该 SSL 主机导入的 3 个 Challenge 密钥。默认值为 1。
tftp_ip url	可选, 该参数指定 Challenge 密钥的 TFTP 服务器的 IP 地址或 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 Challenge 密钥时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入 Challenge 密钥时才需要设置该参数。 默认值为空。
file_name	可选, 该参数指定 TFTP 服务器上的 Challenge 密钥文件名。默认值为 “<Host name>.key”。

使用 TFTP 方式导入 Challenge 密钥时, 即参数 “tftp_ip|url” 取值为 TFTP 服务器的 IP 地址时, 才需要设置该参数。

ssl sm2 export challengekey <host_name> [key_index]

该命令用于为指定 SSL 虚拟主机或后台主机导出 Challenge 密钥。

host_name	该参数指定 SSL 虚拟或后台主机的名称。
key_index	可选，该参数指定证书索引号。取值必须为 1、2 或者 3。 默认值为 1。

no ssl csr <host_name> [domain_name] [csr_type]

该命令用于删除指定 SSL 虚拟或后台主机的 CSR。

host_name	该参数指定 SSL 虚拟或后台主机的名称。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。 取值必须为： • 域名：表示删除该域名的 CSR。 • 空：表示删除指定虚拟或后台主机的 CSR（使用 “ ” 表示空）。 默认值为空。
csr_type	可选。该参数指定要删除的 CSR 的类型。取值必须为： • rsa：表示删除 RSA 类型的 CSR。 • ecc：表示删除 ECC 类型的 CSR。 • sm2：表示删除 SM2 类型的 CSR。 • all：表示删除所有类型的 CSR。 默认值为 “all”。



注意：随命令 “ssl csr”、“ssl ecc csr” 或 “ssl sm2 csr” 生成的测试证书和密钥对不会被删除。

show ssl csr <host_name> [domain_name] [csr_type]

该命令用于显示指定 SSL 虚拟或后台主机的 CSR。

host_name	该参数指定 SSL 虚拟或后台主机的名称。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。 取值必须为： • 域名：表示显示该域名的 CSR。 • 空：表示显示指定虚拟或后台主机的 CSR（使用 “ ” 表示空）。 默认值为空。

`csr_type` 可选。该参数指定需要显示的 CSR 的类型。取值必须为：

- `rsa`：表示显示 RSA 类型的 CSR。
- `ecc`：表示显示 ECC 类型的 CSR。
- `sm2`：表示显示 SM2 类型的 CSR。
- `all`：表示显示所有类型的 CSR。

默认值为“all”。



注意：在执行下文中出现的“`ssl import...`”相关命令时，若采用 copy-n-paste 方式导入，请确保在手动粘贴到 CLI 命令行的证书内容的下方输入字符串“...”，从而结束导入操作。

ssl import key *<host_name> [key_index] [domain_name] [tftp_ip|url] [file_name|password]*

该命令用于为指定 SSL 虚拟或后台主机导入一个私钥，并将这个私钥与指定私钥索引相关联。系统支持为同一 SSL 主机导入最多三个私钥。

当采用 copy-n-paste 方式导入私钥时，只需要运行该命令“**ssl import key**”，并把私钥内容复制粘贴到 CLI 命令行中即可。该命令还支持通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入私钥。

对于装备了 FIPS HSM 的设备，只能导入之前从该 FIPS HSM 导出的 RSA 公私钥对。导出的 RSA 公私钥对是受 FIPS HSM 加密密码保护的。如果 FIPS HSM 加密密码改变，导出的 RSA 公私钥对将不能导回设备。

`host_name` 该参数指定 SSL 虚拟或后台主机的名称。

`key_index` 可选，该参数指定导入的私钥所关联的私钥索引。取值必须为 1、2 或者 3，分别对应为该 SSL 主机导入的三个私钥。默认值为 1。

`domain_name` 可选。该参数指定与 SSL 虚拟主机关联的域名。

- 如果指定参数“`domain_name`”，将会为与指定 SSL 虚拟主机关联的指定域名导入密钥。
- 如果没有指定参数“`domain_name`”，将会为指定的 SSL 主机导入密钥。

默认值为空。

注意：如果需要通过 URL 方式（即“`tftp_ip|url`”参数取值为 URL）为 SSL 虚拟或后台主机导入私钥，该参

数取值应为 “”。

tftp_ip|url

可选, 该参数指定私钥的 TFTP 服务器的 IP 地址或 URL 地址。

- “tftp_ip” 用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入私钥时才需要设置该参数。
- “url” 用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。使用 URL 方式导入私钥时才需要设置该参数。

默认值为空。

file_name|password

可选, 该参数指定 TFTP 服务器上私钥的文件名或通过 URL 获取的私钥文件密码。取值的最大长度受 CLI 支持的命令行最大长度限制, 目前 CLI 最多支持 1024 个字节的命令行。

- 当参数 “tftp_ip|url” 设置为 TFTP 服务器的 IP 地址时, 该参数取值为 TFTP 服务器上的私钥文件名。如果指定了参数 “domain_name”, 该参数默认值为 <hostname>_<domainname>.key。如果没有指定参数 “domain_name”, 该参数默认值为 <virtual_host_name>.key。
- 当参数 “tftp_ip|url” 设置为私钥文件的 URL 地址时, 该参数取值为私钥文件的密码。对于 PFX 格式的证书文件, 必须设置密码, 对于 PEM 格式的证书文件, 密码可选。取值必须置于双引号内。

默认值为空。



注意:

- 当手动将私钥内容复制粘贴到 CLI 命令行时, 对于未装备 FIPS HSM 的设备, 请确保以 “-----BEGIN RSA PRIVATE KEY-----” 字符串开头, “-----END RSA PRIVATE KEY-----” 字符串结尾; 对于装备了 FIPS HSM 的设备, 请确保以 “-----FIPS PUBLIC KEY-----” 字符串开头, “-----FIPS END KEYS-----” 字符串结尾。
- 本命令也可以从 TFTP 服务器上导入未加密的私钥, 但是不建议使用这种不安全的导入方式。
- 虚拟主机或后台主机名称的长度和关联的 SNI 域名长度的总和不能超过 220 个字符。

ssl export key <host_name> [key_index] [domain_name] [key_type]

该命令用于显示指定 SSL 虚拟或后台主机的可导出的私钥文件，可以将私钥复制保存到本地文件中以供后续使用。

对于装备了 FIPS HSM 的设备，导出的文件是 RSA 公私钥对。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
key_index	可选，该参数指定私钥关联的私钥索引号。取值必须为 0、1、2 或 3。 默认值为 0，表示当前的激活私钥。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为： • 域名：表示显示该域名的私钥文件。 • 空：表示显示指定虚拟主机的私钥文件（使用 “ ” 表示空）。 默认值为空。
key_type	可选。该参数指定需要显示的私钥的类型。取值必须为： • rsa：表示只显示 RSA 类型的私钥文件。 • ecc：表示只显示 ECC 类型的私钥文件。 • all：表示显示所有类型的私钥文件。 默认值为 “all”。

ssl sm2 import enckey <host_name> [key_index] [tftp_ip|url] [file_name]

该命令用于为指定 SSL 虚拟主机或后台主机导入 SM2 加密密钥对的私钥（以下简称“加密私钥”），并将这个私钥与指定私钥索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴加密私钥的内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入加密私钥文件。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
key_index	可选，该参数指定导入的加密私钥所关联的私钥索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 主机导入的三个 SM2 加密私钥。 默认值为 1。
tftp_ip url	可选，该参数指定加密私钥的 TFTP 服务器的 IP 地址 URL 地址。

- “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入加密私钥时才需要设置该参数。
- “url”用于配置加密私钥文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入加密私钥时才需要设置该参数。

默认值为空。

file_name 可选, 该参数指定 TFTP 服务器上的加密私钥的文件名。默认值为 “<Host name>.key”。

使用 TFTP 方式导入加密私钥时, 即参数 “tftp_ip|url” 取值为 TFTP 服务器的 IP 地址时, 才需要设置该参数。



注意: 如果为每个 SSL 虚拟主机的三个证书索引都导入了加密证书和签名证书, 那么系统至多支持为 167 个 SSL 虚拟主机导入加密私钥。这个限制只适用于密码卡。

ssl sm2 export enckey <host_name> [key_index]

该命令用于显示指定 SSL 虚拟主机或后台主机的加密私钥。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

key_index 可选, 该参数指定导入的加密私钥所关联的私钥索引号。取值必须为 0、1、2 或者 3。

默认值为 0, 表示当前激活的加密私钥。

ssl sm2 import signkey <host_name> [key_index] [tftp_ip|url] [file_name]

该命令用于为指定的 SSL 虚拟主机或后台主机导入 SM2 签名密钥对的私钥（以下简称“签名私钥”），并将这个私钥与指定私钥索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴签名私钥的内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入签名私钥。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

key_index 可选, 该参数指定导入的签名私钥所关联的私钥索引号。取值必须为 1、2 或者 3, 分别对应为该 SSL 主机导入的三个签名私钥。

默认值为 1。

tftp_ip|url 可选, 该参数指定 TFTP 服务器的 IP 地址或签名私钥文件的 URL 地址。

- “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入签名私钥时才需要设置该参数。
- “url”用于配置签名私钥文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入签名私钥时才需要设置该参数。

默认值为空。

file_name 可选，该参数指定 TFTP 服务器上的签名私钥文件名。默认值为 “<Host name>.key”。

使用 TFTP 方式导入签名私钥时，即参数 “tftp_ip|url” 取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。



注意：如果为每个 SSL 虚拟主机的三个证书索引都导入了加密证书和签名证书，那么系统至多支持为 167 个 SSL 虚拟主机导入签名私钥。这个限制只适用于密码卡。

ssl sm2 export signkey <host_name> [key_index]

该命令用于显示指定 SSL 虚拟主机或后台主机的签名私钥。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

key_index 可选，该参数指定导入的签名私钥所关联的私钥索引号。取值必须为 0、1、2 或者 3。

默认值为 0，表示当前激活的签名私钥。

show ssl status key <host_name> [domain_name]

该命令用于显示指定 SSL 虚拟主机或后台主机的密钥状态。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

domain_name 可选，该参数指定与 SSL 虚拟主机关联的域名，只有参数 “host_name” 的取值为 SSL 虚拟主机的名称时才可用。

- 如果指定该参数，则显示 SSL 虚拟主机关联的指定域名的密钥状态。
- 如果没有指定该参数，则显示 SSL 虚拟主机关联的所有域名的密钥状态。

ssl import certificate <host_name> [certificate_index] [domain_name] [tftp_ip|url] [filename|password]

该命令用于为指定 SSL 虚拟或后台主机导入一个证书，并将这个证书与指定证书索引相关联。要使用一个证书，需要通过命令“**ssl activate certificate**”来激活。

当采用 copy-n-paste 方式导入证书时，只需要运行该命令“**ssl import certificate**”，并把证书内容复制粘贴到 CLI 命令行中即可，该方式仅支持 PEM 格式证书。该命令还支持通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入 PEM、DER 和 PFX 格式的证书。

host_name 该参数指定 SSL 虚拟或后台主机的名称。

certificate_index 可选，该参数指定导入的证书所关联的证书索引。取值必须为 1、2 或者 3，分别对应为该 SSL 主机导入的三个证书。默认值为 1。

SSL 主机的同一证书索引对应的私钥和证书必须匹配，否则系统会提示错误信息。

domain_name 可选，该参数指定与 SSL 虚拟主机关联的域名。

- 如果指定参数“**domain_name**”，将会为与指定 SSL 虚拟主机关联的指定域名导入证书。
- 如果没有指定参数“**domain_name**”，将会为指定的 SSL 主机导入证书。

默认值为空。

注意：

- 如果需要通过 URL 方式（即“**tftp_ip|url**”参数值为 URL）为 SSL 虚拟或后台主机导入证书，该参数取值应为“”。
- 系统模式下，主机名的长度和“**domain_name**”参数取值的长度两者之和必须不大于 255 个字节；分区模式下，分区名的长度、主机名的长度和“**domain_name**”参数取值的长度三者之和必须不大于 255 个字节。
- 如果指定了参数“**domain_name**”，需先通过命令“**ssl activate certificate**”为该 SSL 虚拟或后台主机导入并激活一张证书，才可以为该域名导入证书。

tftp_ip|url 可选，该参数指定证书的 TFTP 服务器的 IP 地址或 URL 地址。

- “**tftp_ip**”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入证书时才需

要设置该参数。

- “url” 用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。使用 URL 方式导入证书时才需要设置该参数。

默认值为空

file_name|password

可选，该参数指定 TFTP 服务器上的证书文件名或通过 URL 获取的证书文件密码。

- 当参数“tftp_ip|url”设置为 TFTP 服务器的 IP 地址时，该参数取值为 TFTP 服务器上的证书文件名。如果指定了参数“domain_name”，该参数默认值为<hostname>_<domainname>.cert。如果没有指定参数“domain_name”，该参数默认值为<virtual_host_name>.cert。
- 当参数“tftp_ip|url”设置为证书文件的 URL 地址时，该参数取值为证书文件的密码。对于 PFX 格式的证书文件，必须设置密码，对于 PEM 格式的证书文件，密码可选。取值必须置于双引号内。

默认值为空。



注意：虚拟主机或后台主机名称的长度和关联的 SNI 域名长度的总和不能超过 220 个字符。

show ssl import certificate match <host_name> [certificate_index]
[domain_name] [certificate_type] [url] [password]

该命令用于检测指定的证书是否已经导入系统。

指定需要检测的证书时，可以采用在该命令的交互模式中粘贴证书内容的方式，也可以采用指定证书文件的 HTTP/FTP/TFTP URL 地址的方式。

host_name 该参数指定 SSL 虚拟或后台主机的名称。

certificate_index 可选，该参数指定需要匹配的证书索引。取值必须为 1、2、3 或者 0，分别对应为该 SSL 主机导入的三个证书和所有证书。默认值为 0。

domain_name 可选，该参数指定需要匹配的 SSL 主机的关联域名。如需跳过该参数的设置，使用双引表示 (“”) 取值为空。默认值为空。

certificate_type 可选，该参数指定需要匹配的证书类型。取值必须为：

- **rsa**: 表示只匹配 RSA 类型的证书。
- **ecc**: 表示只匹配 ECC 类型的证书。
- **all**: 表示 RSA 和 ECC 类型的证书都匹配。

默认值为“all”。

url 可选，该参数指定证书文件在 FTP/TFTP/HTTP 服务器上的 URL 地址。如需跳过该参数的设置，使用双引表示（“”）取值为空。默认值为空。

password 可选，该参数指定证书文件的密码。默认值为空。

no ssl certificate <host_name> <certificate_index> [domain_name]
[certificate_type]

该命令用于删除指定 SSL 虚拟或后台主机的一个证书。

支持删除已激活的证书。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

certificate_index 该参数指定私钥关联的证书索引号。取值必须为 1、2 或 3。

domain_name 可选。该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为：

- **域名**: 表示删除该域名的证书。
- **空**: 表示删除指定虚拟主机的证书（使用“”表示空）。

默认值为空。

certificate_type 可选。该参数指定需要删除的证书的类型。取值必须为：

- **rsa**: 表示只删除 RSA 类型的证书。
- **ecc**: 表示只删除 ECC 类型的证书。
- **all**: 表示删除所有类型的证书。

默认值为“all”。

ssl sm2 import encertificate <host_name> [certificate_index] [tftp_ip|url]
[file_name]

该命令用于为指定的 SSL 虚拟主机或后台主机导入一个 SM2 加密证书，并将这个证书与指定证书索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴证书内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS

和 SCP 方式导入证书文件。导入的证书需要通过“**ssl activate certificate**”命令激活。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
certificate_index	可选，该参数指定导入的 SM2 加密证书所关联的证书索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 主机导入的三个 SM2 加密证书。 默认值为 1。
tftp_ip url	可选，该参数指定加密证书的 TFTP 服务器的 IP 地址或的 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 SM2 加密证书时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入 SM2 加密证书时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的 SM2 加密证书的文件名。默认值为“<Host name>.crt”。 使用 TFTP 方式导入 SM2 加密证书时，即参数“tftp_ip url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

no ssl sm2 encertificate <host_name> <certificate_index>

该命令用于删除指定 SSL 虚拟主机或后台主机的一个 SM2 加密证书。该命令将同时删除关联的 SM2 加密密钥对。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
certificate_index	可选，该参数指定需要删除的 SM2 加密证书的索引号。取值必须为 1、2 或者 3。

ssl sm2 import encevp <host_name> [certificate_index] [format_index] [url]

该命令用于为指定虚拟主机或后台主机导入指定格式的数字信封，并将该格式的数字信封与指定的证书索引相关连。数字信封由 CA 返回，其中包含加密证书和加密私钥。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。

certificate_index	可选，该参数指定证书索引号。取值必须为 1、2 或者 3。 默认值为 1。
format_index	可选，该参数指定数字信封格式的索引号。取值必须为 1 或者 2，分别对应 SCCA 格式和 CFCA 格式。 默认值为 1。
url	可选，该参数指定数字信封在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。 默认值为空。

ssl sm2 import signcertificate <host_name> [certificate_index] [tftp_ip|url] [file_name]

该命令用于为指定的 SSL 虚拟主机或后台主机导入一个 SM2 签名证书，并将这个证书与指定证书索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴证书内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入证书文件。导入的证书需要通过“**ssl activate certificate**”命令激活。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
certificate_index	可选，该参数指定导入的 SM2 签名证书所关联的证书索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 虚拟主机导入的三个 SM2 签名证书。 默认值为 1。
tftp_ip url	可选，该参数指定 TFTP 服务器的 IP 地址或签名私钥文件的 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 SM2 签名证书时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入签名私钥时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的 SM2 签名证书的文件名。默认值为“<Host name>.crt”。 使用 TFTP 方式导入 SM2 签名证书时，即参数

“tftp_ip|url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

no ssl sm2 signcertificate <host_name> <certificate_index>

该命令用于删除指定 SSL 虚拟主机或后台主机的一个 SM2 签名证书。该命令将同时删除关联的 SM2 签名密钥对。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

certificate_index 可选，该参数指定需要删除的 SM2 签名证书的索引号。取值必须为 1、2 或者 3。

ssl sm2 sni csr <host_name> <domain_name> [curve_name] [certificate_index] [format_index]

该命令用于为指定虚拟主机所关联的域名生成 SM2 签名证书的 CSR 文件和签名密钥对。在此过程中系统将提示输入生成 CSR 所需的信息。可以选择将私钥设置为可导出的，并设置私钥的加密密码保护该私钥，密码长度不超过 1024 个字符。此外，该命令也为 SSL 虚拟主机生成了一个测试证书，该证书只能用于测试，不能用于实际运行环境。

host_name 该参数指定 SSL 虚拟主机的名称。

domain_name 该参数指定与 SSL 虚拟主机关联的域名的名称。

curve_name 可选，该参数指定椭圆曲线名称，取值必须为“sm2”。默认值为“sm2”。

certificate_index 可选，该参数指定生成的测试证书的索引。取值必须为 1、2 或者 3。默认值为 1。

format_index 可选，该参数指定数字信封格式的索引。取值必须为 1 或者 2，对应的数字信封格式分别为 SCCA（State Commercial Cryptography Administration，国家商用密码管理局）和 CFCA（China Financial Certification Authority，中国金融认证中心）格式。默认值为 1。

注意：当生成 CFCA 格式的 CSR 时，可以选择是否导出 Challenge 密钥，导出的 Challenge key 会被加密。

ssl sm2 sni import challengekey <host_name> [domain_name] [key_index] [tftp_ip|url] [file_name]

该命令用于为指定 SSL 虚拟主机所关联的域名导入一个 Challenge 密钥，用于解密导入的 CFCA 格式的数字信封，并将 Challenge 密钥与指定密钥索引相关联。系统支持为同一 SSL 虚拟主机导入最多三个私钥。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为： 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入 Challenge 密钥。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入 Challenge 密钥。 默认值为空。
key_index	可选，该参数指定待导入的 Challenge 密钥的索引。取值必须为 1、2 或者 3。分别对应为该 SSL 虚拟主机导入的 3 个 Challenge 密钥。默认值为 1。
tftp_ip url	可选，该参数指定 Challenge 密钥的 TFTP 服务器的 IP 地址或 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 Challenge 密钥时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入 Challenge 密钥时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的 Challenge 密钥文件名。默认值为“<Host name>.key”。 使用 TFTP 方式导入 Challenge 密钥时，即参数“tftp_ip url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

ssl sm2 sni export challengekey <host_name> [domain_name] [key_index]

该命令用于为指定 SSL 虚拟主机所关联的域名导出 Challenge 密钥。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为： 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导出 Challenge 密钥。

如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导出 Challenge 密钥。

默认值为空。

key_index 可选，该参数指定证书索引号。取值必须为 1、2 或者 3。
默认值为 1。

**ssl sm2 sni import enckey <host_name> [domain_name] [key_index]
[tftp_ip|url] [file_name]**

该命令用于为指定 SSL 虚拟主机所关联的域名导入 SM2 加密密钥对的私钥（以下简称“加密私钥”），并将这个私钥与指定私钥索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴加密私钥的内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入加密私钥文件。

host_name 该参数指定 SSL 虚拟主机的名称。

domain_name 可选，该参数指定与 SSL 虚拟主机关联的域名。

如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入加密私钥。

如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入加密私钥。

默认值为空。

key_index 可选，该参数指定导入的加密私钥所关联的私钥索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 虚拟主机导入的三个 SM2 加密私钥。默认值为 1。

tftp_ip|url 可选，该参数指定加密私钥的 TFTP 服务器的 IP 地址 URL 地址。

“tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入加密私钥时才需要设置该参数。

“url”用于配置加密私钥文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入加密私钥时才需要设置该参数。

默认值为空。

file_name 可选，该参数指定 TFTP 服务器上的加密私钥的文件名。
默认值为“<Host name>.key”。

使用 TFTP 方式导入加密私钥时，即参数“tftp_ip|url”

取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

ssl sm2 sni export enckey <host_name> [domain_name] [key_index]

该命令用于导出指定 SSL 虚拟主机所关联的域名的加密私钥。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名。 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导出加密私钥。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导出加密私钥。 默认值为空。
key_index	可选，该参数指定导出的加密私钥所关联的私钥索引号。取值必须为 0、1、2 或者 3。 默认值为 0，表示当前激活的加密私钥。

ssl sm2 sni import signkey <host_name> [domain_name] [key_index] [tftp_ip|url] [file_name]

该命令用于为指定的 SSL 虚拟主机所关联的域名导入 SM2 签名密钥对的私钥（以下简称“签名私钥”），并将这个私钥与指定私钥索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴签名私钥的内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入签名私钥。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名。 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入签名私钥。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入签名私钥。 默认值为空。
key_index	可选，该参数指定导入的签名私钥所关联的私钥索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 虚拟主机导入的三个签名私钥。 默认值为 1。
tftp_ip url	可选，该参数指定 TFTP 服务器的 IP 地址或签名私钥文

件的 URL 地址。

“tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入签名私钥时才需要设置该参数。

“url”用于配置签名私钥文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入签名私钥时才需要设置该参数。

默认值为空。

file_name

可选，该参数指定 TFTP 服务器上的签名私钥文件名。默认值为 “<Host name>.key”。

使用 TFTP 方式导入签名私钥时，即参数 “tftp_ip|url” 取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

ssl sm2 sni export signkey <host_name> [domain_name] [key_index]

该命令用于导出指定 SSL 虚拟主机所关联的域名的签名私钥。

host_name

该参数指定 SSL 虚拟主机的名称。

domain_name

可选，该参数指定与 SSL 虚拟主机关联的域名。

如果指定参数 “domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导出签名私钥。

如果没有指定参数 “domain_name”，将会为指定的 SSL 虚拟主机导出签名私钥。

默认值为空。

key_index

可选，该参数指定导出的签名私钥所关联的私钥索引号。取值必须为 0、1、2 或者 3。

默认值为 0，表示当前激活的签名私钥。

ssl sm2 sni import encertificate <host_name> [domain_name] [certificate_index] [tftp_ip|url] [file_name]

该命令用于为指定的 SSL 虚拟主机所关联的域名导入一个 SM2 加密证书，并将这个证书与指定证书索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴证书内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入证书文件。导入的证书需要通过 “ssl activate certificate” 命令激活。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名。 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入 SM2 加密证书。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入 SM2 加密证书。 默认值为空。 注意： 系统模式下，主机名的长度和“domain_name”参数取值的长度两者之和必须不大于 255 个字节；分区模式下，分区名的长度、主机名的长度和“domain_name”参数取值的长度三者之和必须不大于 255 个字节。 如果指定了参数“domain_name”，需先通过命令“ssl activate certificate”为该 SSL 虚拟主机导入并激活一张证书，才可以为该域名导入证书。
certificate_index	可选，该参数指定导入的 SM2 加密证书所关联的证书索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 虚拟主机导入的三个 SM2 加密证书。 默认值为 1。
tftp_ip url	可选，该参数指定加密证书的 TFTP 服务器的 IP 地址或的 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 SM2 加密证书时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入 SM2 加密证书时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的 SM2 加密证书的文件名。默认值为“<Host name>.crt”。 使用 TFTP 方式导入 SM2 加密证书时，即参数“tftp_ip url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

ssl sm2 sni import enceph <host_name> [domain_name] [certificate_index]
[format_index] [url]

该命令用于为指定虚拟主机所关联的域名导入指定格式的数字信封，并将该格式的数字信封与指定的证书索引相关联。数字信封由 CA 返回，其中包含加密证书和加密私钥。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名的名称。 取值必须为： 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入数字信封。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入数字信封。 默认值为空。
certificate_index	可选，该参数指定证书索引号。取值必须为 1、2 或者 3。 默认值为 1。
format_index	可选，该参数指定数字信封格式的索引号。取值必须为 1 或者 2，分别对应 SCCA 格式和 CFCA 格式。默认值为 1。
url	可选，该参数指定数字信封在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。默认值为空。

ssl sm2 sni import signcertificate <host_name> [domain_name]
[certificate_index] [tftp_ip|url] [file_name]

该命令用于为指定的 SSL 虚拟主机所关联的域名导入一个 SM2 签名证书，并将这个证书与指定证书索引相关联。该命令支持两种导入方式，管理员可以在 CLI 命令行中手动粘贴证书内容，也可以通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入证书文件。导入的证书需要通过“ssl activate certificate”命令激活。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名。 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的指定域名导入 SM2 签名证书。 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入 SM2 签名证书。

默认值为空。

注意：

系统模式下，主机名的长度和“domain_name”参数取值的长度两者之和必须不大于 255 个字节；分区模式下，分区名的长度、主机名的长度和“domain_name”参数取值的长度三者之和必须不大于 255 个字节。

如果指定了参数“domain_name”，需先通过命令“ssl activate certificate”为该 SSL 虚拟主机导入并激活一张证书，才可以为该域名导入证书。

certificate_index	可选，该参数指定导入的 SM2 签名证书所关联的证书索引号。取值必须为 1、2 或者 3，分别对应为该 SSL 虚拟主机导入的三个 SM2 签名证书。默认值为 1。
tftp_ip url	可选，该参数指定 TFTP 服务器的 IP 地址或签名私钥文件的 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 SM2 签名证书时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器上的 URL 地址。取值必须置于双引号内。使用 URL 方式导入签名私钥时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的 SM2 签名证书的文件名。默认值为“<Host name>.crt”。 使用 TFTP 方式导入 SM2 签名证书时，即参数“tftp_ip url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

no ssl sm2 sni encertificate <host_name> [domain_name]
<certificate_index>

该命令用于删除指定 SSL 虚拟主机所关联的域名的一个 SM2 加密证书。该命令将同时删除关联的 SM2 加密密钥对。

host_name	该参数指定 SSL 虚拟主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为：

域名：表示删除该域名的 SM2 加密证书。

空：表示删除指定虚拟主机的 SM2 加密证书（使用 “ ” 表示空）。

默认值为空。

certificate_index 可选，该参数指定需要删除的 SM2 加密证书的索引号。
取值必须为 1、2 或者 3。

no ssl sm2 sni signcertificate <host_name> [domain_name]
<certificate_index>

该命令用于删除指定 SSL 虚拟主机所关联的域名的一个 SM2 签名证书。该命令将同时删除关联的 SM2 签名密钥对。

host_name 该参数指定 SSL 虚拟主机的名称。

domain_name 可选，该参数指定与 SSL 虚拟主机关联的域名的名称。
取值必须为：

域名：表示删除该域名的 SM2 签名证书。

空：表示删除指定虚拟主机的 SM2 签名证书（使用 “ ” 表示空）。

默认值为空。

certificate_index 可选，该参数指定需要删除的 SM2 签名证书的索引号。
取值必须为 1、2 或者 3。

ssl activate certificate <host_name> [certificate_index] [domain_name]
[certificate_type]

该命令用于激活指定 SSL 虚拟或后台主机的一个证书。SSL 虚拟主机关联的每个域名都可以激活一个 RSA 或 RSAPSS 证书和一个 ECC 证书；不关联域名时每个 SSL 虚拟主机可以激活一个 RSA 证书或 RSAPSS、一个 ECC 证书和一对 SM2 证书。每个 SSL 后台主机可以激活最多一个 RSA 或 RSAPSS 证书和一个 ECC 证书。

host_name 该参数指定 SSL 虚拟或后台主机的名称。

certificate_index 可选，该参数指定证书索引。取值必须为 1、2 或者 3，分别对应为该 SSL 主机导入的三个证书。默认值为 1。

domain_name 可选。该参数指定与 SSL 虚拟主机关联的域名的名称。
取值必须为：

- 域名：表示激活该域名的证书。
- 空：表示激活指定虚拟主机的证书（使用 “ ” 表示

空)。

默认值为空。

certificate_type 可选。该参数指定需要激活的证书的类型。取值必须为：

- **rsa**：表示激活 RSA 或 RSAPSS 证书。
- **ecc**：表示激活 ECC 证书。
- **sm2**：表示激活 SM2 证书。
- **all**：表示激活所有类型的证书。

默认值为“all”。

ssl deactivate certificate <host_name> <domain_name> <certificate_type>

该命令用于将指定 SSL 虚拟主机或后台主机的证书设置为非激活状态。

通过“**ssl activate certificate** <host_name> [certificate_index] [domain_name] [certificate_type]”命令激活另一个证书也可以将当前处于激活状态的证书设置为非激活状态。**注意：**在通过“**ssl deactivate certificate**”命令将一个 SSL 主机的激活证书设置为非激活状态前，或者通过“**ssl activate certificate**”命令将 SSL 主机的一个激活证书替换为另一个前，需先通过“**ssl stop**”命令禁用该 SSL 主机。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

domain_name 该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为：

- **域名**：表示将该域名的证书设置为非激活状态。
- **“ ”**：表示将指定虚拟主机的证书设置为非激活状态。

certificate_type 该参数指定需要设置为非激活状态的证书的类型。取值必须为：

- **rsa**：表示将 RSA 或 RSAPSS 证书设置为非激活状态。
- **ecc**：表示将 ECC 证书设置为非激活状态。
- **sm2**：表示将 SM2 证书设置为非激活状态。
- **all**：表示将所有类型的证书都设置为非激活状态。

show ssl certificate <host_name> [display_mode] [certificate_index]
[domain_name] [certificate_type]

该命令用于显示指定 SSL 虚拟或后台主机上的证书相关信息。

host_name	该参数指定 SSL 虚拟或后台主机的名称。取值必须为： • SSL 虚拟主机的名称：表示将显示指定 SSL 虚拟或后台主机上的证书相关信息。 • all：表示将显示虚拟主机的服务器证书、rootca 证书、interca 证书、后台主机证书和全局 CA 证书的相关信息。 当参数取值为 all 时，“host_name”之后的参数无效，系统将输出所有显示模式、证书索引、关联域名和证书类型等信息。
display_mode	可选，该参数指定 SSL 虚拟或后台主机的证书的显示模式。取值必须为： • complete：表示系统将显示证书的全部内容。 • simple：表示系统将只显示证书的字段“Issuer”，“Validity”和“Subject”。 默认值为“complete”。
certificate_index	可选，该参数指定证书索引。取值必须为： • 1、2 或者 3：表示系统将显示索引对应的 SSL 虚拟或后台主机的信息。 • 0：表示系统将显示 SSL 虚拟或后台主机当前被激活的证书的信息。 默认值为 0。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。取值必须为： • 域名：表示显示该域名的证书信息。 • 空：表示显示指定虚拟主机的证书信息（使用“”表示空）。 默认值为空。
certificate_type	可选。该参数指定需要显示的证书的类型。取值必须为： • rsa：表示只显示 RSA 或 RSAPSS 证书信息。 • ecc：表示只显示 ECC 证书信息。

- sm2: 表示只显示 SM2 证书信息。
- all: 表示显示所有类型的证书信息。

默认值为“all”。

show ssl status certificate <host_name> [domain_name]

该命令用于显示指定 SSL 虚拟或后台主机的证书状态。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
domain_name	可选，该参数指定与 SSL 虚拟主机关联的域名。只有参数“host_name”的取值为 SSL 虚拟主机的名称时才可用。 • 如果指定该参数，则显示与 SSL 虚拟主机关联的指定域名的证书状态。 • 如果不指定该参数，将显示与 SSL 虚拟主机关联的所有证书的状态。

ssl import rootca [host_name] [domain_name] [tftp_ip|url] [file_name]

该命令用于为指定 SSL 虚拟主机或后台主机或全局导入一个受信任 CA 证书。为全局导入的受信任 CA 证书将加入系统预置的受信任证书列表。用于所有未导入受信任 CA 证书的 SSL 后台主机校验 SSL 服务器证书。

当采用 copy-n-paste 方式导入受信任 CA 证书时，只需要运行该命令“**ssl import rootca**”，并将受信任 CA 证书的内容复制粘贴到 CLI 命令行中即可，该方式仅支持导入 PEM 格式的证书。该命令还支持通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入 PEM 和 DER 格式的受信任 CA 证书。

host_name	可选，该参数指定 SSL 主机的名称。取值必须为： • SSL 虚拟主机的名称：表示将受信任 CA 证书导入启用了 SSL 客户端认证功能的 SSL 虚拟主机，用于校验客户端证书。 • SSL 后台主机的名称：表示将受信任 CA 证书导入后台主机，用于校验 SSL 服务器证书。 • ALL: 表示将受信任 CA 证书加入系统预置的受信任 CA 证书列表（作为证书链的根证书），用于所有未导入受信任 CA 证书的 SSL 后台主机校验 SSL 服务器证书。

默认值为“ALL”。

domain_name	可选。该参数指定域名的名称。 - 如果指定参数“domain_name”，将会为与指定 SSL 虚拟主机关联的域名导入根 CA 证书。 - 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入根 CA 证书。 默认值为空。 注意： - 如果需要通过 URL 方式（即“tftp_ip url”参数值为 URL）为 SSL 虚拟或后台主机导入受信任 CA 证书，该参数取值应为“”。 - 系统模式下，主机名的长度和“domain_name”参数取值的长度两者之和必须不大于 255 个字节；分区模式下，分区名的长度、主机名的长度和“domain_name”参数取值的长度三者之和必须不大于 255 个字节。
tftp_ip url	可选，该参数指定受信任 CA 证书的 TFTP 服务器的 IP 地址或 URL 地址。 “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入受信任 CA 证书时才需要设置该参数。 “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。使用 URL 方式导入受信任 CA 证书时才需要设置该参数。 默认值为空。
file_name	可选，该参数指定 TFTP 服务器上的受信任 CA 证书的文件名。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。 - 为 SSL 虚拟主机导入受信任 CA 证书时，默认值为“<host_name>.crt”。 - 为系统预置受信任 CA 证书列表导入受信任 CA 证书时，默认值为“grootca.crt”。 使用 TFTP 方式导入受信任 CA 证书时，即参数“tftp_ip url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。



注意：在执行该命令为指定 SSL 主机导入受信任 CA 证书前，首先要确保该 SSL 主机为未激活状态，否则无法导入。如果 SSL 主机处于激活状态，可以使用命令“**ssl stop**”禁用该 SSL 主机。

no ssl rootca <host_name> [certificate_number]

该命令用于删除为指定 SSL 虚拟主机、SSL 后台主机或全局导入的受信任 CA 证书。

host_name

该参数指定 SSL 主机的名称。取值必须为：

- SSL 虚拟主机的名称：表示删除指定 SSL 虚拟主机的受信任 CA 证书。
- SSL 后台主机的名称：表示删除指定 SSL 后台主机的受信任 CA 证书。
- ALL：表示删除系统预置受信任 CA 证书列表中的受信任 CA 证书。

certificate_number

可选，该参数指定要删除的受信任 CA 证书的序号。证书对应的序号可以通过命令“**show ssl rootca**”查看。如果不指定该参数，系统将删除所有的受信任 CA 证书。



注意：在执行该命令从指定 SSL 虚拟主机删除受信任 CA 证书前，首先要确保该 SSL 虚拟主机为未激活状态，否则无法删除。如果 SSL 虚拟主机为激活状态，可以使用命令“**ssl stop** <host_name>”禁用该 SSL 虚拟主机。

show ssl rootca [host_name] [display_mode] [domain_name]

该命令用于显示为指定 SSL 虚拟主机、SSL 后台主机或者全局导入的受信任 CA 证书。

host_name

可选，该参数指定 SSL 主机的名称。取值必须为：

- SSL 虚拟主机的名称：表示显示指定 SSL 虚拟主机的所有受信任 CA 证书。
- SSL 后台主机的名称：表示显示指定 SSL 后台主机的所有受信任 CA 证书。
- ALL：表示显示系统预置受信任 CA 证书列表中的所有受信任 CA 证书。

默认值为“ALL”。

display_mode

可选，该参数指定受信任 CA 证书的显示模式。取值必须为：

- **complete:** 表示系统将显示证书的全部内容。
- **simple:** 表示系统将只显示证书的字段 “Issuer”，“Validity” 和 “Subject”。

默认值为 “complete”。

domain_name

可选。该参数指定域名的名称。

- 如果指定参数 “domain_name”，与指定 SSL 虚拟主机关联的域名的根 CA 证书将被显示。
- 如果没有指定参数 “domain_name”，指定 SSL 虚拟主机的根 CA 根证书将被显示。

no ssl sni rootca <virtual_host_name> [domain_name] [certificate_index]

该命令用于删除指定 SSL 虚拟主机的特定域名的一个根 CA 证书。

virtual_host_name

该参数指定 SSL 虚拟主机的名称。

domain_name

可选。该参数指定域名的名称。如果没有指定参数 “domain_name”，指定 SSL 虚拟主机的每个域名的所有根 CA 证书将被删除。

certificate_index

可选。该参数指定要删除的根 CA 证书的索引。根 CA 证书对应的索引可以通过命令 “**show ssl rootca**” 查看。



注意：只有当根 CA 证书处于非启动状态时，才能删除该证书。

ssl import interca <virtual_host_name> [domain_name] [tftp_ip|url] [file_name]

该命令用于为指定 SSL 虚拟主机导入一个中级 CA 证书，与激活的证书，受信任 CA 证书一起为 SSL 虚拟主机组成完整的证书链。其中，系统最多支持为构建的证书链导入八张中级 CA 证书。如果导入的 CA 证书超过八张，将无法发送所有 interca。

当采用 copy-n-paste 方式导入中级 CA 证书时，只需要运行该命令 “**ssl import interca**”，并将中级 CA 证书的内容复制粘贴到 CLI 命令行中即可，该方式仅支持导入 PEM 格式的证书。该命令还支持通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入 PEM 和 DER 格式的中级 CA 证书。

virtual_host_name

该参数指定 SSL 虚拟主机的名称。

domain_name

可选。该参数指定域名的名称。

- 如果指定参数 “domain_name”，将会为与指定 SSL

虚拟主机关联的域名导入中级 CA 证书。

- 如果没有指定参数“domain_name”，将会为指定的 SSL 虚拟主机导入中级 CA 证书。

默认值为空。

注意：如果需要通过 URL 方式（即“tftp_ip|url”参数值为 URL）为 SSL 虚拟主机导入中级 CA 证书，该参数取值应为“”。

tftp_ip|url

可选，该参数指定中级 CA 证书的 TFTP 服务器的 IP 地址或 URL 地址。

- “tftp_ip”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入中级 CA 证书时才需要设置该参数。
- “url”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。使用 URL 方式导入中级 CA 证书时才需要设置该参数。

默认值为空。

file_name

可选，该参数指定 TFTP 服务器上的中级 CA 证书的文件名。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。默认值为“<virtual_host_name>.crt”。

使用 TFTP 方式导入中级 CA 证书时，即参数“tftp_ip|url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。

no ssl interca <virtual_host_name> [certificate_number]

该命令用于删除指定 SSL 虚拟主机的中级 CA 证书。

virtual_host_name

该参数指定 SSL 虚拟主机的名称。

certificate_number

可选，该参数指定要删除的中级 CA 证书的序号。证书对应的序号可以通过命令“**show ssl interca**”查看。如果不指定该参数，系统将删除所有的中级 CA 证书。

show ssl interca <virtual_host_name> [display_mode] [domain_name]

该命令用于显示指定 SSL 虚拟主机的所有中级 CA 证书。

virtual_host_name

该参数指定 SSL 虚拟主机的名称。

display_mode 可选，该参数指定中级 CA 证书的显示模式。取值必须为：

- **complete**：表示系统将显示证书的全部内容。
- **simple**：表示系统将只显示证书的字段“Issuer”，“Validity”和“Subject”。

默认值为“complete”。

domain_name 可选。该参数指定域名的名称。

- 如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的中级 CA 证书将被显示。
- 如果没有指定参数“domain_name”，指定 SSL 虚拟主机的中级 CA 证书将被显示。

no ssl sni interca <virtual_host_name> [domain_name] [certificate_index]

该命令用于删除为指定的 SSL 虚拟主机的特定域名的一个中级 CA 证书。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

domain_name 可选。该参数指定域名的名称。如果没有指定参数“domain_name”，指定 SSL 虚拟主机的每个域名的所有中级 CA 证书将被删除。

certificate_index 可选。该参数指定要删除的中级 CA 证书的索引。中级 CA 证书对应的索引可以通过命令“**show ssl interca**”查看。



注意：只有当中级 CA 证书处于非启动状态时，才可以被删除。

ssl backup certificate <host_name> <file_name> <password>
[domain_name]

该命令用于为指定 SSL 虚拟或后台主机备份证书和私钥。执行该命令后：

- 对于 RSA 和 ECC，系统将当前使用的 RSA 证书和私钥、ECC 证书和私钥分别备份到一个 PFX 文件中；
- 对于 SM2，系统为 SM2 证书生成另外两个.tgz 文件。其中一个.tgz 文件为加密文件，包含激活和未激活的证书、私钥、受信任 CA 证书（参见命令“**ssl import rootca**”）、中级 CA 证书（参见命令“**ssl import interca**”）；另一个.tgz 文件不加密，包含激活和未激活的证书、受信任 CA 证书、中级 CA 证书和已导入的 Challenge 密钥。

系统将上述 PFX 文件、两个.tgz 文件、该 SSL 主机的 CRL 签发证书（参见命令“**ssl import crlca**”）、受信任 CA 证书和中级 CA 证书文件一起打包到一个.tgz 文件中。该.tgz 文件可以保存在系统中，也可以保存到一个指定的 TFTP 服务器上。

host_name

该参数指定 SSL 虚拟或后台主机的名称。取值必须为：

- SSL 虚拟或后台主机的名称：表示备份 SSL 虚拟或后台主机的证书和私钥。
- all：表示备份所有 SSL 虚拟主机和后台主机的证书和私钥、CA 证书、中级 CA 证书、CRL CA 证书、Challenge 密钥以及 SNI 域名的相关证书。注意：产生的备份包为加密文件，不能打开或解压。

file_name

该参数指定备份文件的名称。取值支持数字、字母和下划线，建议置于双引号内。

- 保存在系统中：取值必须为有效的系统文件名（不包括路径和扩展名）；
- 保存在 IPv4 类型的 TFTP 服务器上：取值格式必须为“tftp://server_ip/filename”。

取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。

password

该参数指定允许访问备份文件的密码。取值支持数字、字母和下划线，建议置于双引号内。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。

domain_name

可选。该参数指定与 SSL 主机关联的域名的名称。

- 如果指定了参数“domain_name”，与 SSL 虚拟主机关联域名的证书和密钥将被备份。
- 如果没有指定参数“domain_name”，SSL 主机的证书和密钥将被备份。



注意：

- 执行该命令之前，需要确保已经通过命令“**ssl activate certificate**”激活了需要备份的证书。
- 多次执行该命令备份证书和私钥文件到系统中，系统只保留最近 2 次的备份文件。
- 虚拟主机或后台主机名称的长度和关联的 SNI 域名长度的总和不能超过 220 个字符。

no ssl backup certificate <host_name> <file_name> [domain_name]

该命令用于删除指定 SSL 虚拟或后台主机保存在系统中的证书和私钥备份文件，参数“file_name”必须为有效的系统文件名。如果没有指定参数“domain_name”，指定 SSL 主机的证书和密钥备份文件的文件名将会被删除；如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的证书和密钥备份文件的文件名将会被删除。

show ssl backup certificate <host_name> [domain_name]

该命令用于显示指定 SSL 虚拟或后台主机保存在系统中的证书和私钥备份文件的文件名。如果没有指定参数“domain_name”，指定 SSL 主机的证书和密钥备份文件的文件名将会被显示；如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的证书和密钥备份文件的文件名将会被显示。

ssl restore certificate <host_name> <file_name> <password> [domain_name]

该命令用于将指定 SSL 虚拟或后台主机先前备份在系统中或者 TFTP 服务器上的.tgz 文件恢复到系统中。

host_name	该参数指定 SSL 虚拟或后台主机的名称。取值必须为： - SSL 虚拟或后台主机的名称：表示恢复 SSL 虚拟或后台主机的备份.tgz 文件。 - all：表示恢复所有 SSL 虚拟主机和后台主机的的备份.tgz 文件。
file_name	该参数指定要恢复的备份文件的名称。文件名中不支持除下划线以外的特殊字符。 - 保存在系统中：有效的本地文件名（不包括路径）； - 保存在 IPv4 类型的 TFTP 上：取值格式必须为“tftp://server_ip/filename”。
password	该参数指定访问要恢复的备份文件的密码。
domain_name	可选。该参数指定与 SSL 虚拟主机关联的域名的名称。 - 如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的证书和密钥将被恢复。 - 如果没有指定参数“domain_name”，指定 SSL 主机的证书和密钥将被恢复。



注意：

- 该命令不支持通过同步功能在设备之间同步。

- 虚拟主机或后台主机名称的长度和关联的 SNI 域名长度的总和不能超过 220 个字符。

9.3 SSL 协议版本和密码套件

ssl globals protocol virtual <version>

该命令用于为所有 SSL 虚拟主机设置全局默认 SSL 协议版本。允许设置的 SSL 协议版本包括 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3 和 SM2v1.1。如果不配置该命令，所有 SSL 虚拟主机的全局默认 SSL 协议版本为 TLSv1.2。对于装备了 FIPS HSM 的设备，所有 SSL 虚拟主机的全局默认 SSL 协议版本为 TLSv1.0。

当新创建一个 SSL 虚拟主机时，系统自动为该 SSL 虚拟主机设置 SSL 协议版本，即与所有 SSL 虚拟主机的全局默认 SSL 协议版本相同。如果需要修改该虚拟主机的 SSL 协议版本，可以使用命令“**ssl settings protocol**”。

version 该参数设置所有 SSL 虚拟主机的全局默认 SSL 协议版本。取值必须为：

- SSLv3：表示支持 SSLv3 协议版本。
- TLSv1：表示支持 TLSv1.0 协议版本。
- TLSv11：表示支持 TLSv1.1 协议版本。
- TLSv12：表示支持 TLSv1.2 协议版本。
- TLSv13：表示支持 TLSv1.3 协议版本。
- SM2v11：表示支持 SM2v1.1 协议版本。
- ALL：表示支持以上全部协议版本。

如果要配置多种版本，请使用冒号(:)来分隔协议版本。

no ssl globals protocol virtual

该命令用于将所有 SSL 虚拟主机的全局默认 SSL 协议版本设置重置为默认值。

ssl globals protocol real <version>

该命令用于为所有 SSL 后台主机设置全局默认 SSL 协议版本。允许设置的 SSL 协议版本包括 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3 和 SM2v1.1。如果不配置该命令，所有 SSL 后台主机的全局默认 SSL 协议版本为 TLSv1.0、TLSv1.1 和 TLSv1.2。对于装备了 FIPS HSM 的设备，SSL 后台主机的全局默认 SSL 协议版本为 TLSv1.0。

当新创建一个 SSL 后台主机时,系统自动为该 SSL 后台主机设置 SSL 协议版本,即与所有 SSL 后台主机全局默认 SSL 协议版本相同。如果需要修改该后台主机的 SSL 协议版本,可以使用命令“**ssl settings protocol**”。

version 该参数设置所有 SSL 后台主机全局默认 SSL 协议版本。取值必须为:

- **SSLv3**: 表示支持 SSLv3 协议版本。
- **TLSv1**: 表示支持 TLSv1.0 协议版本。
- **TLSv11**: 表示支持 TLSv1.1 协议版本。
- **TLSv12**: 表示支持 TLSv1.2 协议版本。
- **TLSv13**: 表示支持 TLSv1.3 协议版本。
- **SM2v11**: 表示支持 SM2v1.1 协议版本。
- **ALL**: 表示支持以上除 SM2v1.1 以外的全部协议版本。

如果要配置多种版本,请使用冒号(:)来分隔协议版本

注意,后台主机不支持同时配置 SSL/TLS 和 SM2v1.1 协议。

no ssl globals protocol real

该命令用于将所有 SSL 后台主机全局默认 SSL 协议版本设置重置为默认值。

ssl settings protocol <host_name> <version>

该命令用于为指定的 SSL 虚拟主机或者 SSL 后台主机设置支持的 SSL 协议版本。允许设置的 SSL 协议版本包括 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3 和 SM2v1.1。如果不配置该命令,所有 SSL 虚拟主机和 SSL 后台主机分别使用其全局默认的 SSL 协议版本。

对于装备了 FIPS HSM 的设备,SSL 虚拟主机和后台主机支持 SSLv3 和 TLSv1 两种版本。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

version 该参数设置 SSL 虚拟主机或后台主机支持的 SSL 协议版本。取值必须为:

- **SSLv3**: 表示该主机支持 SSLv3 协议版本。
- **TLSv1**: 表示该主机支持 TLSv1.0 协议版本。
- **TLSv11**: 表示该主机支持 TLSv1.1 协议版本。

- TLSv12: 表示该主机支持 TLSv1.2 协议版本。
- TLSv13: 表示该主机支持 TLSv1.3 协议版本。
- SM2v11: 表示该主机支持 SM2v1.1 协议版本。
- ALL: 当“host_name”设置为虚拟主机时, 表示支持以上全部协议版本; 设置为后台主机时, 表示支持以上除 SM2v11 以外的全部协议版本。

如果要配置多种版本, 请使用冒号(:)来分隔协议版本。

注意, 后台主机不支持同时配置 SSL/TLS 和 SM2v1.1 协议。

例如:

```
Demo(config)#ssl settings protocol rhost1 SSLv3
Demo(config)#ssl settings protocol vhost1 SSLv3:TLSv12
Demo(config)#ssl settings protocol vhost2 ALL
```

ssl settings fallbackscsv <virtual_host_name>

该命令用于为指定 SSL 虚拟主机启用 TLS Fallback SCSV (Signaling Cipher Suite Value) 功能, 来防止协议降级攻击。

启用该功能后, 当客户端使用的密码套件携带了 TLS_FALLBACK_SCSV 选项时, 设备会检查客户端使用的 SSL 协议版本是否低于虚拟主机支持的最高协议版本。如果低于, 则回复 86 号错误, 关闭连接。

禁用该功能后, 只要客户端使用的 SSL 协议版本在虚拟主机所支持的版本范围内, 就会继续 SSL 握手。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

no ssl settings fallbackscsv <virtual_host_name>

该命令用于为指定 SSL 虚拟主机禁用 TLS Fallback SCSV 功能。

ssl settings ciphersuite <host_name> <cipher_string>

该命令用于为指定的 SSL 虚拟主机或者 SSL 后台主机设置支持的密码套件。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

cipher_string 该参数指定 SSL 虚拟主机或后台主机支持的密码套件, 取值不区分大小写。如果要配置两种或两种以上密码套件, 请使用冒号(:)来分隔密码套件。

对于装备了 FIPS HSM 的设备，SSL 虚拟主机和后台主机支持的密码套件为“DES-CBC3-SHA:AES128-SHA:AES256-SHA:!SSLv2”。

对于未装备 FIPS HSM 的设备，密码套件的支持情况请参见以下表格。表格中，“Y”表示支持该密码套件；“N”表示不支持该密码套件。

- 不同协议版本虚拟主机对密码套件的支持情况

表9 - 1 不同协议版本虚拟主机对密码套件的支持情况

密码套件	位数	SSL 协议 – 虚拟主机					
		SSLv3.0	TLSv1	TLSv1.1	TLSv1.2	TLSv1.3	SM2v1.1
RC4-MD5	128	Y	Y	Y	Y	N	N
RC4-SHA	128	Y	Y	Y	Y	N	N
DES-CBC-SHA	64	Y	Y	Y	N	N	N
DES-CBC3-SHA	192	Y	Y	Y	Y	N	N
AES128-SHA	128	Y	Y	Y	Y	N	N
AES256-SHA	256	Y	Y	Y	Y	N	N
AES128-SHA256	128	N	N	N	Y	N	N
AES256-SHA256	256	N	N	N	Y	N	N
AES128-GCM-SHA256	128	N	N	N	Y	N	N
AES256-GCM-SHA384	256	N	N	N	Y	N	N
ECDHE-RSA-AES128-SHA	128	Y	Y	Y	Y	N	N
ECDHE-RSA-AES256-SHA	256	Y	Y	Y	Y	N	N
ECDHE-ECDSA-AES128-SHA	128	Y	Y	Y	Y	N	N
ECDHE-ECDSA-AES256-SHA	256	Y	Y	Y	Y	N	N
ECDHE-RSA-AES128-SHA256	128	N	N	N	Y	N	N
ECDHE-RSA-AES256-SHA384	256	N	N	N	Y	N	N
ECDHE-RSA-AES128-GCM-SHA256	128	N	N	N	Y	N	N
ECDHE-RSA-AES256-GCM-SHA384	256	N	N	N	Y	N	N
ECDHE-ECDSA-AES128-SHA256	128	N	N	N	Y	N	N

密码套件	位数	SSL 协议 – 虚拟主机					
		SSLv3.0	TLSv1	TLSv1.1	TLSv1.2	TLSv1.3	SM2v1.1
ECDHE-ECDSA-AES256-SHA384	256	N	N	N	Y	N	N
ECDHE-ECDSA-AES128-GCM-SHA256	128	N	N	N	Y	N	N
ECDHE-ECDSA-AES256-GCM-SHA384	256	N	N	N	Y	N	N
TLS-AES128-GCM-SHA256	128	N	N	N	N	Y	N
TLS-AES256-GCM-SHA384	256	N	N	N	N	Y	N
ECDHE-SM4-SM3	128	N	N	N	N	N	Y
ECC-SM4-SM3	128	N	N	N	N	N	Y
ECDHE-SM4-GCM-SM3	128	N	N	N	N	N	Y
ECC-SM4-GCM-SM3	128	N	N	N	N	N	Y

- 不同协议版本后台主机对密码套件的支持情况

表9 - 2 不同协议版本后台主机对密码套件的支持情况

密码套件	位数	SSL 协议 – 后台主机					
		SSLv3.0	TLSv1.0	TLSv1.1	TLSv1.2	TLSv1.3	SM2v1.1
RC4-MD5	128	Y	Y	Y	Y	N	N
RC4-SHA	128	Y	Y	Y	Y	N	N
DES-CBC-SHA	64	N	N	N	N	N	N
DES-CBC3-SHA	192	Y	Y	Y	Y	N	N
AES128-SHA	128	Y	Y	Y	Y	N	N
AES256-SHA	256	Y	Y	Y	Y	N	N
AES128-SHA256	128	N	N	N	Y	N	N
AES256-SHA256	256	N	N	N	Y	N	N
AES128-GCM-SHA256	128	N	N	N	Y	N	N
AES256-GCM-SHA256	256	N	N	N	Y	N	N

密码套件	位数	SSL 协议 – 后台主机					
		SSLv3.0	TLSv1.0	TLSv1.1	TLSv1.2	TLSv1.3	SM2v1.1
HA384							
ECDHE-RSA-AES128-SHA	128	Y	Y	Y	Y	N	N
ECDHE-RSA-AES256-SHA	256	Y	Y	Y	Y	N	N
ECDHE-ECDSA-AES128-SHA	128	Y	Y	Y	Y	N	N
ECDHE-ECDSA-AES256-SHA	256	Y	Y	Y	Y	N	N
ECDHE-RSA-AES128-SHA256	128	N	N	N	Y	N	N
ECDHE-RSA-AES256-SHA384	256	N	N	N	Y	N	N
ECDHE-RSA-AES128-GCM-SHA256	128	N	N	N	Y	N	N
ECDHE-RSA-AES256-GCM-SHA384	256	N	N	N	Y	N	N
ECDHE-ECDSA-AES128-SHA256	128	N	N	N	Y	N	N
ECDHE-ECDSA-AES256-SHA384	256	N	N	N	Y	N	N
ECDHE-ECDSA-AES128-GCM-SHA256	128	N	N	N	Y	N	N
ECDHE-ECDSA-AES256-GCM-SHA384	256	N	N	N	Y	N	N
TLS-AES128-GCM-SHA256	128	N	N	N	N	Y	N
TLS-AES256-GCM-SHA384	256	N	N	N	N	Y	N
ECC-SM4-SM3	128	N	N	N	N	N	Y
ECDHE-SM4-SM3	128	N	N	N	N	N	Y
ECDHE-SM4-GCM-SM3	128	N	N	N	N	N	Y

密码套件	位数	SSL 协议 – 后台主机					
		SSLv3.0	TLSv1.0	TLSv1.1	TLSv1.2	TLSv1.3	SM2v1.1
ECC-SM4-GCM-SM3	128	N	N	N	N	N	Y

对于以上表格信息，管理员应该注意以下几点：

- “ECDHE-ECDSA...” 密码套件仅用于 ECC 证书，“ECDHE-RSA...” 密码套件仅用于 RSA 证书，“ECC-SM4-SM3”、“ECDHE-SM4-SM3”、“ECDHE-SM4-GCM-SM3” 和 “ECC-SM4-GCM-SM3” 仅用于 SM2 证书。
- 当密码套件采用 “EXP-RC4-MD5” 或 “EXP-DES-CBC-SHA” 时，系统仅支持长度不大于 512 位的密钥。
- 当 HTTP 的协议版本为 HTTP/2 时，设置的密码套件必须包含以下四种密码套件中的一种或多种。否则，在 TLS 握手过程中，后台服务将不会发送 ALPN 扩展，导致客户端和后台服务器无法执行 HTTP/2 协商，从而导致 HTTP/2 不生效。但是虚拟服务仍会接收 HTTP/2 的连接请求。
 - ECDHE-RSA-AES128-GCM-SHA256
 - ECDHE-RSA-AES256-GCM-SHA384
 - ECDHE-ECDSA-AES128-GCM-SHA256
 - ECDHE-ECDSA-AES256-GCM-SHA384。
- 后台主机不支持同时配置 SM2 密码套件和 SSL/TLS 密码套件。



注意：建议有经验的管理员使用该命令。如果对这些设置有任何疑问，请在使用命令之前致电公司技术支持。

9.4 签名算法和椭圆曲线

ssl settings signalgo <host_name> <signature_algorithm>

该命令用于为指定的 SSL 主机设置 Server Key Exchange 消息支持的签名算法（仅用于 TLSv1.3 之前的 SSL 协议版本）。如不配置该命令，所有 SSL 主机使用默认设置

“sha256ECDSA:sha256RSA:sha384ECDSA:sha384RSA:sha512ECDSA:sha512RSA:sha224ECDSA:sha224RSA:sha1ECDSA:sha1RSA”（按照优先级由高到低排列）。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

signature_algorithm 该参数指定 Server Key Exchange 消息支持的签名算法，取值必须为 sha256ECDSA、sha256RSA、sha384ECDSA、sha384RSA、sha512ECDSA、sha512RSA、sha224ECDSA、

sha224RSA、sha1ECDSA 或 sha1RSA。如果要配置两种或两种以上签名算法，请使用冒号（:）来分隔。



注意：只配置了 SM2 类型密码套件的 SM2v1.1 后台主机不支持配置该命令。

ssl settings clientcert signalgo <virtual_host_name> <signature_algorithm>

该命令用于为指定的 SSL 虚拟主机设置客户端证书请求消息支持的签名算法（仅用于 TLSv1.3 之前的版本）。如不配置该命令，所有 SSL 主机使用默认设置

“sha256ECDSA:sha256RSA:sha384ECDSA:sha384RSA:sha512ECDSA:sha512RSA:sha224ECDSA:sha224RSA:sha1ECDSA:sha1RSA”（按照优先级由高到低排列）。

host_name

该参数指定 SSL 虚拟主机的名称。

signature_algorithm

该参数指定 SSL 虚拟主机支持的签名算法，取值必须为 sha256ECDSA、sha256RSA、sha384ECDSA、sha384RSA、sha512ECDSA、sha512RSA、sha224ECDSA、sha224RSA、sha1ECDSA 或 sha1RSA。如果要配置两种或两种以上签名算法，请使用冒号（:）来分隔。



注意：

- 当虚拟主机运行的协议版本为 SSLv3、TLSv1 或 TLSv1.1 时，设置的签名算法里必须包含 sha1RSA 或 sha1ECDSA，否则 SSL 握手会失败。
- 如果设置 sha512RSA 为首选签名算法，使用 512 位 RSA 秘钥的客户端会因为无法完成客户端认证而重置连接。

ssl settings curves <host_name> <elliptic_curve>

该命令用于为指定的 SSL 主机设置 Server Key Exchange 消息支持的椭圆曲线。如不配置该命令，所有 SSL 主机使用默认设置 “secp256r1:secp384r1:secp521r1”（按照优先级由高到低排列）。

host_name

该参数指定 SSL 虚拟主机或后台主机的名称。

elliptic_curve

该参数指定 Server Key Exchange 消息支持的椭圆曲线名称，取值必须为 secp256r1、secp384r1 或 secp521r1。如果要配置两种或两种以上椭圆曲线，请使用冒号（:）来分隔。



注意：只配置了 SM2 类型密码套件的 SM2v1.1 后台主机不支持配置该命令。

9.5 TLSv1.3 特性选项

ssl settings tlsv13 signalgo certrequest <virtual_host_name>
<signature_algorithm>

该命令用于为指定的 SSL 虚拟主机设置证书请求支持的 TLSv1.3 签名算法。当不配置该命令时，系统默认支持的签名算法为 ecdsa:rsae:rsapss，分别对应 ECDSA、RSAE 和 RSAPSS。

- ECDSA：包括 ecdsa_secp256r1_sha256、ecdsa_secp384r1_sha384 和 ecdsa_secp521r1_sha512。
- RSAE：包括 rsa_pss_rsae_sha256、rsa_pss_rsae_sha384 和 rsa_pss_rsae_sha512。
- RSAPSS：包括 rsa_pss_pss_sha256、rsa_pss_pss_sha384 和 rsa_pss_pss_sha512。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

signature_algorithm 该参数指定签名算法，取值必须为“ecdsa”、“rsae”或“rsapss”。如果要设置多个签名算法，请使用冒号（:）分隔。

ssl settings tlsv13 signalgo certverify <host_name> <signature_algorithm>

该命令用于为指定的 SSL 主机设置证书验证支持的 TLSv1.3 签名算法。当不配置该命令时，系统默认支持的签名算法为 ecdsa:rsae:rsapss，分别对应 ECDSA、RSAE 和 RSAPSS。

- ECDSA：包括 ecdsa_secp256r1_sha256、ecdsa_secp384r1_sha384 和 ecdsa_secp521r1_sha512。
- RSAE：包括 rsa_pss_rsae_sha256、rsa_pss_rsae_sha384 和 rsa_pss_rsae_sha512。
- RSAPSS：包括 rsa_pss_pss_sha256、rsa_pss_pss_sha384 和 rsa_pss_pss_sha512。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

signature_algorithm 该参数指定签名算法，取值必须为“ecdsa”、“rsae”或“rsapss”。如果要设置多个签名算法，请使用冒号（:）分隔。



注意：后台主机不支持与 TLSv1.2 版本的 SSL 服务器协商 RSAPSS 签名算法。

ssl settings tlsv13 earlydata <host_name>

该命令用于为指定的 SSL 主机启用 TLSv1.3 0-RTT（zero round-trip time）模式。默认设置为启用。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

no ssl settings tlsv13 earlydata <host_name>

该命令用于为指定的 SSL 主机禁用 TLSv1.3 0-RTT 模式。

ssl settings tlsv13 earlydatasize <virtual_host_name> <size>

该命令用于设置指定 SSL 虚拟主机支持的 early data 长度上限。当不配置该命令时，默认的 early data 长度上限是 1024 字节。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

size 该参数指定 early data 的长度上限，取值必须为 1 至 16384 之间的整数。

ssl settings tlsv13 ticketlifetime <virtual_host_name> <lifetime>

该命令用于为指定的虚拟主机设置 NewSessionTicket 消息的令牌有效期。当不配置该命令时，默认的令牌有效期是 7200 秒。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

lifetime 该参数指定令牌有效期，取值必须为 60 至 604800 之间的整数。

ssl settings tlsv13 psk mode <real_host_name> <ke_mode>

该命令用于为指定的 SSL 后台主机设置 TLSv1.3 PSK 交换模式。支持的 PSK 交换模式包括“psk_dhe_ke”和“psk_ke:psk_dhe_ke”。默认为“psk_ke:psk_dhe_ke”。

real_host_name 该参数指定 SSL 后台主机的名称。

ke_mode 该参数指定 TLSv1.3 PSK 交换模式，取值必须为“psk_dhe_ke”或“psk_ke:psk_dhe_ke”。

9.6 客户端认证

ssl settings clientauth <host_name>

该命令用于为指定 SSL 虚拟主机或者 SSL 后台主机启用客户端认证功能。客户端认证功能需为每个 SSL 虚拟主机或后台主机单独启用。该功能默认对每个 SSL 虚拟主机和后台主机是禁用的。

- 为 SSL 虚拟主机启用客户端认证功能后，SSL 虚拟主机将在 SSL 握手过程中发送证书请求给客户端，并对客户端证书进行校验，连接到该虚拟主机的所有 SSL 客户端必须提供证书才能与 SSL 虚拟主机继续通信。
- 为 SSL 后台主机启用客户端认证功能后，SSL 后台主机将在 SSL 握手过程中收到 SSL 后台服务器发来的证书请求时，将证书发送给 SSL 后台服务器。

host_name 该参数指定 SSL 虚拟或后台主机的名称。



注意：

- 当为 SSL 虚拟主机启用 SSL 客户端认证功能时，设备可以将接收到的客户端证书字段通过 HTTP header 或者 HTTP cookie 转发到后台服务器。具体配置方法请参见第 10 章 HTTPS 转发控制小节。
- 对于使用 TLSv1.2 协议和 RSA 密码套件的虚拟主机，如果启用客户端认证功能，那么当客户端的 Certificate Verify 消息中指定 SHA224 作为哈希算法时，SSL 连接会失败。
- 当为虚拟主机配置了密码套件 ECDHE-SM4-SM3 和 ECDHE-SM4-GCM-SM3 时，即使为 SSL 虚拟主机禁用客户端认证，SSL 虚拟主机进行 SSL 握手时仍会进行 SSL 双向认证。

no ssl settings clientauth <host_name>

该命令用于为 SSL 虚拟主机或者 SSL 后台主机禁用客户端认证功能。

ssl settings certfilter <virtual_host_name> <condition_1> [condition_2]

该命令用于为指定 SSL 虚拟主机上的客户端认证功能配置证书过滤规则。

证书过滤规则对 SSL 虚拟主机是可选配置的。一个 SSL 虚拟主机最多支持 1024 条证书过滤规则，它们之间为逻辑“或”关系。如果为 SSL 虚拟主机配置了证书过滤规则并且启用了客户端认证功能，客户端证书必须匹配到一条证书过滤规则；否则 SSL 虚拟主机将拒绝客户端访问。

一个证书过滤规则中包含至少一个匹配条件，至多两个匹配条件，匹配条件是基于客户端证书的“Subject”或“Issuer”字段配置的过滤字符串。即使该字段只有部分匹配过滤字符串，也认为命中了规则。如果一个证书过滤规则包含了两个过滤字符串，那么客户端证书只有同时匹配两个过滤字符串才能匹配该证书过滤规则。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

condition_1 该参数定义一条基于“Subject”或“Issuer”字段的过滤字符串。取值必须为长度不大于 63 字节的字符串，区分大小写，必须置于双引号内，格式为
“subject:/C=US”或“issuer:/C=US”。过滤字符串可以包含多个过滤关键字，以“/”符号分隔，例如
“subject:/C=US/OU=example”。这些过滤关键字之间

是逻辑“与”关系。

过滤字符串里还可以包含转换成 Unicode 编码的中文字符。Unicode 字符串必须为小写,而且必须添加前缀“%u”用于和英文字符区分,例如
“subject:/CN=%u4f60%u597d”。

condition_2 可选,该参数定义第二条基于“Subject”或“Issuer”字段的过滤字符串。配置方法同“condition_1”参数。

设备上支持配置基于“Subject”或“Issuer”字段的所有 RDN(Relative Distinguished Name, 相对唯一标识名或)或其对应 OID 的过滤关键字,如下表所示:

表9 - 3 过滤关键字

RDN	标准名称	OID
C	国家 (Country)	2.5.4.6
ST	省份 (State Or Province)	2.5.4.8
L	城市 (Locality)	2.5.4.7
O	组织 (Organization)	2.5.4.10
OU	组织单位 (Organization Unit)	2.5.4.11
CN	常用名 (Common Name)	2.5.4.3
serialNumber	序号 (Serial Number)	2.5.4.5
dnQualifier	DN 限定符 (DN Qualifier)	2.5.4.46
pseudonym	别名 (Pseudonym)	2.5.4.65
title	标题 (Title)	2.5.4.12
generationQualifier	产生限定符 (Generation Qualifier)	2.5.4.44
initials	姓名起首字母 (Initials)	2.5.4.43
name	名称 (Name)	2.5.4.41
givenName	名 (Given Name)	2.5.4.42
surname	姓 (Surname)	2.5.4.4
UID	用户 ID (User ID)	0.9.2342.19200300.100.1.1
DC	域组件 (Domain Component)	0.9.2342.19200300.100.1.25
emailAddress	邮件地址 (Email Address)	1.2.840.113549.1.9.1
{OID expression}	OID 信息; 例如: 1.2.3.4	

例如:

```
Demo(config)#ssl settings certfilter vhost
"subject:/C=CN/O=Enterprise/OU=QA/emailAddress=admin@mailserver.com"
"issuer:/C=CN"
```

在本例中, 只有当客户端证书同时满足以下两个条件, 才能通过校验:

- “Subject” 字段中, “C” 为 “CN”, “O” 为 “Enterprise”, “OU” 为 “QA”, “emailAddress” 为 “admin@mailserver.com”。

- “Issuer” 字段中，“C” 为 “CN”。

```
Demo(config)#ssl settings certfilter vhost "subject:/2.5.4.6=JP"
```

在本例中，“subject:/2.5.4.6” 代表 “Subject” 字段中的 “国家（Country）”。执行这条命令后，只有 “Subject” 字段包含 OID “2.5.4.6” 且其取值为 “JP” 的客户端证书才能通过校验。



注意：在执行命令 “ssl settings clientauth” 和 “ssl settings certfilter” 之前，要确保相关 SSL 虚拟主机状态为禁用的，否则无法执行命令。如果 SSL 虚拟主机状态为启用的，可以使用命令 “ssl stop <host_name>” 禁用该 SSL 虚拟主机。

no ssl settings certfilter <virtual_host_name> <condition_1> [condition_2]

该命令用于为指定 SSL 虚拟主机上的客户端认证功能删除证书过滤规则。

ssl settings ocsp <virtual_host_name> <ocsp_server_url>

该命令用于为指定 SSL 虚拟主机配置 OCSP 服务器。如果为 SSL 虚拟主机配置了 OCSP 服务器，系统将为该 SSL 虚拟主机启用 OCSP 证书吊销检查功能。本配置对 SSL 虚拟主机是可选的。当为 SSL 虚拟主机配置本命令并且启用了客户端认证功能时，SSL 虚拟主机可以作为 OCSP 客户端，通过与 OCSP 服务器通信来查询证书是否被吊销。

SSL 虚拟主机接收到客户端发来的证书后，首先通过客户端证书中指定的 OCSP 服务器在线检查证书是否吊销。若 OCSP 服务器未返回 “良好” 或 “已撤销” 响应，SSL 虚拟主机将会通过本命令中配置的 OCSP 服务器再次检查证书是否吊销。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

ocsp_server_url 该参数指定 OCSP 服务器的 URL 地址。取值必须以 “http://” 或 “https://” 开头。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。



注意：

1. 如果为 SSL 虚拟主机同时启用了 OCSP 证书吊销检查和下文中将会提到的 CRL 在线/离线证书吊销检查功能，则只有 OCSP 证书吊销检查会生效。
2. 使用 OCSP 功能时，虚拟主机必须导入客户端证书的受信任 CA 证书。

no ssl settings ocsp <virtual_host_name>

该命令用于为指定 SSL 虚拟主机禁用 OCSP 证书吊销检查功能。

ssl settings ocspstapling <virtual_host_name>

该命令用于为指定的 SSL 虚拟主机启用 OCSP Stapling 功能。该功能的默认设置为对所有 SSL 虚拟主机禁用。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机的名称。



注意：

1. SSL 虚拟主机的 OCSP Stapling 功能不支持 RFC 6961 定义的 Multiple Certificate Status Request 扩展。
2. 如果 SSL 虚拟主机存在证书链，那么必须先导入中级 CA 证书后才能支持 OCSP Stapling 功能。
3. 证书中不包含 OCSP 扩展的 SSL 虚拟主机不支持 OCSP Stapling 功能。
4. 运行 SM2 协议的 SSL 虚拟主机不支持 OCSP Stapling 功能。
5. SSL 虚拟主机的 OCSP Stapling 功能不支持 IPv6。
6. SSL 虚拟主机的 OCSP Stapling 功能不支持 TLSv1.3 协议。
7. 系统只支持基于 HTTP 协议的 OCSP。
8. 对于包含“nextupdate”的 OCSP 响应，系统会根据“nextupdate”的时间确定是否向 OCSP 响应器发送请求。如果响应不包含“nextupdate”信息，系统不会向 OCSP 响应器发送请求。

no ssl settings ocspsapling <virtual_host_name>

该命令用于为指定的 SSL 虚拟主机禁用 OCSP Stapling 功能。

show ssl status ocspsapling <virtual_host_name> [domain_name]

该命令用于显示与指定的 SSL 虚拟主机关联的指定域名是否开启了 OCSP Stapling 功能及相关的状态信息。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机的名称。

domain_name 可选。该参数指定与虚拟主机关联的域名。

- 如果指定参数“domain_name”，将会显示指定的 SSL 虚拟主机关联的指定域名是否开启了 OCSP Stapling 功能及相关的状态信息。
- 如果没有指定参数“domain_name”，将会显示指定的 SSL 虚拟主机是否开启了 OCSP Stapling 功能及相关的状态信息。

ssl import clientkey [virtual_host_name] [clientkey_url]

该命令用于为指定 SSL 虚拟主机导入 SSL 客户端私钥，用于同其它服务器进行 SSL 通信，例如 OCSP 或 LDAP（Lightweight Directory Access Protocol）服务器。

virtual_host_name 可选，该参数指定 SSL 虚拟主机的名称。取值必须为：

- SSL 虚拟主机的名称：表示为指定 SSL 虚拟主机导

入 SSL 客户端私钥。

- ALL: 表示为所有的 SSL 虚拟主机导入 SSL 客户端私钥。

默认值为“ALL”。

clientkey_url

可选, 该参数指定 SSL 客户端私钥在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值的最大长度受 CLI 支持的命令行最大长度限制, 目前 CLI 最多支持 1024 个字节的命令行。如果不指定该参数, 需要手动粘贴 SSL 客户端私钥到 CLI。

默认值为空。

no ssl clientkey <virtual_host_name>

该命令用于删除指定 SSL 虚拟主机的 SSL 客户端私钥。

virtual_host_name

该参数指定 SSL 虚拟主机的名称。取值必须为:

- SSL 虚拟主机的名称: 表示删除导入时即被指定给特定 SSL 虚拟主机的 SSL 客户端私钥。
- ALL: 表示删除导入时即被指定给所有 SSL 虚拟主机的 SSL 客户端私钥。

ssl import clientcert [virtual_host_name] [clientcert_url]

该命令用于为指定 SSL 虚拟主机导入与其它服务器 (例如 OCSP 或 LDAP 服务器) 进行 SSL 通信时使用的 SSL 客户端证书。

virtual_host_name

可选, 该参数指定 SSL 虚拟主机的名称。取值必须为:

- SSL 虚拟主机的名称: 表示为指定 SSL 虚拟主机导入 SSL 客户端证书。
- ALL: 表示为所有的 SSL 虚拟主机导入 SSL 客户端证书。

默认值为“ALL”。

clientcert_url

可选, 该参数指定 SSL 客户端证书在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值的最大长度受 CLI 支持的命令行最大长度限制, 目前 CLI 最多支持 1024 个字节的命令行。如不指定该参数, 用户需手动粘贴 SSL 客户端证书到 CLI。

默认值为空。

no ssl clientcert <virtual_host_name>

该命令用于删除指定 SSL 虚拟主机的 SSL 客户端证书。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。取值必须为：

- SSL 虚拟主机的名称：表示删除为特定 SSL 虚拟主机导入的 SSL 客户端证书。
- ALL：表示删除为所有 SSL 虚拟主机导入的 SSL 客户端证书。

show ssl clientcert <virtual_host_name> [display_mode]

该命令用于显示指定 SSL 虚拟主机的 SSL 客户端证书。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

display_mode 可选，该参数指定 SSL 客户端证书的显示模式。取值必须为：

- complete：表示系统将显示 SSL 客户端证书的全部内容。
- simple：表示系统将只显示 SSL 客户端证书的字段“Issuer”，“Validity”和“Subject”。

默认值为“complete”。

ssl settings crl online <virtual_host_name>

该命令用于为指定 SSL 虚拟主机启用 CRL 在线证书吊销检查功能。启用该功能后，SSL 虚拟主机从收到客户端证书中指定的 CDP（CRL Distribution Point，CRL 分发点）在线下载 CRL 文件来检查客户端证书是否吊销。该命令只能在为 SSL 虚拟主机启用了客户端认证功能后才能设置。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

no ssl settings crl online <virtual_host_name>

该命令用于为指定 SSL 虚拟主机禁用 CRL 在线证书吊销检查功能。

ssl import crlca [host_name] [domain_name] [tftp_ip|url] [file_name]

该命令用于为指定 SSL 虚拟主机或后台主机或全局 CRL（Certificate Revocation List，证书撤销列表）签发证书列表导入一个 CRL 签发证书。

SSL 虚拟主机接收到客户端发来的证书后，将通过下载 CA 定期签发的 CRL 文件来检查此客户端证书是否已被吊销。SSL 后台主机接收到服务器证书后，将通

过下载 CA 定期签发的 CRL 文件来检查此服务器证书是否已被吊销。CRL 签发证书用来验证为 CRL 离线证书吊销检查功能下载的 CRL 文件是否有效。

当采用 copy-n-paste 方式导入 CRL 签发证书时，只需要运行该命令“**ssl import *crlca***”，并将 CRL 签发证书的内容复制粘贴到 CLI 命令行中即可，该方式仅支持导入 PEM 格式的证书。该命令还支持通过 TFTP、FTP、SFTP、HTTP、HTTPS 和 SCP 方式导入 PEM 和 DER 格式的 CRL 签发证书。

host_name 可选，该参数指定 SSL 虚拟主机或后台主机的名称。取值必须为：

- **SSL 虚拟主机或后台主机的名称**：表示将 CRL 签发证书导入 SSL 虚拟主机或后台主机，用于校验为该主机下载的 CRL 文件。
- **ALL**：表示将 CRL 签发证书加入全局 CRL 签发证书列表，用于校验为全局下载的 CRL 文件。

默认值为“ALL”。

domain_name 可选。该参数指定域名的名称。

- 如果指定参数“**domain_name**”，将会为与 SSL 虚拟主机关联的域名导入 CRL CA 证书。
- 如果没有指定参数“**domain_name**”，将会为 SSL 虚拟主机导入 CRL CA 证书。

默认值为空。

注意：如果需要通过 URL 方式（即“**tftp_ip|url**”参数值为 URL）为 SSL 虚拟或后台主机导入 CRL 签发证书，该参数取值应为“”。

tftp_ip|url 可选，该参数指定 CRL 签发证书的 TFTP 服务器的 IP 地址或 URL 地址。

- “**tftp_ip**”用于配置 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。使用 TFTP 方式导入 CRL 签发证书时才需要设置该参数。
- “**url**”用于配置证书文件在 FTP、SFTP、TFTP、HTTP、HTTPS 或 SCP 服务器的 URL 地址。取值必须置于双引号内。使用 URL 方式导入 CRL 签发证书时才需要设置该参数。

默认值为空。

file_name 可选，该参数指定 TFTP 服务器上的 CRL 签发证书的文件名。取值的最大长度受 CLI 支持的命令行最大长度限

制，目前 CLI 最多支持 1024 个字节的命令行。

- 为 SSL 主机导入 CRL 签发证书时，默认值为“<host_name>.crt”。
- 为全局 CRL 签发证书列表导入 CRL 签发证书时，默认值为“gcrca.crt”。

使用 TFTP 方式导入 CRL 签发证书时，即参数“tftp_ip|url”取值为 TFTP 服务器的 IP 地址时，才需要设置该参数。



注意：系统只能使用与 CRL CA 证书和客户端证书签发者相同的 CRL 文件来检查客户端或服务器证书是否被吊销。如果下载的 CRL 文件的签发者与 CRL CA 证书和客户端或服务器证书签发者不同，那么该 CRL 文件在客户端或服务器认证中被忽略。

no ssl crlca <host_name> [certificate_number]

该命令用于删除指定 SSL 虚拟主机或后台主机或全局 CRL 签发证书列表中的一个 CRL 签发证书。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。取值必须为：

- SSL 虚拟主机或后台主机的名称：表示删除指定 SSL 虚拟主机或后台主机的 CRL 签发证书。
- ALL：表示删除全局 CRL 签发证书列表中的 CRL 签发证书。

certificate_number 可选，该参数指定要删除的 CRL 签发证书的序号。证书对应的序号可以通过命令“**show ssl crlca**”查看。默认值为空，表示删除所有的 CRL 签发证书。

show ssl crlca [host_name] [display_mode] [domain_name]

该命令用于显示指定 SSL 虚拟主机或后台主机或全局 CRL 签发证书列表中的所有 CRL 签发证书。

host_name 可选，该参数指定 SSL 虚拟主机或后台主机的名称。取值必须为：

- SSL 虚拟主机或后台主机的名称：表示系统将显示指定 SSL 虚拟主机或后台主机的所有 CRL 签发证书。
- ALL：表示系统将显示全局 CRL 签发证书列表中的全部 CRL 签发证书。

默认值为“ALL”。

display_mode 可选，该参数指定 CRL 签发证书的显示模式。取值必须为：

- **complete**: 表示系统将显示 CRL 签发证书的全部内容。
- **simple**: 表示系统将只显示 CRL 签发证书的字段“Issuer”，“Validity”和“Subject”。

默认值为“complete”。

domain_name 可选。该参数指定域名的名称。

- 如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的 CRL CA 证书将会被显示。
- 如果没有指定参数“domain_name”，指定 SSL 虚拟主机的 CRL CA 证书将会被显示。

no ssl sni crlca <host_name> [domain_name] [certificate_index]

该命令用于删除与指定的 SSL 虚拟主机或后台主机的特定域名的一个 CRL CA 证书。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

domain_name 可选。该参数指定域名的名称。如果没有指定参数“domain_name”，指定 SSL 虚拟主机的每个域名的所有 CRL CA 证书将会被删除。

certificate_index 可选。该参数指定要删除的 CRL CA 证书的索引。CRL CA 证书对应的索引可以通过命令“**show ssl crlca**”查看。

ssl settings crl offline <host_name> <cdp_name> <cdp_url> [domain_name] [time_interval] [delay_time] [tls_flag]

该命令用于为指定 SSL 虚拟主机或后台主机配置 CDP 及其 CRL 文件下载规则。当为 SSL 主机配置了 CDP，系统将为 SSL 主机启用 CRL 离线证书吊销检查功能。

SSL 虚拟主机按照 CRL 文件下载规则设定的时间间隔从配置的 CDP 下载 CRL 文件，使用已下载到本地的最新 CRL 文件来检查客户端证书是否已被吊销。SSL 后台主机使用下载的 CRL 文件校验收到的服务器证书。

系统支持通过 HTTP、FTP 和 LDAP 三种协议下载 CRL 文件。对每个 SSL 主机，最多可以配置 10 个 CDP。

对于 SSL 虚拟主机，该命令只能在为 SSL 虚拟主机启用了客户端认证功能后才能设置。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
cdp_name	该参数指定 CDP 的名称。取值必须为长度不大于 31 个字节的字符串。支持数字、字母和下划线，不能为“all”或“ALL”。
cdp_url	该参数指定下载 CRL 文件的 HTTP、FTP 或 LDAP URL 地址。取值必须为长度不大于 1022 个字节的字符串。
domain_name	可选。该参数指定域名的名称。 • 如果指定参数“domain_name”，与指定 SSL 虚拟主机关联的域名的 CRL 将被下载。 • 如果没有指定参数“domain_name”，指定 SSL 虚拟主机的 CRL 将被下载。
time_interval	可选，该参数指定下载 CRL 文件的时间间隔，单位为分钟。取值必须为 1 到 2,147,483,647 之间的整数。默认值为 1440。
delay_time	可选，该参数指定下载的 CRL 文件的延迟到期时间，单位为分钟。取值必须为 0 到 2,147,483,647 之间的整数。默认值为 0。 • 该参数取值大于 0 时，系统在下载 CRL 文件后检查 CRL 文件是否过期。如果当前时间已晚于 CRL 文件内包含的下次更新时间（也就是此文件到期时间）与延迟到期时间之和，那么此 CRL 文件过期，系统将拒绝所有需要通过这个 CRL 文件验证客户端证书的 SSL 连接；如果当前时间未晚于下次更新时间与延迟到期时间之和，CRL 文件即是有效的。 • 该参数取值为默认值 0 时，系统在下载 CRL 文件后不检查 CRL 文件是否过期。
tls_flag	可选。该参数指定是否使用 TLS 协议访问 LDAP 服务器，取值必须为： • 0：表示不使用 TLS 协议访问 LDAP 服务器。 • 1：表示使用 TLS 协议访问 LDAP 服务器。 默认值为 0。

例如：

```
Demo(config)#ssl settings crl offline "ssl_vhost" "cdp1" "http://10.8.6.50/xxx.crl" 1440 0
```



注意：

- 在配置该命令之前，请先使用命令“**ssl import crlca**”为 SSL 主机导入 CRL 签发证书，用来验证为 SSL 主机下载的 CRL 文件是否合法。
- 建议不要配置大量时间间隔很小（比如 1 分钟）的 CRL 文件下载规则，否则可能导致系统无法正常建立 SSH 连接。
- 最多支持通过“**ssl settings crl offline**”和“**ssl globals crl cdp**”命令配置 4010 个 CDP。

no ssl settings crl offline <host_name> [cdp_name]

该命令用于删除为指定 SSL 虚拟主机或后台主机配置的 CDP 及其 CRL 文件下载规则。当删除了为 SSL 主机配置的所有 CDP 后，系统将禁用该 SSL 主机的 CRL 离线检查。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

cdp_name 可选，该参数指定 CDP 的名称。取值必须为：

- CDP 名称：表示删除为 SSL 虚拟主机或后台主机配置的指定 CDP 及其 CRL 文件下载规则。
- ALL：表示删除为 SSL 虚拟主机或后台主机配置的所有 CDP 及其 CRL 文件下载规则。

默认值为“ALL”。

ssl globals crl cdp <cdp_name> <cdp_url> [time_interval] [delay_time] [tls_flag]

该命令用于为全局配置 CDP 及其 CRL 文件下载规则。系统按照 CRL 文件下载规则设定的时间间隔从配置的 CDP 为全局下载 CRL 文件。系统支持通过 HTTP、FTP 和 LDAP 三种协议下载 CRL 文件。

在配置全局 CDP 之后，可以通过命令“**ssl globals crl host**”将此 CDP 关联至指定 SSL 虚拟主机或后台主机，从而可以实现与命令“**ssl settings crl offline**”相同的功能。系统允许配置最多 10 个全局 CDP，一个全局 CDP 可以关联至多个 SSL 主机，多个全局 CDP 也可以关联至一个 SSL 主机。

cdp_name 该参数指定全局 CDP 的名称。取值必须为长度不大于 31 个字节的字符串。支持数字、字母和下划线，不能为“all”或“ALL”。

cdp_url 该参数指定下载 CRL 文件的 HTTP、FTP 或 LDAP URL 地址。取值必须为长度不大于 1023 个字节的字

字符串。

time_interval	可选，该参数指定下载 CRL 文件的时间间隔，单位为分钟。取值必须为 1 到 2,147,483,647 之间的整数。默认值为 1440。
delay_time	可选，该参数指定下载的 CRL 文件的延迟到期时间，单位为分钟。取值必须为 0 到 2,147,483,647 之间的整数。默认值为 0。 - 该参数取值大于 0 时，系统在下载 CRL 文件后检查 CRL 文件是否过期。如果当前时间已晚于 CRL 文件内包含的下次更新时间（也就是此文件到期时间）与延迟到期时间之和，那么此 CRL 文件过期，系统将拒绝所有需要通过这个 CRL 文件验证客户端证书的 SSL 连接；如果当前时间未晚于下次更新时间与延迟到期时间之和，CRL 文件即是有效的。 - 该参数取值为默认值 0 时，系统在下载 CRL 文件后不检查 CRL 文件是否过期。
tls_flag	可选。该参数指定是否使用 TLS 协议访问 LDAP 服务器，取值必须为： 0：表示不使用 TLS 协议访问 LDAP 服务器。 1：表示使用 TLS 协议访问 LDAP 服务器。 默认值为 0。

例如：

```
Demo(config)#ssl globals crl cdp "cdp1" "http://10.8.6.50/xxx.crl" 1440 0
```



注意：

- 在配置该命令之前，请先使用命令“**ssl import crlca**”为全局 CRL CA 证书列表导入 CRL 签发证书，用来验证使用该命令下载的 CRL 文件是否合法。
- 最多支持通过“**ssl settings crl offline**”和“**ssl globals crl cdp**”命令配置 4010 个 CDP。

no ssl globals crl cdp [cdp_name]

该命令用于删除为全局配置的 CDP 及其 CRL 文件下载规则。

cdp_name	可选，该参数指定全局 CDP 的名称。取值必须为： CDP 名称：表示删除为全局配置的指定 CDP 及其

CRL 文件下载规则。

- ALL: 表示删除为全局配置的所有 CDP 及其 CRL 文件下载规则。

默认值为“ALL”。

ssl globals crl host <cdp_name> <host_name>

该命令用于将为指定全局 CDP 关联至指定 SSL 虚拟主机或后台主机。如果为 SSL 主机关联了全局 CDP, 该 SSL 主机的 CRL 离线证书吊销检查功能将使用系统从该全局 CDP 下载的 CRL 文件。一个全局 CDP 可以关联至多个 SSL 主机, 多个全局 CDP 也可以关联至一个 SSL 主机。

cdp_name 该参数指定全局 CDP 的名称。

host_name 该参数指定 SSL 虚拟主机或后台主机的名称。

no ssl globals crl host <cdp_name> <host_name>

该命令用于解除指定全局 CDP 与指定 SSL 虚拟主机或后台主机之间的关联关系。

ssl load crl

该命令用于立即从所有由命令“ssl settings crl offline”和“ssl globals crl cdp”定义的 CDP 重新下载 CRL 文件。

ssl import crlfilter <cdp_name> <tftp_ip> [file_name]

该命令用于为指定全局 CDP 导入 CRL 过滤器文件, 用于过滤需要下载的 CRL 文件。该文件包含的必须为简化的正则表达式。正则表达式支持“\d”、“\w”以及 OpenLDAP 服务器允许的格式。

若需要从全局 CDP 中下载所有的 CRL 文件, 请确保已经为该 CDP 导入了所需要的 CRL 过滤器文件。

cdp_name 该参数指定全局 CDP 的名称。

tftp_ip 该参数指定 CRL 过滤器文件所在的 TFTP 服务器的 IP 地址。取值必须为 IPv4 地址。

file_name 可选, 该参数指定 TFTP 服务器上的 CRL 过滤器文件的文件名。取值必须为长度不大于 1023 个字节的字符串。默认值为“crlfilter.conf”。



注意:

- 该命令仅对通过命令“ssl globals crl cdp”配置的全局 CDP 生效。

- 配置该命令后，本次下载 CRL 文件不生效，下一次下载 CRL 文件时才生效。

ssl globals crl studyfilter <cdp_name> [time_interval]

该命令用于为指定全局 CDP 启用 CRL 过滤器自主学习功能，以便更加有效地下载 CRL 文件。

cdp_name 该参数指定全局 CDP 的名称。

time_interval 可选，该参数指定两次学习之间的时间间隔，单位为分钟。取值必须为 1 到 2,147,483,647 之间的整数，默认值为 10,080。



注意：该命令仅对通过命令“**ssl globals crl cdp**”配置的全局 CDP 生效。

no ssl crlfilter <cdp_name>

该命令用于删除指定全局 CDP 的所有导入的 CRL 过滤器文件、解析的 CRL 过滤器文件和学习到的 CRL 过滤器文件。

ssl globals fastcrl {on|off}

该命令用于启用或禁用 CRL 缓存功能。启用该功能后，系统将为 CRL 离线证书吊销检查下载到本地的 CRL 文件立刻载入到缓存中，从而提高了检查证书吊销状态的速度。该功能默认是禁用的。

系统分配给 CRL 文件缓存的最大内存取决于系统内存的大小，如下表所示：

表9 - 4 CRL 文件缓存的最大内存

系统内存	CRL 文件缓存区最大内存
1 GB 或小于 1 GB	10 MB
2 GB	25 MB
4 GB	150 MB
8 GB	200 MB
16 GB	600 MB
大于 16 GB	1200 MB



注意：当缓存的 CRL 文件达到分配的最大内存后，系统会自动禁用 CRL 缓存功能。

show ssl crlstatus [host_name] [cdp_name]

该命令用于显示系统为指定 SSL 虚拟主机或后台主机或全局从指定或者全部 CDP 下载的 CRL 文件，包括 CDP 名称、CRL 文件的更新时间以及它的状态。CRL 文件有三种状态：success（成功）、failed（失败）以及 downloading（正在下载）。

- host_name** 可选，该参数指定 SSL 虚拟主机或后台主机的名称。
- SSL 虚拟主机或 SSL 后台主机的名称：表示显示系统为指定 SSL 虚拟主机或后台主机下载的 CRL 文件。
 - ALL：表示显示系统为全局下载的 CRL 文件。
- 默认值为“ALL”。
- cdp_name** 可选，该参数指定 CDP 的名称。
- CDP 名称：表示显示从指定 CDP 下载的 CRL 文件。
 - ALL：表示显示从全部 CDP 下载的 CRL 文件。
- 默认值为“ALL”。

以下是一个输出例子：

```
Demo(config)#show ssl crlstatus all cdp1
Host "vhost":
  CRL Distribution Point "cdp1":
    Parse status      : N/A
    Study time        : N/A
    Study status      : N/A
    Download time     : Tue Apr 25 15:40:41 2017
    Download status: Downloading
    Nextupdate        : N/A
    Delay              : N/A
    Validity           : Valid
```

ssl settings crlmode certcdpfirst <virtual_host_name>

该命令用于为指定 SSL 虚拟主机配置优先使用客户端证书 CDP 模式。在该模式下：

- 如果客户端证书携带 CDP，且 CDP 为 LDAP 或 LDAPS 格式的 Full Name 或者为 DA（Directory Address）格式，系统会首先使用客户端证书中的 CDP 指定的地址查找 CRL 缓存，来判断客户端证书的有效性。如果未能查找到有效的 CRL 数据，系统则逐一查找从 SSL 虚拟主机关联的 CDP 缓存的所有 CRL 数据，并与客户端证书进行匹配，来判断客户端证书的有效性。
- 如果客户端证书携带 CDP，且 CDP 为 HTTP 或 FTP 格式的 Full Name 格式，系统则逐一查找从 SSL 虚拟主机关联的 CDP 指定的 HTTP 和 FTP 类型的 Full Name 缓存的 CRL 数据，并与客户端证书进行匹配，来判断客户端证书的有效性。

- 如果客户端证书中不携带 CDP, 系统将逐一查找从 SSL 虚拟主机关联的 CDP 缓存的所有 CRL 数据, 并与客户端证书进行匹配, 来判断客户端证书的有效性。

使用该模式前, 需要先通过命令 “**ssl globals fastcrl on**” 启用 CRL 缓存功能, 并通过以下两种方式中的任意一种, 为虚拟主机配置 CDP 和 CRL 文件下载规则:

- 为指定虚拟主机执行命令 “**ssl settings crl offline**”。
- 先执行 “**ssl globals crl cdp**” 命令配置全局 CDP 及 CRL 文件下载规则, 再通过 “**ssl globals crl host**” 命令将全局 CDP 关联至指定虚拟主机。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。



注意: 只能为同一个虚拟主机配置命令 “**ssl settings crlmode certcdpfirst**”、“**ssl settings crlmode certcdponly**” 和 “**ssl settings crlmode hostcdponly**” 中的一条。

ssl settings crlmode certcdponly <virtual_host_name> [certificate_status]

该命令用于为指定 SSL 虚拟主机配置仅使用客户端证书 CDP 模式。启用该模式后, 系统仅使用客户端证书中的 CDP 指定的地址查找 CRL 缓存, 来判断客户端证书的有效性。如果未能查找到有效的 CRL 数据, 或者客户端证书中不携带 CDP, 系统按照参数 “certificate_status” 的配置, 来判断客户端证书的有效性。

使用该模式前, 需要先通过命令 “**ssl globals fastcrl on**” 启用 CRL 缓存功能, 并通过以下两种方式中的任意一种, 为虚拟主机配置 CDP 和 CRL 文件下载规则:

- 为指定虚拟主机执行命令 “**ssl settings crl offline**”。
- 先执行 “**ssl globals crl cdp**” 命令配置全局 CDP 及 CRL 文件下载规则, 再通过 “**ssl globals crl host**” 命令将全局 CDP 关联至指定虚拟主机。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

certificate_status 可选, 该参数用于设置在系统未能按照客户端证书中的 CDP 指定的地址查找到有效的 CRL 数据, 或者客户端证书中不携带 CDP 时, 客户端证书是否有效。取值必须为:

- **valid:** 表示将客户端证书状态判断为有效。
- **revoked:** 表示将客户端证书状态判断为已吊销。

默认值为 **valid**。



注意：只能为同一个虚拟主机配置命令“**ssl settings crlmode certcdpfirst**”、“**ssl settings crlmode certcdponly**”和“**ssl settings crlmode hostcdponly**”中的一条。

ssl settings crlmode hostcdponly <virtual_host_name>

该命令用于为指定 SSL 虚拟主机配置仅使用 SSL 主机 CDP 模式。启用该模式后，系统通过逐一查看从 SSL 虚拟主机关联的 CDP 缓存的所有 CRL 数据，来判断客户端证书的有效性。

使用该模式前，需要先通过命令“**ssl globals fastcrl on**”启用 CRL 缓存功能，并通过以下两种方式中的任意一种，为虚拟主机配置 CDP 和 CRL 文件下载规则：

- 为指定虚拟主机执行命令“**ssl settings crl offline**”。
- 先执行“**ssl globals crl cdp**”命令配置全局 CDP 及 CRL 文件下载规则，再通过“**ssl globals crl host**”命令将全局 CDP 关联至指定虚拟主机。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。



注意：只能为同一个虚拟主机配置命令“**ssl settings crlmode certcdpfirst**”、“**ssl settings crlmode certcdponly**”和“**ssl settings crlmode hostcdponly**”中的一条。

9.7 客户端认证高级选项

ssl settings authmandatory <virtual_host_name>

该命令用于为指定 SSL 虚拟主机启用客户端认证强制模式。

系统支持两种客户端认证方式：强制的和非强制的。当服务器发送一个证书请求到客户端时，如果客户端点击“取消”拒绝发送客户端证书给服务器，或者客户端证书未能通过验证时：

- 强制模式下，服务器将会丢弃这个 SSL 连接，拒绝客户端的所有请求。
- 非强制模式下，服务器将会允许客户端连接到限制性的网络资源（可使用命令“**http acl url**”配置，注意访问级别应设为“level 1”）。

客户端认证的强制模式默认设置为启用。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

no ssl settings authmandatory <virtual_host_name>

该命令用于为指定 SSL 虚拟主机禁用客户端认证强制模式。

ssl settings acceptchain <host_name>

该命令用于为指定 SSL 虚拟或后台主机启用证书链支持。当启用证书链支持时，SSL 主机在对方发送的证书链中找到一个存在于受信任 CA 证书列表中的 CA 证书则认证通过。对于 SSL 虚拟主机，该命令仅在启用了客户端认证时才有效。

host_name 该参数指定 SSL 虚拟或后台主机的名称。



注意：通过命令“**ssl settings acceptchain**”启用证书链支持后，如果用户证书的颁发者和子 CA 证书的使用者编码方式不一致，设备会返回 903。

no ssl settings acceptchain <host_name>

该命令用于为指定 SSL 虚拟或后台主机禁用证书链支持。

ssl settings clientcert minkey <virtual_host_name> <key_length>

该命令用于设置访问指定 SSL 虚拟主机时客户端证书所需要支持的 RSA 密钥的最小长度。该配置对 SSL 虚拟主机是可选的。当没有为 SSL 虚拟主机配置该命令，SSL 虚拟主机将不检查客户端证书的 RSA 密钥长度。

如果 RSA 密钥的长度小于设置的最小长度：

- 对于关联 HTTPS 虚拟服务的 SSL 虚拟主机，系统将拒绝客户端访问，并生成错误码“902: The SSL client certificate's key size is too small”。
- 对于关联 TCPS 和 FTPS 虚拟服务的 SSL 虚拟主机，系统将拒绝客户端访问，并生成日志。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

key_length 该参数指定访问 SSL 虚拟主机的客户端证书所需要支持的 RSA 密钥的最小长度，单位为比特。

- 对于装备了 FIPS HSM 的设备，取值必须为 1024、2048 或 4096。
- 对于未装备 FIPS HSM 的设备，取值必须为 512、1024、2048 或 4096。



注意：执行该命令之前，需要确保已经通过命令“**ssl settings clientauth**”为 SSL 虚拟主机启用了客户端认证功能。

no ssl settings clientcert minkey <virtual_host_name>

该命令用于删除对访问指定 SSL 虚拟主机时客户端证书所需要支持的 RSA 密钥的最小长度设置。

ssl settings minimum <virtual_host_name> <cipher_strength> <redirect_url>

该命令用于设置访问指定 SSL 虚拟主机时客户端需要支持的最小加密强度。该配置对 SSL 虚拟主机是可选的。

如果连接到该 SSL 虚拟主机的客户端不支持由参数“cipher_strength”所指定的最小加密强度，则将客户端的访问请求重定向到由参数“redirect_url”所指定的 URL 地址。

virtual_host_name	该参数指定 SSL 虚拟主机的名称。
cipher_strength	该参数指定访问特定 SSL 虚拟主机时客户端需要支持的最小加密强度，单位为比特。取值必须为 40、56、128、168、256 或 512。
redirect_url	该参数指定重定向的 URL 地址。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。



注意： 本命令仅适用于关联到 HTTPS 虚拟服务的 SSL 虚拟主机。

no ssl settings minimum <virtual_host_name>

该命令用于删除对访问指定 SSL 虚拟主机的客户端所需要支持的最小加密强度设置。

9.8 服务器认证

ssl globals verifycert {on|off}

该命令用于为所有 SSL 后台主机启用或禁用服务器认证功能。在设备作为 SSL 代理客户端时，服务器认证功能允许 SSL 后台主机验证 SSL 服务器的证书。如果启用服务器认证，SSL 后台主机与 SSL 服务器将进行带单向认证的 SSL 握手。如果禁用服务器认证功能，SSL 后台主机在 SSL 握手过程中将不验证服务器的证书。该功能默认是启用的。

ssl settings verifycert <real_host_name>

该命令用于为指定的 SSL 后台主机启用服务器认证功能。当设备作为 SSL 代理客户端时，SSL 后台主机在 SSL 握手过程中对服务器的证书进行验证。该功能默认为启用。当全局和指定 SSL 后台主机均启用服务器认证功能时，此功能才生效。

no ssl settings verifycert <real_host_name>

该命令用于为指定的 SSL 后台主机禁用服务器认证功能。当设备作为 SSL 代理客户端时，SSL 后台主机在 SSL 握手过程中不验证服务器的证书。

ssl settings servername <real_host_name> <common_name>

该命令用于为指定 SSL 后台主机启用 SSL 服务器通用名称检查，并指定期望的 SSL 服务器通用名称。在成功校验服务器证书后，SSL 后台主机还要检查服务器证书的通用名称是否与期望的 SSL 服务器通用名称匹配。如果不匹配，则 SSL 后台主机拒绝服务器证书。

real_host_name	该参数指定 SSL 后台主机的名称。
common_name	该参数指定期望的 SSL 服务器通用名称。取值必须为长度不大于 64 个字节的字符串。支持数字、字母和特殊字符。当取值包含特殊字符时，名称必须置于双引号内。

no ssl settings servername <real_host_name>

该命令用于为指定 SSL 后台主机禁用 SSL 服务器通用名称检查。

9.9 SSL 重协商



注意：SSL 重协商是指 SSL 安全重协商。系统不支持非安全重协商。

以下命令用于控制全局和单个 SSL 虚拟主机上 SSL 重协商功能的开启状态。



注意：在 HTTP/2 运行于 TLS 之上的部署环境里，必须禁用 SSL 重协商。

ssl globals renegotiation {on|off}

该命令用于为全局（即所有 SSL 主机）启用或禁用 SSL 重协商功能（SSL renegotiation）。该功能默认对全局是禁用的。

ssl settings renegot <host_name>

该命令用于为指定 SSL 虚拟主机或后台主机启用 SSL 重协商功能。该功能默认对 SSL 主机是禁用的。当全局和指定 SSL 主机均开启此功能时，此功能才生效。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。

no ssl settings renegot <host_name>

该命令用于为指定 SSL 虚拟主机或后台主机禁用 SSL 重协商功能。

ssl settings clientreneg <real_host_name> [reneg_mode]

该命令用于为 SSL 后台主机指定安全重协商拓展强制模式。该功能默认为禁用。

real_host_name	该参数指定 SSL 后台主机的名称。

reneg_mode 可选，该参数指定安全重协商拓展强制模式，取值必须为：

- 1: 表示允许服务器发送的 **serverhello** 不携带安全重协商拓展项。
- 2: 表示允许服务器发送的 **serverhello** 不携带安全重协商拓展项时后台主机发送的 **RESET** 断开连接。

默认值为 1。



注意：

- 启用该功能后，将无法正常使用浏览器。请谨慎使用该功能。
- 只有为 SSL 虚拟主机设置的协议版本是 TLSv1.0、TLSv1.1、TLSv1.2 或 SM2v1.1 中的一种或几种时，该命令才会生效。

9.10 SSL 会话功能选项

ssl settings reuse <host_name>

该命令用于为指定 SSL 虚拟主机或者 SSL 后台主机启用 SSL 会话复用功能。该功能默认是启用的。

host_name 该参数指定 SSL 虚拟或后台主机的名称。



注意：复用的会话仍然使用上一次会话中已经协商的密码套件。如果密码套件配置发生变化，SSL 后台主机不会发起会话复用，SSL 虚拟主机会直接重置连接。

no ssl settings reuse <host_name>

该命令用于为指定 SSL 虚拟主机或者 SSL 后台主机禁用 SSL 会话复用功能。

ssl settings insertclientip <virtual_host_name> <ip_type> <extension_type> <port_flag>

该命令用于为指定虚拟主机启用在 **ServerHello** 报文中插入客户端 IP 地址及端口的功能。该命令还可以用于为指定虚拟主机修改已插入 **ServerHello** 报文中的客户端 IP 地址及端口。

virtual_host_name 该参数指定已有虚拟主机的名称。

ip_type 该参数指定要插入的客户端 IP 地址的类型。

- **ipv4:** 表示 IPv4 地址。

- **ipv6:** 表示 IPv6 地址。

extension_type	该参数指定 Server Hello 报文的扩展类型值。取值必须为 57 至 65,535 之间的整数。
port_flag	可选。该参数指定系统是否向 ServerHello 报文中插入端口。如果插入的是 IPv4 地址，格式为“ipv4:port”；如果插入的是 IPv6 地址，格式为“[ipv6]:port”。取值必须为： • 1: 表示系统将向 ServerHello 报文中插入端口。 • 0: 表示不插入端口。 默认值为 0。



注意：

- 启用该功能后，将无法正常使用浏览器。请谨慎使用该功能。
- 只有为 SSL 虚拟主机设置的协议版本是 TLSv1.0、TLSv1.1、TLSv1.2 或 SM2v1.1 中的一种或几种时，该命令才会生效。

no ssl settings insertclientip <virtual_host_name> [ip_type]

该命令用于为指定虚拟主机禁用在 ServerHello 报文中插入指定类型的客户端 IP 的功能

virtual_host_name	该参数指定已有虚拟主机的名称。
ip_type	可选。该参数指定要删除的客户端 IP 地址的类型。 • ipv4: 表示 IPv4 地址。 • ipv6: 表示 IPv6 地址。 默认值为 IPv4。

ssl globals sessiontimeout <timeout>

该命令用于设置 SSL 会话超时时间。当没有配置该命令时，默认的 SSL 会话超时时间为 1800 秒。

timeout	该参数指定超时时间，单位为秒。取值必须为 60 到 86,400 之间的整数。

ssl globals sendclosenotify {on|off}

该命令用于为所有 SSL 虚拟主机和 SSL 后台主机启用或禁用在 SSL 主机终止 SSL 会话时发送 SSL 关闭通知的功能。如果启用本功能，在 SSL 会话中，当 SSL

虚拟主机或 SSL 后台主机终止 SSL 连接时，将向对端发送 SSL 关闭通知。该功能默认是启用的。

ssl globals ignoreclosenotify {on|off}

该命令用于为所有 SSL 虚拟主机和 SSL 后台主机启用或禁用忽略对端发送的 SSL 关闭通知的功能。该功能默认是启用的。

在 SSL 会话中，任何一方终止 SSL 连接时，都需要向对端发送 SSL 关闭通知。

- 如果启用本功能，当 SSL 连接被终止时，即使 SSL 虚拟主机/后台主机没有收到对端发送的 SSL 关闭通知，系统也会忽略不正常的连接关闭并保持对依附于该连接的 SSL 会话的复用。
- 如果禁用本功能，当 SSL 连接被终止时，SSL 虚拟主机/后台主机需要接收到对端发送的 SSL 关闭通知，否则依附于该连接的 SSL 会话将被标记为无效并被清除。

9.11 SSL 错误页面定制

ssl import error <error_code> <url> [host_name]

该命令用于为指定 SSL 主机或全局（即所有 SSL 主机）导入定制的返回给客户端的 SSL 相关错误页面，大小不超过 10 MB。可为指定错误码导入一个自定义的静态错误页面，自定义的静态错误页面必须为不包含图片及 flash 动画的静态 HTML 页面。

error_code 该参数指定自定义错误页面的错误码。目前，系统支持为以下错误码定制错误页面：

- 901: SSL host requires the client certificate;
- 902: The certificate's key size is too small;
- 903: The certificate is not trusted;
- 904: The certificate is expired;
- 905: The certificate isn't validate yet;
- 906: The certificate has been revoked.

url 该参数指定自定义错误页面的 HTTP 或者 FTP URL 地址。取值的最大长度受 CLI 支持的命令行最大长度限制，目前 CLI 最多支持 1024 个字节的命令行。

注意：FTP 类型 URL (ftp://user:password@host:port/path) 中的“path”需使用相对路径。

host_name 可选，该参数指定 SSL 主机的名称。取值必须为：

- SSL 主机的名称：表示为指定 SSL 主机导入自定义错误页面。
- ALL：表示为全局导入自定义错误页面。

默认值为“ALL”。



注意：

- 为确保 SSL 错误页面能正常显示，请在导入 SSL 错误页面前将其文件编码转为 UTF-8 无 BOM。
- 在 WebUI 上，除了 URL 方式外，系统还支持通过本地文件导入错误页面。

no ssl import error <error_code> [host_name]

该命令用于删除已经为指定 SSL 主机或全局导入的自定义错误页面。

show ssl import error page <error_code> [host_name]

该命令用于显示为指定 SSL 主机或全局导入的自定义错误页面。

show ssl import error list

该命令用于显示为单个 SSL 主机和全局导入的自定义错误页面列表。

clear ssl import error

该命令用于清除为单个 SSL 主机和全局导入的自定义错误页面。

ssl load error <error_code> [host_name]

该命令用于为指定 SSL 主机或全局启用已导入的自定义错误页面。当客户端认证失败时，在 SSL 客户端将显示启用的自定义错误页面。

error_code 该参数指定已使用命令“**ssl import error**”导入到设备中的自定义错误页面的错误码。目前，系统支持配置以下错误码：

- 901: SSL host requires the client certificate;
- 902: The certificate's key size is too small;
- 903: The certificate is not trusted;
- 904: The certificate is expired;
- 905: The certificate isn't validate yet;
- 906: The certificate has been revoked.

host_name 可选，该参数指定 SSL 主机的名称。取值必须为：

- SSL 主机的名称：表示为指定 SSL 主机启用已导入

的自定义错误页面。

- ALL: 表示为全局启用已导入的自定义错误页面。

默认值为“ALL”。



注意: 对 SSL 主机的一个 error code, 如果为 SSL 主机启用了自定义错误页面, 则返回该 SSL 主机的自定义错误页面; 如果没有为该 SSL 主机启用自定义错误页面, 但为全局启用了自定义错误页面, 则返回全局的自定义错误页面。如果没有为全局启用自定义错误页面, 则返回默认的错误页面。

no ssl load error <error_code> [host_name]

该命令用于禁用已经为指定 SSL 主机或全局启用的自定义错误页面。

show ssl load error page <error_code> [host_name]

该命令用于显示已经为指定 SSL 主机或全局启用的自定义错误页面。

show ssl load error list

该命令用于显示为单个 SSL 主机和全局启用的自定义错误页面列表。

clear ssl load error

该命令用于禁用为单个 SSL 主机和全局启用的自定义错误页面。

9.12 SSL 通道

ssl channel name <channel_name> <ip> <port> <encryption_port>
<direction> <host_name>

该命令用于创建一条 SSL 通道。执行该命令后, 只有满足下面条件之一时, 流量会经过 SSL 通道:

- 目的 IP 和目的端口匹配出向 (参数 “direction” 为 “out”) SSL 通道的 IP 和端口;
- 源 IP 和源端口匹配入向 (参数 “direction” 为 “in”) SSL 通道的 IP 和端口。

并且, 执行该命令后系统将基于流量方向自动生成相关 SLB 配置和 SSL 配置。具体如下:

- 参数 “direction” 为 “in”: 自动生成 TCPS 类型的后台服务和 TCPS 类型的虚拟服务并采用静态策略关联, 自动生成 SSL 虚拟主机并且自动与虚拟服务关联。
- 参数 “direction” 为 “out”: 自动生成 TCPS 类型的后台服务和 TCP 类型的虚拟服务并采用静态策略关联, 自动生成 SSL 后台主机并且自动与后台服务关联。

对于自动生成的虚拟主机和后台主机，需要手动向虚拟主机或后台主机中添加证书。

系统支持创建最多 200 个 SSL 通道。

channel_name	该参数指定 SSL 通道的名称，取值必须为长度不超过 120 个字节的字符串，支持数字、字母和特殊字符，区分大小写。当取值包含特殊字符时，必须置于双引号内。该参数取值不能设置为系统保留字“default”、“all”或“global”（不区分大小写）。
ip	该参数指定通道内部 IP，一般为设备上需要提供加解密服务的 IP，即自动生成的 SLB 虚拟服务和 SLB 后台服务的 IP。
port	该参数指定 SSL 通道的内部端口，取值必须为 1 至 65,535 之间的整数。 • 当参数“direction”取值为“in”时，该参数指定 TCP 类型的后台服务的端口。 • 当参数“direction”取值为“out”时，该参数指定 TCP 类型的虚拟服务的端口。
encrypt_port	该参数指定 SSL 通道的加密端口，取值必须为 1 至 65,535 之间的整数。 • 当参数“direction”取值为“in”时，该参数指定 TCPS 类型的虚拟服务的端口。 • 当参数“direction”取值为“out”时，该参数指定 TCPS 类型的后台服务的端口。
direction	该参数指定 SSL 通道的方向，取值必须为“in”或者“out”。
host_name	该参数指定 SSL 主机的名称。取值可以为已存在的 SSL 虚拟主机或后台主机的名称，也可以为新生成的 SSL 虚拟主机或后台主机的名称。取值必须为长度不大于 240 个字节的字符串。支持数字、字母和下划线，但不能以下划线开头。不支持特殊字符。 • 当参数 direction 取值为“in”时，参数取值需要设置为 SSL 虚拟主机。 • 当参数 direction 取值为“out”时，参数取值需要设置为 SSL 后台主机。

示例：

➤ “in” 方向

```
AN(config) ssl channel name channel1 1.1.1.1 6000 443 in ssl_vhost1
```

执行上述命令后，自动生成 TCPS 类型的虚拟服务 “channel1”，及 TCP 类型的后台服务 “channel1_chauto”。具体如下：

```
slb virtual tcps channel1 1.1.1.1 443
slb real tcp channel1_chauto 1.1.1.1 6000 tcp
slb policy static channel1 channel1_chauto
ssl host virtual ssl_vhost1 channel1
system mode transparent channel1
```

➤ “out” 方向：

```
AN(config) ssl channel name channel1 1.1.1.1 6000 443 out ssl_rhost1
```

执行上述命令后，自动生成 TCP 类型的虚拟服务 “channel1_chauto”，及 TCPS 类型的后台服务 “channel1”。具体如下：

```
slb virtual tcp channel1_chauto 1.1.1.1 6000 noarp
slb real tcps channel1 1.1.1.1 443 tcp
slb policy static channel1_chauto channel1
ssl host real ssl_rhost1 channel1
system mode transparent channel1_chauto
```

需要注意的是，上述自动生成的命令在通过 “show” 命令显示时，会在前面添加 “#” 标记。



注意：

- 设备的后台流量不允许访问 “in” 方向的 SSL 通道的虚拟服务，设备的入向流量不允许访问 “out” 方向的 SSL 通道的虚拟服务。
- “out” 方向的 SSL 通道的虚拟服务默认启用 “noarp”。
- SSL 通道默认启用对虚拟服务的健康检查功能（通过命令 “**slb virtual health on**”）。
- 创建 SSL 通道时自动生成的配置只能通过 “**no ssl channel name**” 或 “**clear ssl channel name**” 删除。

no ssl channel name <channel_name>

该命令用于删除指定 SSL 通道的配置。

show ssl channel name

该命令用于显示所有的 SSL 通道的配置。

clear ssl channel name

该命令用于清除所有的 SSL 通道的配置。

需要注意的是，执行该命令后，通过命令“**ssl channel name**”生成的 ssl 主机不会被删除。

show ssl channel relations [channel_name]

该命令用于显示指定 SSL 通道的配置及自动生成的关联配置。如果不指定参数“channel_name”，系统将显示所有 SSL 通道的配置及自动生成的关联配置。

show ssl channel status [channel_name]

该命令用于显示指定 SSL 通道的状态以及统计信息。如果不指定参数“channel_name”，系统将显示所有的 SSL 通道的状态以及统计信息。

9.13 SSL 通用命令

ssl globals statistics handshake on [duration]

该命令用于启用 SSL 握手成功率统计功能。启用该功能后，系统将统计指定时间段内所有 SSL 主机及其关联的 SLB 服务的握手成功率。默认情况下，该功能是禁用的。

duration 可选，该参数指定 SSL 握手成功率的统计时间。取值必须为 1 到 86,400 之间的整数。单位为秒。默认值为 300。

当取值小于等于 1000 时，握手成功率统计的采样周期为 1 秒；当取值大于 1000 时，握手成功率统计的采样周期为 duration/1000。

注意：取值大于 1000 时，采样周期为 duration/1000，需要等待一段时间，系统才会显示 SSL 握手成功率的统计数据。

ssl globals statistics handshake off

该命令用于禁用 SSL 握手成功率统计功能。禁用该功能后，已有的统计数据都将被清除。

ssl globals ems {on|off}

该命令用于启用或禁用 TLS EMS（Extended Master Secret）支持。启用 TLS EMS 支持后，系统将支持协商 TLS EMS 扩展。默认情况下，TLS EMS 支持为禁用。

ssl settings alpn <virtual_host_name>

该命令用于为指定的 TCPS 类型虚拟主机启用 ALPN 支持。默认情况下，所有 TCPS 类型的虚拟主机都禁用 ALPN 支持。

virtual_host_name 该参数指定 TCPS 类型的虚拟主机的名称。

no ssl settings alpn <virtual_host_name>

该命令用于为指定的 TCPS 类型虚拟主机禁用 ALPN 支持。

ssl globals serialnumber {upper|lower}

该命令用于设置转发到后台服务的客户端证书序列号的大小写，“**ssl globals serialnumber upper**”表示采用大写的序列号，“**ssl globals serialnumber lower**”表示采用小写的序列号。

系统的默认设置为“**ssl globals serialnumber upper**”。

ssl globals certexpdays [days]

该命令用于设置证书到期提醒天数。执行该命令后，对于已启用的 SSL 主机，如果证书到期天数小于等于设置的提醒天数，系统会通过日志进行提醒。提醒规则为：

- 如果证书到期天数大于等于 30 天，系统将显示“notice”级别日志。
- 如果证书到期天数大于等于 7 天，小于 30 天，系统将显示“warning”级别日志。
- 如果证书到期天数小于 7 天，系统将显示“critical”级别日志。
- 若证书已经过期，系统将显示“critical”级别日志。

days 可选。该参数指定证书到期提醒天数，单位为“天”。
取值必须为 1 到 180 之间的整数。默认值为 60。



注意：

- 对于 CRL CA 证书和全局根 CA 证书，证书到期后，系统不会提醒。
- 对于 SSL 客户端证书，证书到期后，系统不会提醒。

ssl globals certchkinterval [interval]

该命令用于设置检测证书到期天数的时间间隔。

interval 可选。该参数指定检测证书到期天数的时间间隔，单位为分钟。取值必须为 1 至 1440 之间的整数。
默认值为 1440。

show ssl globals

该命令用于显示所有 SSL 全局配置。

show ssl settings <host_name>

该命令用于显示指定 SSL 虚拟或后台主机的配置，包括名称、密码套件、协议版本等。

ssl start <host_name>

该命令用于启用指定 SSL 虚拟或后台主机。启用 SSL 主机后，该 SSL 主机的设置将对所有与之关联的 SLB 服务生效。SSL 主机默认是禁用的。

host_name 该参数指定 SSL 虚拟或后台主机的名称。取值必须为：

- SSL 主机的名称：表示启用指定 SSL 虚拟或后台主机。
- ALL：表示启用所有的 SSL 虚拟或后台主机。



注意：在以下情况中，必须先通过“**ssl activate certificate**”命令激活 SM2 证书，才能启用指定后台主机：

- 为后台主机配置了 ECDHE SM2 密码套件
- 为后台主机配置了 SM2v1.1 版本的 SSL 协议且开启了客户端认证

ssl stop <host_name>

该命令用于禁用指定 SSL 虚拟或后台主机，但是并不删除其配置，比如私钥和证书。禁用 SSL 主机后，该 SSL 主机的设置将不再对所有与之关联的 SLB 服务生效。

host_name 该参数指定 SSL 虚拟或后台主机的名称。取值必须为：

- SSL 主机的名称：表示禁用指定 SSL 虚拟或后台主机。
- ALL：表示禁用所有的 SSL 虚拟或后台主机。

show ssl status host

该命令用于显示所有已配置的 SSL 虚拟和后台主机的当前状态。

show statistics ssl [host_name]

该命令用于显示与指定 SSL 虚拟或后台主机相关的 SSL 连接和会话的当前统计信息。如果没有指定参数“host_name”，则显示所有 SSL 虚拟和后台主机的统计信息。

例如：

```
Demo#show statistics ssl
SSL Connection Statistics for "ssl_test"
    Open SSL connections: 106
```

```
Accepted SSL connections: 38287224
Requested SSL connections: 38387157
5 minutes requested rate: 1203 connections/sec
```

SSL Session Statistics for "ssl_test"

```
Resumed SSL sessions: 38368158
Resumable SSL sessions: 43
Session Misses: 0
```

SSL handshake statistics(300s):

```
Global: success: 1 all: 1 success rate: 100.00%
```



注意：在 SSL 统计信息中，“Resumed SSL sessions”，“Resumable SSL sessions”和“Session Misses”均为累积值。其中，“Resumable SSL sessions”的值即使在 SSL 会话超时的情况下也不会减少。

clear statistics ssl [host_name]

该命令用于清除指定 SSL 虚拟或后台主机的所有相关统计信息。如果没有指定参数“host_name”，则清除所有 SSL 虚拟和后台主机的统计信息。

9.14 FIPS

ssl fips so hsminit

该命令用于初始化 FIPS（Federal Information Processing Standard，联邦信息处理标准）HSM（Hardware Security Module，硬件安全模块）。FIPS HSM 通过 Security Officer（SO）帐户来完成初始化。SO 的默认用户名和密码分别为“cavium”和“default”。使用默认的 SO 用户名和密码登录 FIPS HSM 后，可以创建新的 SO 和 Crypto User（CU）。初始化完成后，设备将自动重启。

请注意该操作还将删除 FIPS HSM 中为所有 SSL 主机配置的公私钥对和证书、证书签发请求和根 CA 证书、中级 CA 证书和 CRL。执行该操作前，推荐将 FIPS HSM 上的这些条目通过 FIPS 克隆备份到另一个 FIPS 系统。关于 FIPS 克隆的细节，请参见 FIPS 用户手册。

ssl fips user login

该命令用于让 CU 登录 FIPS HSM。登录成功后，CU 就可以进行加解密操作。

ssl fips user logout

该命令用于让 CU 退出 FIPS HSM。退出后，FIPS 加解密操作不可以执行。推荐用户在系统启动时登录，并在系统运行期间保持登录来避免中断 SSL 流量。

ssl fips user autologin

该命令用于启用自动登录功能。启用该功能后，管理员需要执行命令“write memory”来永久保存设置，从而使得每次重启后 CU 可以自动登录 FIPS HSM。

no ssl fips user autologin

该命令用于禁用自动登录功能。执行该命令后，管理员需要执行命令“write memory”来永久保存设置，这样每次系统重启后，CU 都需要手动登录。

ssl fips so hsmzeroize

该命令用于将 FIPS HSM 恢复为出厂设置。执行该命令后，系统将自动重启。

请注意该操作还将清除 FIPS HSM 中为所有 SSL 主机配置的公私钥对和证书、证书签发请求和根 CA 证书、中级 CA 证书和 CRL。执行该操作前，推荐将 FIPS HSM 上的这些条目通过 FIPS 克隆备份到另一个 FIPS 系统。关于 FIPS 克隆的细节，请参见 FIPS 用户手册。



注意：如果 SO 连续 20 次登录失败，FIPS HSM 也会被恢复为出厂设置。

9.15 密码卡

设备支持三种密码卡：三未密码卡、渔翁密码卡和国芯密码卡。其中，当设备安装的是渔翁密码卡时，管理员可以使用的命令只有通用命令。



注意：三未密码卡、渔翁密码卡和国芯密码卡均不支持运行时配置同步。

9.15.1 通用配置

ssl gmsdf random [random_length]

该命令用于生成一个随机数。

random_length	该参数指定随机数的长度，单位为字节。取值必须为 1 到 16,384 之间的整数。默认值为 16。

ssl gmsdf reset

该命令用于重置密码卡。执行该命令后，密码卡将恢复到出厂状态，所有的管理员和操作员信息，以及存储的所有密钥都将被清除。



注意：对于安装了 CCUPH3001 V1.0 PCI-E 密码卡的设备，该命令会同时初始化用户密钥管理系统。

show ssl gmsdf device

该命令用于显示密码卡的信息，包括密码卡的发行商，名称、序列号和版本号等。

show ssl gmsdf permission

该命令用于显示密码卡的权限状态，包括密码卡当前的权限级别、管理员数量、所有管理员 ID、已登录的管理员 ID 和操作员状态。

ssl gmsdf failover [mode]

该命令用于启用或禁用国密卡故障容错机制功能。系统优先使用国密卡进行 SSL 加解密，国密卡无法正常工作系统使用软件 SSL 进行加解密。默认情况下，该功能是启用的。

mode 可选，该参数用于启用或者禁用国密卡故障容错机制功能。

- on: 表示启用国密卡故障容错机制功能。启用该功能后，当系统检测到国密卡无法正常工作，将在日志中记录国密卡故障，并使用软件 SSL 进行加解密。
- off: 表示禁用国密卡故障容错机制。禁用该功能后，当系统检测到国密卡无法正常工作，在日志中记录国密卡故障后，直接断开 SSL 连接。

默认值为“on”。

show ssl gmsdf failover

该命令用于显示国密卡故障容错机制功能的状态。

9.15.2 三未密码卡

设备通过支持 SM2/SM3/SM4 算法的国产密码算法的三未密码卡进行安全通信，目前三未密码卡只支持对 SM2 虚拟主机上的 SSL 通信进行加解密。

三未密码卡中的用户包括管理员和操作员，且三未密码卡只有在用户登录后才能正常工作。每个用户持有一个智能密码钥匙（USB Key, Ukey），用户必须将自己的智能密码钥匙插入设备的 USB 插口才能登录并使用三未密码卡。当设备启动或重启后，三未密码卡的所有用户都会被自动注销。

三未密码卡具有权限管理功能，四个权限级别从低到高依次为“Init”、“None”、“Operator”和“Administrator”。用户处于较高权限级别时，能够执行较低权限级别中所能执行的所有操作：

- Init: 三未密码卡被重置后处于该级别，此时用户只能执行重置三未密码卡操作或添加第一个管理员。

- **None:** 已经给三未密码卡添加了一些用户但没有用户登录时，三未密码卡处于该级别，此时用户可以执行登录或注销操作。
- **Operator:** 只有操作员登录时，三未密码卡处于该级别，此时用户可以执行密码运算操作。
- **Administrator:** 当大于一半的管理员登录后，三未密码卡处于该级别，此时用户可以添加或删除管理员或操作员，并可以添加或删除三未密码卡中存储的密钥。

ssl gmsdf sanwei admin <admin_id> <pin> [force]

该命令用于向三未密码卡添加一个管理员。添加管理员成功后，该管理员将自动登录到三未密码卡。当一个管理员添加成功后，需要拔出该管理员的 Ukey，插入下一个管理员的 Ukey，添加下一个管理员。系统支持最多添加 5 个管理员。

admin_id	该参数指定管理员的序号。取值必须为 1 到 5 之间的整数。
pin	该参数指定管理员 Ukey 的 PIN 码。添加管理员后，建议使用命令 “ ssl gmsdf sanwei changepin ” 修改管理员的默认 PIN 码。
force	可选。该参数用于强制改写三未密码卡的 Ukey。

no ssl gmsdf sanwei admin <pin> [confirmed]

该命令用于从三未密码卡中删除一个管理员。请注意最后一个管理员不能被删除。

pin	该参数指定管理员 Ukey 的 PIN 码。
confirmed	可选，指定该参数后，将直接删除管理员，不再提示用户是否要删除管理员。

ssl gmsdf sanwei operator <pin> [force]

该命令用于向三未密码卡添加一个操作员。添加操作员成功后，操作员不能自动登录到三未密码卡。操作员需要执行 “**ssl gmsdf sanwei login**” 命令登录到三未密码卡。系统支持最多添加 1 个操作员。

pin	该参数指定操作员 Ukey 的 PIN 码。添加操作员后，建议使用命令 “ ssl gmsdf sanwei changepin ” 修改操作员的默认 PIN 码。
force	可选。该参数用于强制改写三未密码卡的 Ukey。

no ssl gmsdf sanwei operator <pin>

该命令用于从三未密码卡中删除一个操作员。

ssl gmsdf sanwei login <pin>

该命令用于让用户登录到三未密码卡。当用户插入自己的 Ukey 后，三未密码卡自动识别并允许用户登录。

pin 该参数指定用户 Ukey 的 PIN 码。

ssl gmsdf sanwei logout <user_type> <pin>

该命令用于注销三未密码卡中的用户（管理员和操作员）。任意已添加到三未密码卡的管理员和操作员都可以执行该命令。

user_type 该参数指定要注销的用户类型。取值必须为：

- **admin:** 表示注销所有的管理员。
- **operator:** 表示注销所有的操作员。
- **all:** 表示注销所有的管理员和操作员。

pin 该参数指定用户 Ukey 的 PIN 码。

ssl gmsdf sanwei changepin <old_pin> <new_pin>

该命令用于修改用户 Ukey 的 PIN 码。

old_pin 该参数指定用户 Ukey 的已有 PIN 码。Ukey PIN 码的默认值为“12345678”。

new_pin 该参数指定用户 Ukey 的新 PIN 码。取值必须为长度为 8 个字符（包括字母、数字和符号）的字符串。

9.15.3 国芯密码卡

设备通过支持 SM2/SM3/SM4 算法的国产密码算法的国芯密码卡进行安全通信，目前国芯密码卡只支持对 SM2 虚拟主机上的 SSL 通信进行加解密。

国芯密码卡中的用户包括管理员和操作员，每个用户持有一个智能密码钥匙（USB Key, Ukey）。当设备启动或重启后，国芯密码卡的所有用户都会被自动注销。

ssl gmsdf guoxin admin <username>

该命令用于向国芯密码卡添加一个管理员。当一个管理员添加成功后，需要拔出该管理员的 Ukey，插入下一个管理员的 Ukey，添加下一个管理员。

username 该参数指定国芯密码卡的管理员名称。

no ssl gmsdf guoxin admin <username>

该命令用于从国芯密码卡中删除一个管理员。

ssl gmsdf guoxin operator <username>

该命令用于向国芯密码卡添加一个操作员。添加操作员成功后，操作员不能自动登录到国芯密码卡。操作员需要执行“**ssl gmsdf guoxin login**”命令登录到国芯密码卡。

username 该参数指定国芯密码卡的操作员名称。

no ssl gmsdf guoxin operator <username>

该命令用于从国芯密码卡中删除一个操作员。

ssl gmsdf guoxin login admin <username>

该命令用于让用户以管理员的身份登录到国芯密码卡。

username 该参数指定国芯密码卡的管理员名称。

ssl gmsdf guoxin login operator <username>

该命令用于让用户以操作员的身份登录到国芯密码卡。

username 该参数指定国芯密码卡的操作员名称。

ssl gmsdf guoxin logout <user_type>

该命令用于注销国芯密码卡中的用户（管理员和操作员）。已添加到国芯密码卡的管理员和操作员都可以执行该命令。

user_type 该参数指定要注销的用户类型。取值必须为：

- admin: 表示注销所有的管理员。
- operator: 表示注销所有的操作员。

ssl gmsdf guoxin changepin

该命令用于修改用户 Ukey 的 PIN 码。执行该命令后将提示插入 Ukey 并输入当前 PIN 码，输入正确后提示用户输入新的 PIN 码。

第10章 SSL 侦听

10.1 SSL 侦听功能和证书配置

ssli on <host_name> <distribution_mode>

该命令用于为指定 SSL 虚拟主机或后台主机启用 SSL 侦听功能，并指定入口节点和出口节点的分布方式。管理员可以通过“**show ssl status host**”命令查看 SSL 主机上 SSL 侦听功能的启用状态。

host_name	该参数指定 SSL 虚拟主机或后台主机的名称。
distribution_mode	该参数指定入口节点和出口节点分布模式，取值必须为： 0：表示入口节点和出口节点分布于两台设备上。 1：表示入口节点和出口节点集成于一台设备上。



注意：

1. 启用 SSL 侦听后，客户端认证和重协商功能将自动被禁用。另外 SSL 主机支持的协议版本会变为“SSLv3:TLSv1:TLSv1.1:TLSv1.2”，密码套件也会变为这四种协议版本所支持的密码套件，且不能修改。
2. SM2 虚拟主机和后台主机不支持 SSL 侦听功能。

ssli off <host_name>

该命令用于为指定 SSL 虚拟主机或后台主机禁用 SSL 侦听功能。

ssli cacert rsa <virtual_host_name> [key_length] [certificate_index]
[signature_algorithm_index]

该命令用于为指定 SSL 虚拟主机生成一个 RSA CA 证书和私钥。通过该命令生成的证书可以通过“**ssl activate certificate**”、“**no ssl certificate**”和“**show ssl certificate**”命令激活、删除和查看。

virtual_host_name	该参数指定 SSL 虚拟主机的名称。
key_length	可选，该参数指定生成的 RSA 密钥对的长度，单位为比特。取值必须为 512、1024、2048 或 4096（只有特定型号的设备支持 4096 比特证书）。 默认值为 2048。
certificate_index	可选，该参数指定生成的证书的索引号，取值必须为 1、2 或 3。

默认值为 1。

signature_algorithm_index 可选，该参数指定证书签名算法的索引号，取值必须为 1、2、3 或 4，分别对应 sha256RSA、sha384RSA、sha512RSA 和 sha1RSA 签名算法。

默认值为 1。

ssli cacert ecc <virtual_host_name> [curve_name] [certificate_index] [signature_algorithm_index]

该命令用于为指定 SSL 虚拟主机生成一个 ECC CA 证书和私钥。通过该命令生成的证书可以通过“**ssl activate certificate**”、“**no ssl certificate**”和“**show ssl certificate**”命令激活、删除和查看。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

curve_name 可选，该参数指定椭圆曲线名称，取值必须为 prime256v1、secp384r1 或 secp521r1。

默认值为 prime256v1。

certificate_index 可选，该参数指定生成的证书的索引号，取值必须为 1、2 或 3。

默认值为 1。

signature_algorithm_index 可选，该参数指定证书签名算法的索引号。取值必须为 1、2、3 或者 4，分别对应 sha256ECDSA、sha384ECDSA、sha512ECDSA 和 sha1ECDSA 签名算法。

默认值为 1。

ssli settings certcache timeout <timeout>

该命令用于设置模拟证书的缓存超时时间。如不配置该命令，虚拟证书的缓存超时时间默认为 1800s。如果在指定时间内，模拟证书未被再次命中，则会被移出缓存。

timeout 该参数指定模拟证书的缓存超时时间，取值必须为 60 至 86,400 之间的整数，单位为秒。

系统支持缓存的模拟证书个数取决于系统内存的大小：

表10 - 1 不同系统内存支持缓存的模拟证书个数

系统内存	支持缓存的模拟证书个数
4 GB/8 GB	40,000
16GB/24 GB	80,000

32 GB	160,000
64 GB/96 GB/128 GB	320,000

show ssl settings

该命令用于显示 SSL 侦听功能的所有全局配置。

10.2 域名列表

通过域名列表功能，管理员可以为 SSL 侦听虚拟主机应用旁路或侦听类型的域名列表或字符串，旁路类型和侦听类型的域名列表（字符串）是互斥的，在同一个虚拟主机上不能同时配置。当客户端请求的 SNI 或服务器证书的 Common Name 或 SAN（Subject Alternative Name）匹配到旁路类型的域名列表或字符串时，虚拟主机将允许 SSL 流量以密文形式通过。当客户端请求的 SNI 或服务器证书的 Common Name 或 SAN 匹配到侦听类型的域名列表或字符串时，虚拟主机将对 SSL 流量侦听。

ssli domainlist {on|off}

该命令用于启用或禁用域名列表功能。该功能的默认设置为禁用。



注意：入口节点只在获取服务器证书时进行域名列表的匹配，所以在系统运行了一段时间后新增的域名列表配置可能不会对已经缓存的证书生效。管理员可以通过将证书缓存超时时间（通过“**ssli settings certcache timeout**”命令配置）设置为最小值“60”来避免上述情况。

show ssl domainlist status

该命令用于显示域名列表功能的开启状态。

ssli domainlist list <list_name> <list_type>

该命令用于创建一个域名列表。系统允许创建最多 256 个域名列表。

list_name 该参数指定域名列表的名称，取值必须为长度不大于 64 个字节的字符串，区分大小写。

list_type 该参数指定域名列表的类型，取值必须为：

- **bypass**：表示创建一个旁路类型的域名列表。
- **intercept**：表示创建一个侦听类型的域名列表。

no ssl domainlist list <list_name>

该命令用于删除指定的域名列表及其包含的所有项目。

show ssl domainlist list [list_type]

该命令用于显示指定类型的域名列表。

list_type 该参数指定需要显示的域名列表类型，取值必须为：

- **bypass**：表示显示旁路类型的域名列表。
- **intercept**：表示显示侦听类型的域名列表。
- **all**：表示显示所有类型的域名列表。

默认值为“all”。

clear ssli domainlist list [list_type]

该命令用于清除所有已配置的域名列表及其包含的所有项目。

list_type 该参数指定需要清除的域名列表类型，取值必须为：

- **bypass**：表示清除旁路类型的域名列表。
- **intercept**：表示清除侦听类型的域名列表。
- **all**：表示清除所有类型的域名列表。

默认值为“all”。

ssli domainlist item <list_name> <sni_regex>

该命令用于向一个域名列表中添加域名字符串项目。每个域名列表允许包含最多 1024 个域名字符串项目。

list_name 该参数指定 SNI 列表的名称。

sni_regex 该参数指定需要添加到 SNI 列表中的域名字符串项目，取值必须为长度不超过 64 个字节的字符串，不区分大小写。该参数取值支持使用快速正则表达式，格式为 “[^]string.[*string2[*stringN]][\$]”，置于双引号内。关于快速正则表达式的介绍，请参见第一章“正则表达式”小节。

no ssli domainlist item <list_name> <sni_regex>

该命令用于从指定的域名列表中删除指定的域名字符串项目。

show ssli domainlist item <list_name>

该命令用于显示指定域名列表中的所有域名字符串项目。

clear ssli domainlist item <list_name>

该命令用于清除指定域名列表中的所有域名字符串项目。

ssli domainlist apply list <virtual_host_name> <list_name>

该命令用于为指定虚拟主机应用一个域名列表。每个虚拟主机可以应用最多 256 个域名列表。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

list_name 该参数指定域名列表的名称。



注意：如果已经为虚拟主机应用了旁路类型的域名列表或域名字符串，则不能再应用侦听类型的域名列表或域名字符串，反之亦然。

no ssli domainlist apply list <virtual_host_name> <list_name>

该命令用于删除指定虚拟主机与域名列表之间的应用关系。

ssli domainlist apply item <virtual_host_name> <sni_regex> <item_type>

该命令用于为指定虚拟主机应用一个旁路或侦听类型的域名字符串，每个 SSL 虚拟主机可以单独应用最多 1024 个域名字符串。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

sni_regex 该参数指定域名字符串，取值必须为长度不超过 64 个字节的字符串，不区分大小写。该参数取值支持使用快速正则表达式，格式为 “[^]string.[*string2[*stringN]][\$]”，置于双引号内。关于快速正则表达式的介绍，请参见第一章“正则表达式”小节。

item_type 该参数指定需要应用的域名字符串的类型，取值必须为：

- **bypass:** 表示应用一个旁路类型的域名字符串。
- **intercept:** 表示应用一个侦听类型的域名字符串。



注意：如果已经为虚拟主机应用了旁路类型的域名列表或域名字符串，则不能再应用侦听类型的域名列表或域名字符串，反之亦然。

no ssli domainlist apply item <virtual_host_name><sni_regex>

该命令用于删除指定虚拟主机与域名字符串的应用关系。

show ssli domainlist apply <virtual_host_name> [type]

该命令用于显示应用于指定虚拟主机的所有域名字符串和（或）域名列表。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

type 可选，该参数指定需要显示的域名列表类型，取值必须为：

- item: 只显示通过 “**ssli domainlist apply item**” 命令应用于虚拟主机的域名字符串。
- list: 只显示通过 “**ssli domainlist apply list**” 命令应用于虚拟主机的域名列表。
- all: 显示虚拟主机上应用的所有域名字符串和域名列表。

默认值为 “all”。

clear ssli domainlist apply <virtual_host_name> [type]

该命令用于清除指定虚拟主机与所有域名字符串和（或）域名列表的关联关系。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

type 可选，该参数指定需要清除的关联类型，取值必须为：

- item: 只清除通过 “**ssli domainlist apply item**” 命令应用于虚拟主机的域名字符串。
- list: 只清除通过 “**ssli domainlist apply list**” 命令应用于虚拟主机的域名列表。
- all: 清除应用于虚拟主机的所有域名字符串和域名列表。

默认值为 “all”。

show statistics ssli domainlist [virtual_host_name]

该命令用于显示指定虚拟主机上域名列表的匹配统计数据。如果匹配的域名列表的名称显示为 “-”，则表示该域名是单独应用到虚拟主机上的。如不指定参数 “virtual_host_name”，则显示所有虚拟主机的域名列表匹配统计数据。

clear statistics ssli domainlist [virtual_host_name]

该命令用于清除指定虚拟主机上域名列表的匹配统计数据。如不指定参数 “virtual_host_name”，则清除所有虚拟主机上域名列表的匹配统计数据。

show ssli domainlist match <virtual_host_name> <domain_name>

该命令用于测试指定虚拟主机上是否应用了指定的域名。。

virtual_host_name 该参数指定 SSL 虚拟主机的名称。

domain_name 该参数指定需要测试的域名。

10.3 URL 过滤

ssli webclassify {on|off} <virtual_host_name>

该命令用于为 SSL 侦听模块的指定虚拟主机启用或禁用网站分类功能实现智能的 URL 过滤。该功能仅在全局网站分类功能启用（“**webclassify on**”）且该主机启用 SSL 侦听功能后才生效。关于全局网站分类功能的命令的说明，请参考第 2 章中的“网站分类”小节。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机的名称，取值必须为入口节点上 TCPS 虚拟服务所关联的虚拟主机名称。

ssli webclassify defaction <virtual_host_name> <action>

该命令用于配置指定的虚拟主机对访问无法判断类别的网站的流量进行旁路或侦听。如不配置该命令，系统默认不对此类流量进行侦听。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机名称，取值必须为入口节点上 TCPS 虚拟服务所关联的虚拟主机名称。

action 该参数指定处理方式，取值必须为：

- 0：表示对访问无法判断类别的网站的流量进行旁路。
- 1：表示对访问无法判断类别的网站的流量进行侦听。

ssli webclassify url bypass <virtual_host_name> <category_name>

该命令用于为指定虚拟主机配置一个需要旁路的网站类别，即不侦听所有访问该网站类别内网址的流量。该配置的作用等同于旁路类型的域名列表（字符串），当虚拟主机既有域名列表（字符串）也有网站类别配置时，系统会优先匹配域名列表（字符串）。

在同一个虚拟主机上，“**ssli webclassify url bypass**”和“**ssli webclassify url intercept**”命令不能同时配置。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机的名称，取值必须为入口节点上 TCPS 虚拟服务所关联的虚拟主机名称。

category_name 该参数指定网站类别，取值必须为网站类别的名称，置于双引号内，区分大小写，例如“Real Estate”。系统支持的网站类别的名称如下：

- Real Estate (Category ID: 1)
- Computer and Internet Security (Category ID: 2)

- Financial Services (Category ID: 3)
- Business and Economy (Category ID: 4)
- Computer and Internet Info (Category ID: 5)
- Auctions (Category ID: 6)
- Shopping (Category ID: 7)
- Cult and Occult (Category ID: 8)
- Travel (Category ID: 9)
- Abused Drugs (Category ID: 10)
- Adult and Pornography (Category ID: 11)
- Home (Category ID: 12)
- Military (Category ID: 13)
- Social Network Category ID: 14)
- Dead Sites (Category ID: 15)
- Individual Stock Advice and Tools (Category ID: 16)
- Training and Tools (Category ID: 17)
- Dating (Category ID: 18)
- Sex Education (Category ID: 19)
- Religion (Category ID: 20)
- Entertainment and Arts (Category ID: 21)
- Personal Sites and Blogs (Category ID: 22)
- Legal (Category ID: 23)
- Local Information (Category ID: 24)
- Streaming Media (Category ID: 25)
- Job Search (Category ID: 26)
- Gambling (Category ID: 27)
- Translation (Category ID: 28)
- Reference and Research (Category ID: 29)
- Shareware and Freeware (Category ID: 30)

- P2P (Category ID: 31)
- Marijuana (Category ID: 32)
- Hacking (Category ID: 33)
- Games (Category ID: 34)
- Philosophy and Political Advocacy (Category ID: 35)
- Weapons (Category ID: 36)
- Pay to Surf (Category ID: 37)
- Hunting and Fishing (Category ID: 38)
- Society (Category ID: 39)
- Educational Institutions (Category ID: 40)
- Online Greeting cards (Category ID: 41)
- Sports (Category ID: 42)
- Swimsuits & Intimate Apparel (Category ID: 43)
- Questionable (Category ID: 44)
- Kids (Category ID: 45)
- Hate and Racism (Category ID: 46)
- Online Personal Storage (Category ID: 47)
- Violence (Category ID: 48)
- Keyloggers and Monitoring (Category ID: 49))
- Search Engines (Category ID: 50)
- Internet Portals (Category ID: 51)
- Web Advertisements (Category ID: 52)
- Cheating (Category ID: 53)
- Gross (Category ID: 54)
- Web based Email (Category ID: 55)
- Malware Sites (Category ID: 56)
- Phishing and Other Frauds (Category ID: 57)
- Proxy Avoid and Anonymizers (Category ID: 58)

- Spyware and Adware (Category ID: 59)
- Music (Category ID: 60)
- Government (Category ID: 61)
- Nudity (Category ID: 62)
- News and Media (Category ID: 63)
- Illegal (Category ID: 64)
- CDNs (Category ID: 65)
- Internet Communications (Category ID: 66)
- Bot Nets (Category ID: 67)
- Abortion (Category ID: 68)
- Health & Medicine (Category ID: 69)
- Confirmed SPAM Sources (Category ID: 70)
- SPAM URLs (Category ID: 71)
- Unconfirmed SPAM Sources (Category ID: 72)
- Open HTTP Proxies (Category ID: 73)
- Dynamic Content (Category ID: 74)
- Parked Sites (Category ID: 75)
- Alcohol and Tobacco (Category ID: 76)
- Private IP Addresses (Category ID: 77)
- Image and Video Search (Category ID: 78)
- Fashion and Beauty (Category ID: 79)
- Recreation and Hobbies (Category ID: 80)
- Motor Vehicles (Category ID: 81)
- Web Hosting (Category ID: 82)

no ssli webclassify url bypass <virtual_host_name> <category_name>

该命令用于删除指定虚拟主机的一条“**ssli webclassify url bypass**”配置。

clear ssli webclassify url bypass <virtual_host_name>

该命令用于清除指定虚拟主机的所有“**ssli webclassify url bypass**”配置。

ssli webclassify url intercept <virtual_host_name> <category_name>

该命令用于为指定虚拟主机配置一个侦听类型的网站类别，即侦听所有访问该类别内网址的流量。侦听类型的网站类别在功能上等同于侦听类型的域名列表（字符串），但是匹配优先级低于域名列表（字符串）。当虚拟主机既有 SNI 列表也有网站类别配置时，系统会优先匹配域名列表（字符串）。

在同一个虚拟主机上，“**ssli webclassify url bypass**”和“**ssli webclassify url intercept**”命令不能同时配置。

virtual_host_name 该参数指定已存在的 SSL 虚拟主机的名称，取值必须为入口节点上 TCPS 虚拟服务所关联的虚拟主机名称。

category_name 该参数指定网站类别，取值必须为网站类别的名称，置于双引号内，区分大小写，例如“Real Estate”。系统支持的网站类别的名称如下：

- Real Estate (Category ID: 1)
- Computer and Internet Security (Category ID: 2)
- Financial Services (Category ID: 3)
- Business and Economy (Category ID: 4)
- Computer and Internet Info (Category ID: 5)
- Auctions (Category ID: 6)
- Shopping (Category ID: 7)
- Cult and Occult (Category ID: 8)
- Travel (Category ID: 9)
- Abused Drugs (Category ID: 10)
- Adult and Pornography (Category ID: 11)
- Home (Category ID: 12)
- Military (Category ID: 13)
- Social Network Category ID: 14)
- Dead Sites (Category ID: 15)
- Individual Stock Advice and Tools (Category ID: 16)
- Training and Tools (Category ID: 17)
- Dating (Category ID: 18)

- Sex Education (Category ID: 19)
- Religion (Category ID: 20)
- Entertainment and Arts (Category ID: 21)
- Personal Sites and Blogs (Category ID: 22)
- Legal (Category ID: 23)
- Local Information (Category ID: 24)
- Streaming Media (Category ID: 25)
- Job Search (Category ID: 26)
- Gambling (Category ID: 27)
- Translation (Category ID: 28)
- Reference and Research (Category ID: 29)
- Shareware and Freeware (Category ID: 30)
- P2P (Category ID: 31)
- Marijuana (Category ID: 32)
- Hacking (Category ID: 33)
- Games (Category ID: 34)
- Philosophy and Political Advocacy (Category ID: 35)
- Weapons (Category ID: 36)
- Pay to Surf (Category ID: 37)
- Hunting and Fishing (Category ID: 38)
- Society (Category ID: 39)
- Educational Institutions (Category ID: 40)
- Online Greeting cards (Category ID: 41)
- Sports (Category ID: 42)
- Swimsuits & Intimate Apparel (Category ID: 43)
- Questionable (Category ID: 44)
- Kids (Category ID: 45)
- Hate and Racism (Category ID: 46)

- Online Personal Storage (Category ID: 47)
- Violence (Category ID: 48)
- Keyloggers and Monitoring (Category ID: 49)
- Search Engines (Category ID: 50)
- Internet Portals (Category ID: 51)
- Web Advertisements (Category ID: 52)
- Cheating (Category ID: 53)
- Gross (Category ID: 54)
- Web based Email (Category ID: 55)
- Malware Sites (Category ID: 56)
- Phishing and Other Frauds (Category ID: 57)
- Proxy Avoid and Anonymizers (Category ID: 58)
- Spyware and Adware (Category ID: 59)
- Music (Category ID: 60)
- Government (Category ID: 61)
- Nudity (Category ID: 62)
- News and Media (Category ID: 63)
- Illegal (Category ID: 64)
- CDNs (Category ID: 65)
- Internet Communications (Category ID: 66)
- Bot Nets (Category ID: 67)
- Abortion (Category ID: 68)
- Health & Medicine (Category ID: 69)
- Confirmed SPAM Sources (Category ID: 70)
- SPAM URLs (Category ID: 71)
- Unconfirmed SPAM Sources (Category ID: 72)
- Open HTTP Proxies (Category ID: 73)
- Dynamic Content (Category ID: 74)

- Parked Sites (Category ID: 75)
- Alcohol and Tobacco (Category ID: 76)
- Private IP Addresses (Category ID: 77)
- Image and Video Search (Category ID: 78)
- Fashion and Beauty (Category ID: 79)
- Recreation and Hobbies (Category ID: 80)
- Motor Vehicles (Category ID: 81)
- Web Hosting (Category ID: 82)

no ssl webcl url intercept <virtual_host_name> <category_name>

该命令用于删除指定虚拟主机的一条“**ssl webclassify url intercept**”配置。

clear ssl webcl url intercept <virtual_host_name>

该命令用于清除指定虚拟主机的所有“**ssl webclassify url intercept**”配置。

show ssl webclassify settings <virtual_host_name>

该命令用于显示 SSL 侦听模块指定虚拟主机上网址分类功能的启用状态、旁路类型或侦听类型的网站类别配置以及“**ssl webclassify defaction**”命令的配置。

show statistics ssl webclassify <virtual_host_name>

该命令用于显示 SSL 侦听模块指定虚拟主机上网址分类功能相关的统计数据，包括网站类别命中次数以及通过本地数据库、缓存和在线查询网址类别的记录数据以及“**ssl webclassify defaction**”命令的匹配数据。

clear statistics ssl webclassify

该命令用于清除 SSL 侦听模块指定虚拟主机上网址分类功能相关的统计数据，包括网站类别命中次数以及通过本地数据库、缓存和在线查询网址类别的记录数据以及“**ssl webclassify defaction**”命令的匹配数据。

第11章 安全应用访问 (SAA)

11.1 AAA

aaa {on|off} <virtual_service>

该命令用于为指定的虚拟服务启用或禁用 AAA 功能。启用 AAA 功能后，用户必须登录后才能获取内部资源。禁用该功能后，用户无需认证即可以获得授权的资源。该功能的默认设置为对所有虚拟服务禁用。

virtual_service 该参数指定已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。



注意： 启用了 HTTP/2 协议的虚拟服务不支持 AAA 功能。

show aaa status [virtual_service]

该命令用于显示指定虚拟服务上 AAA 功能的开启状态。如不指定参数 “virtual_service”，则显示所有虚拟服务上 AAA 功能的开启状态。

aaa server <type> <server_name> [display_string]

该命令用于定义一个指定类型的 AAA 服务器。系统支持 SAML SP、RADIUS LDAP 和 OAuth 类型的 AAA 服务器。每种类型的 AAA 服务器最多配置 32 个。

type 该参数指定 AAA 服务器的类型，取值必须为“samlsp”、“radius”、“ldap”或“oauth”。

server_name 该参数指定 AAA 服务器的名称，取值必须为长度不大于 32 个字节的字符串。

display_string 可选。该参数指定 AAA 服务器在登录页面的显示字符串，取值必须为长度不大于 127 个字节的字符串。

如不设置该参数，默认值与 “server_name” 参数的取值相同。

no aaa server <server_name>

该命令用于删除指定的 AAA 服务器。

server_name 该参数指定已存在的 AAA 服务器的名称。

show aaa server [type]

该命令用于显示指定类型的 AAA 服务器。

type 可选。该参数指定 AAA 服务器的类型，取值必须为 “samlsp”、“radius”、“ldap”、“oauth” 或空。如不指定该参数，则显示所有类型的 AAA 服务器。

默认值为空。

aaa method server <method_name> <authentication_server> [authorization_server] [display_string]

该命令用于将指定认证服务器（和授权服务器）定义为一种 AAA 方案。

method_name 该参数指定 AAA 方案的名称，取值必须为长度不大于 32 个字节的字符串，不区分大小写。当参数取值以数字开头时，必须置于双引号内。

authentication_server 该参数指定认证服务器，取值必须为已存在的 AAA 服务器的名称。系统支持设置最多三个认证服务器，可以为相同类型也可以为不同类型。当设置两个或三个认证服务器时，各个服务器名称之间需用逗号分隔，整个取值置于双引号内，例如 “auth_server1, auth_server2, auth_server3”。

authorization_server 该参数指定授权服务器。

当参数 “authentication_server” 仅指定了一个认证服务器时，该参数可以设置为一个已存在 AAA 服务器的名称、“none” 或空。取值 “none” 表示略过授权步骤，取值为空表示授权服务器和认证服务器相同。默认值为空。

当参数 “authentication_server” 指定了两个或三个认证服务器时，该参数必须设置为一个已存在的 AAA 服务器的名称或 “none”。

display_string 可选。该参数指定登录页面上 AAA 方案的显示字符串，如不设置该参数，默认值与 “method_name” 参数的取值相同。



注意：

1. SAML SP 服务器不能和其他类型的服务器（例如 LDAP、RADIUS 和 OAuth 服务器）配合使用。
2. 如果通过该命令设置了一个认证服务器后设置了一个不同于认证服务器的授权服务器，那么两个服务器的用户名和密码必须相同。

no aaa method server <method_name>

该命令用于删除指定的 AAA 方案。

show aaa method server [method_name]

该命令用于显示指定的 AAA 方案配置。如不指定参数 “method_name”，则显示所有的 AAA 方案配置。

aaa method bind <method_name> <virtual_service>

该命令用于将指定的 AAA 方案与指定虚拟服务关联，每个虚拟服务最多可关联五种 AAA 方案。

method_name	该参数指定已存在的 AAA 方案的名称。
virtual_service	该参数指定已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。

no aaa method bind <method_name> <virtual_service>

该命令用于删除指定的 AAA 方案与指定虚拟服务的关联关系。

show aaa method bind [method_name]

该命令用于显示指定 AAA 方案关联的虚拟服务。如不指定参数 “method_name”，则显示所有 AAA 方案关联的虚拟服务。

clear aaa method bind [method_name]

该命令用于清除指定 AAA 方案与虚拟服务的关联关系。如不指定参数 “method_name”，则清除所有 AAA 方案与虚拟服务的关联关系。

aaa method rank {on|off} <virtual_service>

该命令用于为指定的虚拟服务启用或禁用 AAA 方案排序功能。启用该功能后，如果一个虚拟服务上绑定了多个 AAA 方案，系统会按照绑定顺序排序，登录界面会显示最先绑定的 AAA 方案。如果禁用该功能，所有 AAA 方案都会显示在登录界面，用户可以选择任意一个 AAA 方案进行认证。该功能的默认设置为对所有虚拟服务禁用。

virtual_service	该参数指定已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。

aaa role name <role_name> [description]

该命令用于添加一个用户角色。当参数 “role_name” 的取值为一个已存在的用户角色时，该命令还可以用来修改该用户角色的配置。系统支持配置最多 256 个用户角色。

role_name	该参数指定需要添加的用户角色名称，取值必须为长度不大于 127 个字节的字符串。
description	可选。该参数指定用户角色相关描述信息，取值必须为

长度不大于 255 个字节的字符串。

默认值为空。

no aaa role name <role_name>

该命令用于删除指定的用户角色。

show aaa role name [role_name]

该命令用于显示指定的用户角色。如不指定参数“role_name”，则显示所有的用户角色。

clear aaa role name

该命令用于清除所有的用户角色。

aaa role qualification <role_name> <qual_name> [description]

该命令用于为指定的用户角色添加一条限制规则。每个用户可以添加最多 32 条限制规则。

role_name	该参数指定已存在的用户角色名称。
qual_name	该参数指定限制规则的名称，取值必须为长度不大于 127 个字节的字符串。
description	可选。该参数指定限制规则相关描述信息，取值必须为长度不大于 255 个字节的字符串。 默认值为空。

no aaa role qualification <role_name> <qual_name>

该命令用于删除指定用户角色的一条限制规则配置。

show aaa role qualification [role_name]

该命令用于显示指定用户角色的限制规则配置。如不指定参数“role_name”，则显示所有用户角色的限制规则配置。

clear aaa role qualification

该命令用于清除所有用户角色的限制规则配置。

aaa role condition <role_name> <qual_name> <condi_string>

该命令用于为指定用户角色和限制规则添加一条限定条件。如果一条限制规则关联了多条限定条件，终端用户只有在同时满足限制规则内的所有限定条件时才能获取指定用户角色。每个限制规则内可以添加最多 32 条限定条件。

role_name	该参数指定已存在的用户角色名称。

qual_name	该参数指定已存在的限制规则的名称。
condi_string	该参数指定限定条件字符串，取值必须为长度不大于 511 个字节的字符串，全大写，置于双引号内，格式为“condition string [IS NOT] [value]”。“condition string”和“value”的取值请参考下表。

示例：

假设为每个月第一天登录的所有用户分配用户角色“stuff”，该用户角色已经关联了一个名为“work”的限制规则，那么可以执行以下命令为用户角色“stuff”和限制规则“work”添加限定条件。

```
Demo(config)#aaa role condition stuff work "LOGINDAY IS 1"
```

下表列出了系统支持的限定条件字符串。

表11 - 1 限定条件字符串

条件字符串	含义	取值
LOGINYEAR	终端用户登录时的年份。	1970 至 2999
LOGINMONTH	终端用户登录时的月份。	1 至 12
LOGINDAY	终端用户登录时的日期。	1 至 31
LOGINWEEK	终端用户登录时的星期名称。	1 至 7
LOGINDATE	终端用户登录时的年份、月份、日期、小时和分钟数。	yyyyMMddhhmm
LOGINTIME	终端用户登录时的小时和分钟数。	00:00 至 23:59
USERNAME	终端用户登录的用户名。	字母数字字符、特殊字符、可打印的 ASCII 字符和多字节字符。
GROUPNAME	终端用户所属的群组。	字母数字字符、特殊字符、可打印的 ASCII 字符和多字节字符。
AUTHMETHOD	认证方法。	字母数字字符、特殊字符、可打印的 ASCII 字符和多字节字符。
SRCIP	终端用户的源 IP 地址。	IPv4 或 IPv6 地址，例如： 10.10.10.0/24 10.10.10.0/255.255.255.0 10.10.10.1 2012:1030::1 2012:1030::1/64

no aaa role condition <role_name> <qual_name>

该命令用于删除指定用户角色和限制规则的所有的限定条件配置。

show aaa role condition [role_name]

该命令用于显示指定用户角色的所有限制规则和限定条件配置。如不指定参数“role_name”，则显示所有用户角色的限制规则和限定条件配置。

aaa role bind <role_name> <virtual_service>

该命令用于将指定用户角色与指定虚拟服务关联，每个虚拟服务可以关联最多 32 个用户角色。

role_name	该参数指定已存在的用户角色名称。
virtual_service	该参数指定已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。

no aaa role bind <role_name> <virtual_service>

该命令用于删除指定用户角色与指定虚拟服务的关联关系。

show aaa role bind [role_name]

该命令用于显示指定用户角色关联的虚拟服务。如不指定参数“role_name”，则显示所有用户角色关联的虚拟服务。

clear aaa role bind [role_name]

该命令用于清除指定用户角色与所有虚拟服务的关联关系。如不指定参数“role_name”，则清除所有用户角色和虚拟服务的关联关系。

show aaa all

该命令用于显示 AAA 功能相关的所有配置，包括 SAMLSP、LDAP、RADIUS 和 OAuth 相关配置。

clear aaa all

该命令用于清除 AAA 功能相关的所有配置，并将 AAA 功能和 AAA 方案排序功能恢复为默认配置。

11.1.2 SAML

aaa samlsp idp metadata <server_name> <url>

该命令用于为指定的 SAML SP 服务器导入 IdP（Identity Provider，身份提供者）服务器的元数据文件。注意，如果 IdP 服务器的元数据文件有更改，需执行该命令重新导入更新后的文件，新文件将覆盖原有文件。

server_name	该参数指定已存在的 SAML SP 服务器的名称。
url	该参数指定 IdP 服务器的元数据文件的下载地址，取值必须为长度不大于 900 个字节的字符串，支持 HTTP、

HTTPS 和 FTP 类型的 URL。

no aaa samlsp idp metadata <server_name>

该命令用于删除指定 SAML SP 服务器上的 IdP 服务器的元数据文件。

show aaa samlsp idp metadata <server_name>

该命令用于显示指定 SAML SP 服务器上的 IdP 服务器的元数据文件的内容。

show aaa samlsp sp metadata <server_name> [virtual_service]

该命令用于显示与指定虚拟服务关联的 SAML SP 服务器的元数据文件的下载地址。如不指定参数“virtual_service”，则显示与所有虚拟服务关联的 SAML SP 服务器的元数据文件的下载地址。

aaa samlsp idp attributes <server_name> <username> [password]

该命令用于为指定的 SAML SP 服务器配置用于获取用户身份信息的属性名称，目前系统仅支持设置用户名属性。当 IdP 服务器返回 SAML 响应时，SAML SP 服务器会根据配置的属性从响应中提取用户名来获取用户身份。

该配置会被保存到 SAML SP 服务器的元数据文件中，如果发生更改，需同时更新 IdP 服务器端的 SAML SP 服务器的元数据文件，否则更改不生效。

server_name	该参数指定已存在的 SAML SP 服务器的名称。
username	该参数指定用户名属性，取值必须为长度不大于 900 个字节的字符串。该参数取值也可以设置为“subject.nameid”，表示 SAML 响应中的 NameID 字段。当该命令用于支持 Web SSO 时，该参数取值必须为“uid”，表示用户名字段。
password	可选。该参数指定密码属性，取值必须为长度不大于 900 个字节的字符串。该参数仅在使用 Web SSO 功时才需要配置。

aaa samlsp sp acs <server_name> [type]

该命令用于为指定的 SAML SP 服务器配置 ACS 服务支持的协议绑定类型，IdP 服务器会通过配置的协议绑定方式将 SAML 断言响应发送给 SAML SP 服务器的 ACS（Assertion Consumer Service）模块。

该配置会被保存到 SAML SP 服务器的元数据文件中，如果发生更改，需同时更新 IdP 服务器端的 SAML SP 服务器的元数据文件，否则更改不生效。

server_name	该参数指定已存在的 SAML SP 服务器的名称。
type	可选，该参数指定 ACS 服务支持的协议绑定类型，取

值必须为:

- post: 表示 HTTP POST 协议绑定类型。
- artifact: 表示 HTTP Artifact 协议绑定类型。

默认值为 “post”。

aaa samlsp sp slo <server_name> [type]

该命令用于为指定的 SAML SP 服务器配置 SLO (Single Logout, 单点注销) 服务支持的协议绑定类型, IdP 服务器会通过配置的协议绑定方式与 SAMP SP 服务器的 SLO 服务通信。

该配置会被保存到 SAML SP 服务器的元数据文件中, 如果发生更改, 需同时更新 IdP 服务器端的 SAML SP 服务器的元数据文件, 否则更改不生效。

server_name 该参数指定已存在的 SAML SP 服务器的名称。

type 可选, 该参数指定 SLO 服务支持的协议绑定类型, 取值必须为:

- redirect: 表示 HTTP Redirect 协议绑定类型。
- post: 表示 HTTP POST 协议绑定类型。
- both: 表示以上两种协议绑定类型。

默认值为 “both”。

show aaa samlsp settings [server_name]

该命令用于显示指定 SAML SP 服务器的所有配置, 具体包括以下命令。如不指定 “server_name” 参数, 则显示所有 SAML SP 服务器上以下命令的配置。

- **aaa saml idp attributes**
- **aaa samlsp sp slo**
- **aaa samlsp sp acs**

clear aaa samlsp settings [server_name]

该命令用于清除指定 SAML SP 服务器的所有配置, 包括导入的 IdP 的元数据文件和以下命令。如不指定 “server_name” 参数, 则清除所有 SAML SP 服务器上导入的 IdP 的元数据文件和以下命令的配置。

- **aaa saml idp attributes**
- **aaa samlsp sp slo**
- **aaa samlsp sp acs**

11.1.3 RADIUS

aaa radius host <radius_server_name> <ip> <authentication_port> <secret>
<retries> <timeout> [index]

该命令用于为指定的 RADIUS 服务器配置一个 RADIUS 主机，每个 RADIUS 服务器最多可以配置三个 RADIUS 主机。

radius_server_name	该参数指定已存在的 RADIUS 服务器的名称。
ip	该参数指定 RADIUS 主机的 IP 地址，系统只支持使用 IPv4 地址的 RADIUS 主机。
authentication_port	该参数指定用于 RADIUS 认证的端口号，取值必须为 1 至 65,535 之间的整数。
secret	该参数指定设备和 RADIUS 服务器之间用于加密密码和交换响应的共享密钥，取值必须为长度不大于 80 个字节的字符串。
retries	该参数指定设备试图连接 RADIUS 服务器时允许的最大尝试次数，取值必须为 1 至 65,535 之间的整数。
timeout	该参数指定超时时间，单位为秒，取值必须为 1 至 65535 之间的整数。
index	可选。该参数指定 RADIUS 主机的索引号，取值必须为 1、2 或 3。 默认值为 1。

no aaa radius host <radius_server_name> <index>

该命令用于删除指定 RADIUS 服务器的一个 RADIUS 主机配置。

show aaa radius host [radius_server_name]

该命令用于显示指定 RADIUS 服务器的 RADIUS 主机配置。如不指定参数“radius_server_name”，则显示所有 RADIUS 服务器的 RADIUS 主机配置。

aaa radius attribute group <radius_server_name> <attribute_id>

该命令用于为指定 RADIUS 服务器设置用于从 RADIUS 记录项中获取终端用户所属的外部 RADIUS 群组的属性，该属性可能随网络环境的变化而不同。

radius_server_name	该参数指定已存在的 RADIUS 服务器的名称。
attribute_id	该参数指定用于获取终端用户所属的外部 RADIUS 群组的属性 ID，系统支持的属性和相应 ID 为：

- 1: User-Name
- 2: User-Password
- 3: CHAP-Password
- 4: NAS-IP-Address
- 5: NAS-Port
- 6: Service-Type
- 7: Framed-Protocol
- 8: Framed-IP-Address
- 9: Framed-IP-Netmask
- 10: Framed-Routing
- 11: Filter-Id
- 12: Framed-MTU
- 13: Framed-Compression
- 14: Login-IP-Host
- 15: Login-Service
- 16: Login-TCP-Port
- 17: (unassigned)
- 18: Reply-Message
- 19: Callback-Number
- 20: Callback-Id
- 21: (unassigned)
- 22: Framed-Route
- 23: Framed-IPX-Network
- 24: State
- 25: Class
- 26: Vendor Specific
- 27: Session Timeout
- 28: Idle-Timeout

- 29: Termination-Action
- 30: Called-Station-Id
- 31: Calling-Station-Id
- 32: NAS-Identifier
- 33: Proxy-State
- 34: Login-LAT-Service
- 35: Login-LAT-Node
- 36: Login-LAT-Group
- 37: Framed-AppleTalk-Link
- 38: Framed-AppleTalk-Network
- 39: Framed-AppleTalk-Zone
- 40:-59 (rev. for accounting)
- 60: CHAP-Challenge
- 61: NAS-Port-Type
- 62: Port-Limit
- 63: Login-LAT-Port

no aaa radius attribute group <radius_server_name>

该命令用于删除指定 RADIUS 服务器的“**aaa radius attribute group**”配置。

show aaa radius attribute group [radius_server_name]

该命令用于显示指定 RADIUS 服务器的“**aaa radius attribute group**”配置。如不指定参数“radius_server_name”，则显示所有 RADIUS 服务器的“**aaa radius attribute group**”配置。

aaa radius defaultgroup <radius_server_name> <group>

该命令用于为指定的 RADIUS 服务器设置一个默认的 RADIUS 群组。对于已经通过认证的终端用户,如果无法从 RADIUS 记录项中获取该用户所属的 RADIUS 群组,则认为该用户属于默认群组。

radius_server_name 该参数指定已存在的 RADIUS 服务器的名称。

group 该参数指定默认 RADIUS 群组的名称,取值必须为长度不大于 80 个字节的字符串。

no aaa radius defaultgroup <radius_server_name>

该命令用于删除指定 RADIUS 服务器的“aaa radius defaultgroup”配置。

show aaa radius defaultgroup [radius_server_name]

该命令用于显示指定 RADIUS 服务器的“aaa radius defaultgroup”配置。如不指定参数“radius_server_name”，则显示所有 RADIUS 服务器的“aaa radius defaultgroup”配置。

aaa radius nasip <radius_server_name> <nasip>

该命令用于为指定 RADIUS 服务器设置或修改 NAS 服务器的 IP 地址。如不配置该命令，系统会按照“port1、port2、port3...”的顺序选择一个可用的接口 IP 地址作为 NAS 的 IP 地址。

radius_server_name 该参数指定已存在的 RADIUS 服务器的名称。

group 该参数指定 NAS 的 IP 地址。



注意：如果系统上只有聚合或 VLAN 接口配置了 IP 地址，而没有任何系统接口配置 IP 地址，那么必须通过该命令配置“NAS-IP-Address”属性。

no aaa radius nasip <radius_server_name>

该命令用于删除指定 RADIUS 服务器的 NAS IP 配置。

show aaa radius nasip [radius_server_name]

该命令用于显示指定 RADIUS 服务器的 NAS IP 配置。如不配置该命令，则显示所有 RADIUS 服务器的 NAS IP 配置。

11.1.4 LDAP

**aaa ldap host <ldap_server_name> <ip> <port> <username> <password>
<base_dn> <timeout> [index] [tls_flag]**

该命令用于为指定的 LDAP 服务器配置一个 LDAP 主机，每个 LDAP 服务器最多可以配置三个 LDAP 主机。

ldap_server_name 该参数指定已存在的 LDAP 服务器的名称。

ip 该参数指定 LDAP 主机的 IP 地址，系统只支持 IPv4 类型的 LDAP 主机。

port 该参数指定 LDAP 主机的端口号，取值必须为 1 至 65,535 之间的整数。

username 该参数指定 LDAP 服务器管理员账户的用户名，取值必

须为长度不大于 127 个字节的字符串。

password	该参数指定 LDAP 服务器管理员账户的密码。
base_dn	该参数指定 LDAP 记录项的 DN，即为用户进行搜索的起始位置，取值必须为长度不大于 900 个字节的字符串。
timeout	该参数指定搜索的超时值，取值必须为 1 至 65536 之间的整数。
index	可选。该参数指定 LDAP 主机的索引号，取值必须为 1、2 或 3。 默认值为 1。
tls_flag	可选。该参数指定是否使用 TLS 协议访问 LDAP 服务器，取值必须为： • tls：表示使用 TLS 协议访问 LDAP 服务器。 • 空：表示不使用 TLS 协议访问 LDAP 服务器。 默认值为空。

no aaa ldap host <ldap_server_name> <index>

该命令用于删除指定 LDAP 服务器的一个 LDAP 主机配置。

show aaa ldap host [ldap_server_name]

该命令用于显示指定 LDAP 服务器的 LDAP 主机配置。如不指定参数“ldap_server_name”，则显示所有 LDAP 服务器的 LDAP 主机配置。

aaa ldap idletime <ldap_server_name> [idle_time]

该命令用于为指定 LDAP 服务器设置闲置超时时间。如果设备与 LDAP 服务器之间的连接闲置时间达到指定的超时时间，连接会断开。

ldap_server_name	该参数指定已存在的 LDAP 服务器的名称。
idle_time	可选，该参数指定闲置连接的超时时间，单位为秒，取值必须为 60 至 3000 之间的整数。 默认值为 600。

no aaa ldap idletime <ldap_server_name>

该命令用于删除指定 LDAP 服务器的超时时间配置。

show aaa ldap idletime [ldap_server_name]

该命令用于显示指定 LDAP 服务器的超时时间配置。如不指定参数“ldap_server_name”，则显示所有 LDAP 服务器的超时时间配置。

aaa ldap searchfilter <ldap_server_name> <filter_string>

该命令用于为指定的 LDAP 服务器配置一个搜索过滤器，每个 LDAP 服务器只能配置一个搜索过滤器。搜索过滤器在 LDAP 认证和授权过程中具有重要作用，“aaa ldap bind dynamic”和“aaa ldap bind static”命令描述中详细说明了静态和动态绑定方式下搜索过滤器的功能。

ldap_server_name 该参数指定已存在的 LDAP 服务器的名称。

filter_string 该参数指定用于搜索 LDAP 记录项的过滤字符串，取值必须为长度不大于 80 个字节的字符串，置于双引号中。

过滤字符串由以下元素构成：

- 属性：Common Name (cn)、Distinguished Name (dn)、User Id (uid)、Organization Unit (ou)等等。
- 比较运算符：“>”、“<”或“=”。
- 逻辑运算符：“&”、“|”、“!”、“=”或“*”。

过滤字符串可以包含最多三个由“<USER>”表示的令牌，不区分大小写。

no aaa ldap searchfilter <ldap_server_name>

该命令用于删除指定 LDAP 服务器的搜索过滤器配置。

show aaa ldap searchfilter [ldap_server_name]

该命令用于显示指定 LDAP 服务器的搜索过滤器配置。如不指定参数“ldap_server_name”，则显示所有 LDAP 服务器的搜索过滤器配置。

aaa ldap attribute group <ldap_server_name> <attribute>

该命令用于为指定的 LDAP 服务器设置一个属性，该属性用于从 LDAP 记录项中获取用户所属的外部 LDAP 群组。

ldap_server_name 该参数指定已存在的 LDAP 服务器的名称。

attribute 该参数指定用于获取用户所属的外部 LDAP 群组的属性名称，取值必须为长度不大于 80 个字节的字符串。

no aaa ldap attribute group<ldap_server_name>

该命令用于删除指定 LDAP 服务器的“aaa ldap attribute group”配置。

show aaa ldap attribute group [ldap_server_name]

该命令用于显示指定 LDAP 服务器的“**aaa ldap attribute group**”配置。如不指定参数“**ldap_server_name**”，则显示所有 LDAP 服务器的“**aaa ldap attribute group**”配置。

aaa ldap defaultgroup <ldap_server_name> <group>

该命令用于为指定的 LDAP 服务器设置一个默认的 LDAP 群组。对于已经通过认证的用户，如果无法从 LDAP 记录项中获取该用户所属的 RADIUS 群组，则认为该用户属于默认群组。

ldap_server_name 该参数指定已存在的 LDAP 服务器的名称。

group 该参数指定默认 LDAP 群组名称。取值必须为长度不大于 80 个字节的字符串。

no aaa ldap defaultgroup <ldap_server_name>

该命令用于删除指定 LDAP 服务器的默认群组配置。

show aaa ldap defaultgroup [ldap_server_name]

该命令用于显示指定 LDAP 服务器的默认群组配置。如不指定参数“**ldap_server_name**”，则显示所有 LDAP 服务器的默认群组配置。

aaa ldap bind dynamic <ldap_server_name>

该命令用于为指定的 LDAP 服务器启用动态 LDAP 绑定模式，在该模式下，系统会优先从 LDAP 服务器获取用户的 DN。启用动态 LDAP 绑定模式后，系统会向 LDAP 服务器发送一个包含终端用户的用户名和密码的绑定请求，随后发送一个搜索请求用于获取终端用户的 LDAP 记录项，搜索请求携带通过“**aaa ldap searchfilter**”命令配置的搜索过滤字符串。从 LDAP 记录项获取到用户的 DN 后，系统会将该 DN 和终端用户的密码通过另一个绑定请求一起发送给 LDAP 服务器。终端用户通过认证后，LDAP 记录项会被再次用来进行授权。

ldap_server_name 该参数指定已存在的 LDAP 服务器的名称。

no aaa ldap bind static <ldap_server_name>

该命令用于为指定 LDAP 服务器禁用 LDAP 动态绑定模式。

aaa ldap bind static <ldap_server_name> <dn_prefix> <dn_suffix>

该命令用于为指定的 LDAP 服务器启用静态 LDAP 绑定模式，在该模式下，系统会使用“<dn_prefix><USER><dn_suffix>”字符串来构建用户的 DN，其中“<USER>”表示用于登录站点所用的用户名，“<dn_prefix>”和“<dn_suffix>”对于访问同一个站点的所有用户必须是相同的。启用静态 LDAP 绑定模式后，系统会将“<dn_prefix><USER><dn_suffix>”字符串和终端用户的密码通过一个绑定请求一起发送给 LDAP 服务器。终端用户通过认证后，系统会向 LDAP 服务器发送一个搜索请求来获取终端用户的 LDAP 记录项，搜索请求携带通过“**aaa**

ldap searchfilter”命令配置的搜索过滤字符串。获取到的 LDAP 记录项会用于后续的用户授权。

注意：动态和静态 LDAP 绑定模式不能同时启用。

ldap_server_name	该参数指定已存在的 LDAP 服务器的名称。
dn_prefix	该参数指定从 LDAP 服务器获取到的 DN 前缀，取值必须为长度不大于 80 个字节的字符串。
dn_suffix	该参数指定从 LDAP 服务器获取到的 DN 后缀，取值必须为长度不大于 80 个字节的字符串。

no aaa ldap bind static <ldap_server_name>

该命令用于为指定 LDAP 服务器禁用 LDAP 静态绑定模式。

show aaa ldap bind [ldap_server_name]

该命令用于显示指定 LDAP 服务器的 LDAP 绑定模式设置。如不指定参数“ldap_server_name”，则显示所有 LDAP 服务器的 LDAP 绑定模式设置。

11.1.5 OAuth

aaa oauth vendor <server_name> <vendor_name>

该命令用于配置指定 OAuth 服务器的供应商名称，系统支持的 OAuth 供应商包括：

- Google
- WeChat
- 如果通过该命令定义了 Google OAuth 服务器，系统会自动添加以下配置：
 - **aaa oauth tokenurl** “goo_server”
“https://accounts.google.com/o/oauth2/token”
 - **aaa oauth authenticatorurl** “goo_server”
“https://accounts.google.com/o/oauth2/auth”
 - **aaa oauth jwksurl** “goo_server”
“https://www.googleapis.com/oauth2/v3/certs”

如果通过该命令定义了 WeChat OAuth 服务器，系统会自动添加以下配置：

- **aaa oauth tokenurl** “wech_server”
“https://api.weixin.qq.com/sns/oauth2/access_token”
- **aaa oauth authenticatorurl** “wech_server”
“https://open.weixin.qq.com/connect/qrconnect”

- **aaa oauth resourceurl “wech_server”**
“https://api.weixin.qq.com/sns/userinfo”

server_name	该参数指定已存在的 OAuth 服务器名称。
vendor_name	该参数指定第三方 OAuth 服务器的供应商名称，取值必须为： • google: 表示 Google OAuth 服务器。 • wechat: 表示 WeChat 服务器。

aaa oauth authenticatorurl <server_name> <authenticator_url>

该命令用于修改指定 OAuth 服务器登录页面的 URL 地址。

server_name	该参数指定已存在的 OAuth 服务器名称。
authenticator_url	该参数指定第三方 OAuth 服务器的登录页面的 URL 地址，取值必须为长度不大于 900 个字节的字符串。

aaa oauth tokenurl <server_name> <token_url>

该命令用于修改从指定 OAuth 服务器获取访问令牌的 URL 地址。

server_name	该参数指定已存在的 OAuth 服务器名称。
token_url	该参数指定用于从 OAuth 服务器获取访问令牌的 URL 地址，取值必须为长度不大于 900 个字节的字符串。

aaa oauth jwksurl <server_name> <jwks_url>

该命令用于修改获取指定 OAuth 服务器的 JWK (JSON Web Key) 密钥集的 URL 地址。该命令仅用于 Google OAuth 服务器。

server_name	该参数指定已存在的 OAuth 服务器名称。
jwks_url	该参数指定获取 OAuth 服务器的 JWK 密钥集的 URL 地址，取值必须为长度不大于 900 个字节的字符串。

aaa oauth registerid <server_name> <register_id>

该命令用于设置或修改 OAuth 客户端与指定 OAuth 服务器通信时使用的注册 ID。

server_name	该参数指定已存在的 OAuth 服务器名称。
register_id	该参数指定 OAuth 客户端的注册 ID，取值必须为长度不大于 128 个字节的字符串。

aaa oauth registersecret <server_name> <register_secret>

该命令用于设置或修改 OAuth 客户端与指定的 OAuth 服务器通信时使用的注册密码。

server_name	该参数指定已存在的 OAuth 服务器名称。
register_secret	该参数指定 OAuth 客户端的注册密码，取值必须为长度不大于 128 个字节的字符串。

aaa oauth redirecturl <server_name> <redirect_url>

该命令用于为指定的 OAuth 服务器设置或修改重定向响应的目的 URL 地址。

server_name	该参数指定已存在的 OAuth 服务器名称。
redirect_url	该参数指定重定向响应的目的 URL 地址，取值必须为长度不大于 900 个字节的字符串。 如果是 Google OAuth 服务器，参数“redirect_url”的取值必须设置为 Google 的第三方开发平台上注册的重定向 URL 地址，格式为 “https://<virtual_service_domain_name>/prx/000/http/localhost/oauth_code”。 如果是 WeChat OAuth 服务器，参数“redirect_url”的取值格式必须为 “https://<virtual_service_domain_name>/prx/000/http/localhost/oauth_wechat_code”，且虚拟服务的域名已经在 WeChat 的开发平台完成注册。

aaa oauth resourceurl <server_name> <resource_url>

该命令用于设置或修改 OAuth 客户端从指定的 OAuth 服务器获取用户信息的 URL 地址。目前，该命令仅用于 WeChat OAuth 服务器。Google OAuth 服务器 Google OAuth 服务器会通过访问令牌响应返回用户，所以不需要配置该命令。

server_name	该参数指定已存在的 OAuth 服务器名称。
resource_url	该参数指定从 OAuth 服务器获取用户信息的 URL 地址，取值必须为长度不大于 900 个字节的字符串。

aaa method register <method_name>

该命令用于设置注册 OAuth 应用程序时使用的 AAA 方案。

method_name	该参数指定已存在的 AAA 方案的名称，取值必须为 RADIUS 或 LDAP 类型的认证方案的名称（该 AAA 方案仅用于认证）。SAML SP 和 OAuth 类型的 AAA 方案

不能用于 OAuth 应用程序注册。

no aaa method register <method_name>

该命令用于删除指定 AAA 方案的“aaa method register”命令配置。

show aaa method register [method_name]

该命令用于显示指定 AAA 方案的“aaa method register”命令配置。如不指定参数“method_name”，则显示所有 AAA 方案的“aaa method register”命令配置。

aaa oauth registration on <server_name> [save_password]

该命令用于为指定的 OAuth 服务器启用或禁用 OAuth 认证后注册功能。

启用该功能时，OAuth 用户在通过 OAuth 认证后必须向系统注册。注册过程中，OAuth 用户需要向 AAA 方案中（通过“aaa method register”命令配置）的认证服务器进行认证。通过认证后，系统会将认证后获取到的 OAuth 用户 ID 和用于注册的用户名绑定。该注册用户名（而不是获取到的 OAuth 用户名）会用于后续的授权。

该功能的默认设置为启用。

server_name 该参数指定已存在的 OAuth 服务器名称。

save_password 可选。该参数指定是否保存用户密码，取值必须为：

- **save:** 保存用户密码。
- **nosave:** 不保存用户密码。

注意当使用 Web SSO 功能时，该参数取值必须设置为“save”。

aaa oauth registration off <server_name>

该命令用于为指定的 OAuth 服务器禁用 OAuth 认证后注册功能。

aaa oauth prefixasusername <server_name>

该命令用于配置允许指定的 OAuth 服务器使用 email 账号前缀作为 OAuth 用户名。该选项的默认设置为禁用。

no aaa oauth prefixasusername <server_name>

该命令用于配置禁止指定的 OAuth 服务器使用 email 账号前缀作为 OAuth 用户名。

aaa oauth authorizationfilter <server_name> <authorization_filter>

该命令用于为指定的 OAuth 服务器配置或修改 OAuth 认证后授权过滤器。只有当 OAuth 用户名（Google OAuth 服务器：email 账号；WeChat OAuth 服务器：昵称）匹配 OAuth 认证后授权过滤器时，系统才会在 OAuth 认证后对 OAuth 用户授权。如不配置 OAuth 认证后过滤器，系统会对所有通过 OAuth 认证的用户进行授权。

server_name	该参数指定已存在的 OAuth 服务器名称。
authorization_filter	该参数指定 OAuth 用户名过滤字符串，取值必须为长度不大于 64 个字节的字符串。

no aaa oauth authorizationfilter <server_name>

该命令用于删除指定 OAuth 服务器的 OAuth 认证后授权过滤器。

aaa oauth bind import <url>

该命令用于从指定的 URL 地址导入 OAuth 用户绑定信息。

url	该参数指定 OAuth 用户绑定信息的 URL 地址，取值必须为 HTTP 或 FTP 类型的 URL 地址。

注意：FTP 类型 URL(ftp://user:password@host:port/path) 中的“path”需使用相对路径。

aaa oauth bind export <url>

该命令用于将 OAuth 用户绑定信息导出到指定的 URL 地址。

url	该参数指定用于存放 OAuth 用户绑定信息的 URL 地址，取值必须为 FTP 类型的 URL 地址，包含需要导出的文件的名称，例如当文件名是“oauth_bind”时，URL 地址应设置为“ftp://test:abc@10.4.21.112/oauth_bind”。

no aaa oauth bind <virtual_service> <oauth_uid>

该命令用于从指定的虚拟服务上删除一个 OAuth 用户的绑定信息。

virtual_service	该参数指定已存在的虚拟服务名称。
oauth_uid	该参数指定 OAuth 用户的 ID。

show aaa oauth bind [virtual_service] [oauth_uid]

该命令用于显示指定虚拟服务上的一个 OAuth 用户的绑定信息。如不指定参数“oauth_id”，则删除该虚拟服务上的所有 OAuth 用户绑定信息。

clear aaa oauth bind <virtual_service>

该命令用于清除指定虚拟服务上的所有 OAuth 用户绑定信息。

show aaa oauth settings

该命令用于显示所有 OAuth 相关配置。

11.1.6 会话管理

aaa session virtual limit <virtual_service> <max_session_number>

该命令用于为指定虚拟服务设置允许的最大并发会话数。注意：修改该配置时，新的数值必须大于等于当前已存在的会话数。

virtual_service 该参数指定已存在的虚拟服务名称。

max_session_number 该参数指定最大并发会话数。取值为 0 时表示不限制虚拟服务上的会话数量。

系统支持的最大会话数取决于系统内存的大小，如下表所示（实际数值可能因为内存的使用情况而有变动）：

表11 - 2 最大会话数

系统内存	支持的最大会话数
1 GB	500
2 GB	1000
4 GB	2000
8 GB	4000
16 GB	8000
32 GB	16,000
64 GB	32,000
128 GB	64,000

no aaa session virtual limit <virtual_service>

该命令用于删除指定虚拟服务的最大并发会话数配置。

show aaa session virtual limit [virtual_service]

该命令用于显示指定虚拟服务的最大并发会话数配置。如不指定参数“virtual_service”，则显示所有虚拟服务的最大并发会话数配置。

clear aaa session virtual limit

该命令用于清除所有虚拟服务的最大并发会话数配置。

aaa session virtual maxperuser <virtual_service> <maximum_session_number>

该命令用于设置指定虚拟服务上单个用户允许的最大会话数。注意：单个用户允许的最大会话数不能大于虚拟服务上允许的总最大会话数。

virtual_service	该参数指定已存在的虚拟服务名称。
maximum_session	该参数指定单个用户允许的最大会话数。取值为 0 时，系统不限制单个用户的最大会话数。

系统支持的最大会话数取决于系统内存的大小，如下表所示（实际数值可能因为内存的使用情况而有变动）：

表11 - 3 支持的最大会话数

系统内存	支持的最大会话数
1 GB	500
2 GB	1000
4 GB	2000
8 GB	4000
16 GB	8000
32 GB	16,000
64 GB	32,000
128 GB	64,000

no aaa session virtual maxperuser <virtual_service>

该命令用于删除指定虚拟服务的单个用户最大会话数配置。

show aaa session virtual maxperuser [virtual_service]

该命令用于显示指定虚拟服务的单个用户最大会话数配置。如不指定参数“virtual_service”，则显示所有虚拟服务的单个用户最大会话数配置。

clear aaa session virtual maxperuser

该命令用于清除所有虚拟服务的单个用户最大会话数配置。

aaa session virtual reuse {on|off} <virtual service>

该命令用于为指定虚拟服务启用或禁用会话重用功能。只有关联了 SAML SP 服务器的虚拟服务才能启用会话重用功能。该功能的默认设置为禁用。

virtual_service 该参数指定已存在的虚拟服务名称。

show aaa session virtual reuse [virtual_service]

该功能用于显示指定虚拟服务的会话重用功能的开启状态。如不指定参数“virtual_service”，则显示所有虚拟服务的会话重用功能的开启状态。

aaa session virtual timeout idle <virtual_service> <idle_time>

该命令用于设置指定虚拟服务上闲置会话的超时时间。如不配置该命令，默认的闲置会话的超时时间为 3600 秒。

virtual_service	该参数指定已存在的虚拟服务名称。
idle_timeout	该参数指定闲置会话的超时时间,取值必须为 1 至 86400 之间的整数,单位为秒。

no aaa session virtual timeout idle <virtual_service>

该命令用于将指定虚拟服务的闲置会话超时时间设置恢复为默认值。

show aaa session virtual timeout idle [virtual_service]

该命令用于显示指定虚拟服务的闲置会话超时时间设置。如不指定参数“virtual_service”,则显示所有虚拟服务的闲置会话超时时间设置。

clear aaa session virtual timeout idle

该命令用于将所有虚拟服务的闲置会话超时时间设置恢复为默认值。

aaa session virtual timeout lifetime <virtual_service> <lifetime>

该命令用于设置指定虚拟服务上会话的有效期。如不配置该命令,默认的会话有效期为 86400 秒。注意:会话有效期必须大于闲置会话的超时时间。

virtual_service	该参数指定已存在的虚拟服务名称。
lifetime	该参数指定会话的有效期,取值必须为 1 至 94,608,000 之间的整数,单位为秒。

no aaa session virtual timeout lifetime <virtual_service>

该命令用于将指定虚拟服务的会话有效期设置恢复为默认值。

show aaa session virtual timeout lifetime [virtual_service]

该命令用于显示指定虚拟服务的会话有效期设置。如不设置参数“virtual_service”,则显示所有虚拟服务的会话有效期设置。

clear aaa session virtual timeout lifetime

该命令用于将所有虚拟服务的会话有效期设置恢复为默认设置。

show aaa session virtual settings [virtual_service]

该命令用于显示指定虚拟服务的所有会话管理相关配置。如不指定参数“virtual_service”,则显示所有虚拟服务的会话管理相关配置。

clear aaa session virtual settings [virtual_service]

该命令用于清除指定虚拟服务的所有会话管理相关配置。如不指定参数“virtual_service”,则清除所有虚拟服务的会话管理相关配置。

show aaa session active [filter_string]

该命令用于显示匹配指定过滤字符串的活动会话。

filter_string

可选。该参数指定过滤字符串，取值必须为“all”或者为一个或多个关键词组成的字符串，格式为

“Keyword1=xxx, Keyword2=yyy, ...”，不受先后顺序限制，置于双引号内。

取值为“all”或不指定该参数时将显示当前所有的活动会话。取值为字符串时支持的关键词包括：

- **id**: 表示会话 ID。
- **user**: 表示用户名。
- **vs**: 表示虚拟服务名称。
- **format**: 取值必须为“count”或“data”，分别表示会话数和会话的详细信息。

示例：

“id=123456, user = Jack, vs = v-web, format = data”

示例：

Demo(config)#show aaa session active all

User Name	Session ID	Age	Last Active
_5ad71ec964956f67cf8f82538926c6a01d126786f7	4D5A56F8	00:11:47	00:11:47
_5611a9b3f629663fd5428219b039047f65e054a7c0	4D5A56F7	00:17:03	00:17:03
_ab167aa63b844b83f3ef97abf57165ba1951b7dd4f	4D5A56F6	00:01:44	00:01:40
_e1aab484dd1220b3e0ccf8bcc06031f3eb5381d480	4D5A56F9	415402:13:01	
		415402:13:01	
_58041654444a23e8e92438c9f0c57fdffb3c19fa80	4D5A56FA	415402:13:01	
		415402:13:01	

aaa session kill [filter_string]

该命令用于终止匹配指定过滤字符串的活动会话。

filter_string

可选。该参数指定过滤字符串，取值必须为“all”或者为一个或多个关键词组成的字符串，格式为

“Keyword1=xxx, Keyword2=yyy, ...”，不受先后顺序限制，置于双引号内。

取值为“all”或不指定该参数时将终止当前所有的活动会话。取值为字符串时支持的关键词包括：

- **id**: 表示会话 ID。

- user: 表示用户名。
- vs: 表示虚拟服务名称。

示例:

“id=123456, user = Jack, vs = v-web”

11.2 Web SSO

aaa sso {on|off} <virtual_service>

该命令用于为指定虚拟服务启用或禁用 Web SSO 功能。Web SSO 功能依赖于 SAML、LDAP、RADIUS 或 OAuth 认证实现。在需要使用 Web SSO 的应用场景，必须先部署 SAML、LDAP、RADIUS 或 OAuth 认证。该功能默认设置为禁用。

virtual_service 该参数指定一个已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。



注意：当基于 SAML 部署和实现 Web SSO 时，管理员必须确保设备能从 IdP 服务器获取到用户的登录凭据。公司 NetGate 系列设备可以作为 IdP 服务器与设备协作实现 Web SSO 支持，如需更多信息，请联系公司技术支持。

aaa sso post <virtual_service> <hostname> <login_url> <username_field> <password_field> [post_host] [post_url] [other_post_field] [other_header_field]

该命令用于为指定虚拟服务配置一条 HTTP POST SSO 规则。通过该命令，管理员可以指定一个登录页面的 URL 地址，系统会代替终端用户将凭据提交到该地址，终端用户无需再次输入登录凭据即可访问多个后台应用。系统支持配置最多 64 条 HTTP POST SSO 规则。

virtual_service 该参数指定一个已存在的虚拟服务名称，取值必须为 HTTPS 类型的虚拟服务。

hostname 该参数指定后台服务的主机名，取值必须为长度不大于 128 个字节的字符串。

login_url 该参数指定登录页面的 URL 地址，取值必须为长度不大于 900 个字节的字符串。

username_field 该参数指定用于提交验证用户名的字段名称，取值必须为长度不大于 64 个字节的字符串。

password_field 该参数指定用于提交验证密码的字段名称，取值必须为长度不大于 32 个字节的字符串。

post_host 可选。该参数指定提交 POST 请求的目标主机名（和端口），取值必须为长度不大于 128 个字节的字符串，格

式为“hostname”或“hostname: port”。如不指定该参数，系统默认使用“hostname”参数的取值。

post_url

可选。该参数指定提交 POST 请求的目标 URL 地址。取值必须为长度不大于 900 个字节的字符串。如不指定该参数，系统默认使用“login_url”参数的取值。

other_post_field

可选。该参数指定除了验证用户名和密码以外后台服务需要设置的其他字段名称。取值必须为长度不大于 1024 个字节的字符串，格式必须为仅由字符构成的字符串或者包含多个“field=value”对的字符串，各项之间通过“&”符号分隔，置于双引号内。另外，该参数取值支持设置令牌，系统运行中，令牌会被动态替换成真实的值。

系统支持的令牌及其含义如下：

- <IP_ADDR_UINT>：表示无符号整数格式的客户端 IP 地址，例如 1677920266。
- <IP_ADDR_DOTDEC>表示点分十进制格式的客户端 IP 地址，例如 10.8.3.100。

示例：

“domain=abc&deptname=xyz&ipaddress=<IP_ADDR_DOTDEC>”

other_header_field

可选。该参数指定后台服务需要设置的其他用于用户验证的 HTTP 头部字段。取值必须为长度不大于 1024 个字节的字符串，置于双引号内。如果设置多个 HTTP 头部字段，各字段之间必须通过“\r\n”分隔。

示例：

“User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)\r\nCookie: PBack=0;\r\n”

no aaa sso post <virtual_service> <hostname> <login_url>

该命令用于删除指定虚拟服务的一条 HTTP POST SSO 规则。

show aaa sso [virtual_service]

该命令用于显示指定虚拟服务的所有 HTTP POST SSO 规则。如不指定参数“virtual_service”，则显示所有虚拟服务的 HTTP POST SSO 规则。

clear aaa sso [virtual_service]

该命令用于清除指定虚拟服务的 HTTP POST SSO 规则。如不指定参数“virtual_service”，则清除所有虚拟服务的 HTTP POST SSO 规则。

第12章 链路负载均衡（LLB）

对于可以同时通过多条链路访问 Internet 的用户而言，LLB（Link Load Balance，链路负载均衡）功能是非常有必要的。LLB 用于对出向和入向的流量进行负载均衡。本章介绍 LLB 功能的相关配置命令。

12.1 LLB 路由

LLB 功能主要基于策略路由（Eroute）为报文选择链路进行转发。设备支持多种路由，系统根据路由的优先级来为报文匹配路由，各类路由的优先级见下表。

表12 - 1 路由优先级

路由名称	优先级
优先 Eroute（Eroute-P）	2001-2999
接口路由（Interface Route，Iroute）	2000
直连路由（Direct Route，Droute）	2000
RTS 路由	1999
IP region 路由	1001-1999（默认 1999）
普通 Eroute（Normal Eroute，Eroute-N）	1001-1999
IPflow 路由	1000-1999（默认 1000）
静态路由（Static Route）	101-132 (IPv4) 101-228 (IPv6)
动态路由（Dynamic Route）	101-132 (IPv4) 101-228 (IPv6)
LLB 链路路由（LLB Link Route）	2
默认路由（Default Route）	1

接口路由

在管理员配置了接口 IP 地址后，系统会自动生成一条从任何 IP/端口对到该接口所在网段的路由。该路由称为接口路由（Interface Route，Iroute）。

直连路由

在管理员配置了接口 IP 地址后，系统自动通过 ARP 学习生成的路由称为直连路由（Direct Route，Droute），直连路由的超时时间为 1 小时。

RTS 路由

启用原路返回（Return to Source，RTS）路由功能后，当客户端的请求报文命中设备后，设备将通过反查路由找到客户端请求到达设备的原链路，并自动为该链路创建一条 RTS 路由，确保响应通过原链路返回。

在下面两种情况下设备会创建一条 RTS 路由：

- 设备在反查路由时匹配到大于等于两条相同优先级的路由，并且这些路由的优先级低于 RTS 路由的优先级；
- 设备在反查路由时匹配到一条路由，并且该路由的优先级低于 RTS 路由的优先级，但该路由的网关与到达设备的请求报文的上一跳不一致。

IP region 路由

将系统中的 IP region 表与网关绑定可以生成 IP region 路由。当报文的目的 IP 地址匹配该 IP region 表中的任何子网时，将命中生成的 IP region 路由。

Eroute

Eroute 允许设备基于报文五元组（源 IP 地址、目的 IP 地址、源端口、目的端口和协议类型）为出向数据流选择一条路由。优先级在 2001-2999 之间的 Eroute 称为优先 Eroute（Preferential Eroute, Eroute-P），优先级为在 1001-1999 之间的 Eroute 称为普通 Eroute（Normal Eroute, Eroute-N）。

IPflow 路由

启用 IPflow 路由功能后，当选择一条路由转发报文时，系统会自动创建基于源 IP 地址和目的 IP 地址的 IPflow 路由，后续来自相同源 IP 地址的报文将一直通过该路由转发。

静态路由

静态路由由管理员手动配置。静态路由的优先级等于子网掩码或前缀长度加上 100。例如，如果静态路由的子网掩码为 24，则该静态路由的优先级是 124。

动态路由

动态路由是系统根据动态路由协议（例如 OSPF 和 BGP）动态生成的路由。

LLB 链路路由

LLB 链路路由为使用命令 “**llb link route**” 生成的路由。

默认路由

默认路由由管理员手动配置。默认路由是设备的缺省路由，只有当报文没有匹配任何其他路由时才会通过默认路由转发。



注意：当 RTS 路由、IPflow 路由、IP region 路由和普通 Eroute 具有相同的优先级时，路由匹配顺序依次为 RTS 路由、IPflow 路由、IP region 路由和普通 Eroute。

llb link route <link_name> <route_ip> [weight] [hc_srcip]
[bandwidth_threshold]

该命令用于定义一条 LLB 链路，或者更新已有 LLB 链路的带宽阈值。执行该命令后，系统将为新添加的 LLB 链路自动生成一条优先级为 2 的 Eroute。系统允许配置最多 128 条 LLB 链路，包括 IPv4 及 IPv6 LLB 链路。

对于已经定义的 LLB 链路，可以通过该命令修改链路的权重值和带宽阈值。

link_name	该参数指定 LLB 链路的名称。取值必须为长度不大于 31 个字节的字符串，支持数字、字母和特殊符号，区分大小写。包含特殊符号时，名称必须置于双引号内。
route_ip	该参数指定 LLB 链路的网关 IP 地址。取值必须为 IPv4 或 IPv6 地址。
weight	可选，用于指定使用 wrt 或 hi 算法时 LLB 链路的权重值。取值必须为 1 到 1,048,576 之间的整数。链路的权重值越大，该链路被选择的可能性越大。 默认值为 1。
hc_srcip	可选，该参数指定健康检查的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。对于 IPv4 链路，默认值为 0.0.0.0。对于 IPv6 链路，默认值为：：。建议参数“hc_srcip”使用其默认值。此时，进行健康检查时，设备会自动选择和网关在同一网段的接口 IP 地址作为源 IP 地址。
bandwidth_threshold	可选，该参数指定链路允许的最大带宽，即带宽阈值，单位为 Mbps 或 Gbps。该阈值不是严格的限定。即使当前链路的流量负载大于设定的带宽阈值，数据报也不会被丢弃，而会通过其它未达到带宽阈值的链路转发；如果没有可选的链路，数据报将继续通过该链路转发。参数取值必须为 0Mbps~10Gbps。 默认值为 0Mbps，即对带宽没有限制。

示例：

```
Demo(config)#llb link route "link1" 10.191.2.100 1 10.191.2.105 10Mbps
```

要更新该 LLB 链路的带宽阈值为 20Mbps，可以执行以下命令：

```
Demo(config)#llb link route "link1" 10.191.2.100 1 10.191.2.105 20Mbps
```



注意：系统执行配置同步时，如果在本地节点上参数“hc_srcip”的取值非默认值“0.0.0.0”，而对端节点上没有该“hc_srcip”，则会造成同步失败。为了避免同步失败，建议参数“hc_srcip”使用其默认值。

no llb link route <link_name>

该命令用于删除一条 LLB 链路的配置。

show llb link route [*link_name*]

该命令用于显示指定 LLB 链路的配置。如果没有指定参数 “link_name”，将显示系统中所有的 LLB 链路的配置。

clear llb link route

该命令用于清除系统中所有的 LLB 链路的配置。

llb link {enable|disable} <link_name>

该命令用于启用或禁用一条 LLB 链路。当一条 LLB 链路被禁用后，系统将会使用其他可用的 LLB 链路转发数据包，如果没有其他可用的 LLB 链路，该条 LLB 链路上的数据包将被丢弃。默认情况下，LLB 链路是启用的。



注意：网络流量不能流经一条被禁用的 LLB 链路。但是以下情况是例外：

- 如果入向的流量没有经过 LLB DNS 解析，那么它可能通过一条禁用的链路流入。
- 如果已经启用 RTS 路由并且流量已经从某条禁用的链路流入的，那么对应的出向流量也将通过该条禁用链路流出，因为 RTS 路由的优先级比 LLB 链路路由更高。

llb link bw_priority <priority>

该命令用于为 LLB 出向的链路配置带宽优先级。如果不配置该命令，LLB 出向链路的默认带宽优先级为 1800。

priority 该参数指定 LLB 出向的链路的带宽优先级。取值必须为 0 到 1999 间的整数。取值越大，优先级越高。



注意：如果出向流量匹配的 Eroute 的优先级高于 LLB 出向链路带宽的优先级，那么由 Eroute 确定的 LLB 链路不受带宽阈值的限制，否则将受到带宽阈值的限制。

show llb link bw_priority

该命令用于显示为 LLB 出向的链路的配置的带宽优先级。

ip eroute <name> <priority> {srcip|src_ip_group} {srcmask|prefix} <srcport> {dsthost|dst_ip_group} {dstmask|prefix} <dstport> <protocol> <gateway_ip> [weight]

该命令用于定义一条策略路由（Eroute）。Eroute 允许设备基于报文五元组（源 IP 地址/源 IP 地址组、目的 IP 地址/目的 IP 地址组、源端口、目的端口和协议类型）为出向数据流选择一条路由。优先级为 2001-2999 的 Eroute 称为优先 Eroute（Preferential Eroute, Eroute-P），优先级为 1001-1999 的 Eroute 称为普通 Eroute（Normal Eroute, Eroute-N）。

name	该参数指定 Eroute 的名称。取值必须为最大长度不大于 103 个字节的字符串。 注意：参数取值不能为空。
priority	该参数指定 Eroute 的优先级。取值必须为 1001 至 2999 之间的整数，不包括 2000。
srcip src_ip_group	该参数指定源 IP 地址或源 IP 地址组。IP 地址取值必须为 IPv4 或 IPv6 地址。
srcmask prefix	该参数指定源 IP 地址对应的子网掩码或前缀长度。 “srcmask”用于配置 IPv4 地址对应的子网掩码，其取值可以是点分地址格式或是一个 0 至 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其取值应是一个 0 到 128 之间的整数。 当参数“srcip src_ip_group”取值为源 IP 地址组时，该参数无效。
srcport	该参数指定一个源端口或端口范围。取值必须为 1 到 65,535 之间的整数。端口范围的格式应为“X-Y”，如“1000-2000”表示处于 1000 到 2000 之间的端口。该参数取值还可以设置为 0，表示通配，只有协议类型为 TCP 或 UDP 时生效。
dsthost dst_ip_group	该参数指定目的主机的域名、IP 地址，或者目的 IP 地址组。当取值为 IP 地址时，支持 IPv4 和 IPv6 地址。 当取值为域名时，支持快速正则表达式。如果使用正则表达式，则需要将其置于双引号内。更多信息，请参见第一章关于正则表达式的介绍。 注意：域名的正则表达式必须包含“.”字符，且不能以“.”或“-”开始或结束。正则表达式长度不能超过 254 个字符，且字符串中由“.”分隔的各部分长度不能超过 63 个字符。 取值为域名时，需要使用的资源类型取决于参数“gateway_ip”的设置： - 当需要使用 IPv4 资源时，“gateway_ip”的取值必须为 IPv4 地址。 - 当需要使用 IPv6 资源时，“gateway_ip”的取值必

须为 IPv6 地址。

dstmask prefix	该参数指定目的地址对应的子网掩码或前缀长度。参数的含义同“srcmask prefix”。 当参数“dsthost dst_ip_group”取值为目的 IP 地址组时，该参数无效。
dstport	该参数指定一个目的端口或端口范围。参数含义和取值同“srcport”。
protocol	该参数指定匹配的协议类型。取值必须为“TCP”、“UDP”或者“any”。如果参数取值为“any”，表示该 Eroute 将匹配所有协议的报文都将匹配该 Eroute。
gateway_ip	该参数指定网关的 IP 地址。取值必须为 IPv4 或 IPv6 地址。
weight	可选，用于指定使用 wrr 或 hi 算法时该 Eroute 的权重值。取值必须为 1 至 1,048,576 之间的整数，默认值为 1。



注意：

- 如果新增 Eroute 的源子网、目的子网、源端口号范围、目的端口号范围或协议类型中的任一值和已有 Eroute 相同，则无法新增 Eroute。
- 关于普通 Eroute 路由和其他路由优先级相同时的匹配顺序，请参见本章开头的描述。
- 同一个 IP 地址组可以关联到多条 Eroute。
- 参数“dsthost”取值为目的主机域名时，系统允许配置最多 512 条 Eroute。

设备上支持的 Eroute 的最大数量取决于系统内存的大小，如下表所示。

表12 - 2 Eroute 的最大数量

系统内存	Eroute 的最大数量
≤4 GB	5,000
8 GB	10,000
16 GB	20,000
24 GB	20,000
32 GB	40,000
64 GB	40,000
96 GB	80,000
128 GB	80,000

no ip eroute <name>

该命令用于删除一条 Eroute。

show ip eroute [ipv4|ipv6] [all|valid|invalid]

该命令用于显示系统中 Eroute 路由表中的路由，包括 Eroute、LLB 链路路由、IP region 路由、接口路由、默认路由、静态路由、动态路由、管理路由和直连路由。

ipv4|ipv6 可选，该参数指定输出结果中将要显示的 Eroute 的类型。取值必须为“IPv4”和“IPv6”，不区分大小写。如果不指定该参数，系统会显示所有 IPv4 和 IPv6 的 Eroute 的配置。

all|valid|invalid 可选。取值必须为：

- **all**: 显示为所有 IP region 路由生成的 Eroute 的配置。
- **valid**: 显示可用的 Eroute。对于因域名解析生成的 Eroute，显示 TTL。
- **invalid**: 显示不可用的 Eroute 及其不可用的原因。



注意：

- RTS 和 IPflow 路由不存放于 Eroute 路由表中，而是分别存放于单独的 RTS 路由表和 IPflow 路由表。
- 该命令输出信息中名称为“management”的 Eroute 路由优先级显示为 0，表示管理路由。管理路由只会生成一条，且业务流量不会命中管理路由，只有管理流量才会命中该路由。

clear ip eroute

该命令用于清除 Eroute 路由表，以及 Eroute、Droute、IPflow 和 LLB 链路路由的统计信息。

ipregion route <ipregion_name> <gateway> [priority] [weight] [start_port] [end_port]

该命令用于为指定的 IP region 表创建 IP region 路由。配置该命令后，系统将根据 IP region 表中的每个 IP 网段分别生成对应的 Eroute。系统支持的 IP region 路由的最大数目与支持的 Eroute 的最大数目有关，具体请参见命令“**ip eroute**”。

ipregion_name 该参数指定 IP region 表的名称。取值必须为命令 **ipregion table import <ipregion_name> <url>** 定义的 IP region 表的名称或预定义的 IP region 表的名称。预定义的 IP region 表包括“predefined_cernet”、“predefined_cnc”和“predefined_ct”。管理员可以通过命令“**show ipregion name**”查看系统中已经存在的 IP region 表的名称。

gateway	该参数指定网关的 IP 地址。取值必须为 IPv4 或 IPv6 地址。
priority	可选，该参数指定该路由的优先级。取值必须为 1001 到 1999 之间的整数，默认值为 1999。
weight	可选，该参数用于指定使用 wrr 或 hi 算法时该 IP region 路由的权重。取值必须为 1 至 1,048,576 之间的整数。默认值为 1。
start_port	可选，该参数指定起始端口号。取值必须为 1 到 65,535 之间的整数，默认值为 1。
end_port	可选，该参数指定结束端口号。取值必须为 1 到 65,535 之间的整数，默认值为 65535。



注意：关于 IP region 路由和其他路由优先级相同时的匹配顺序，请参见本章开头的描述。

no ipregion route <ipregion_name>

该命令用于删除指定 IP region 表的 IP region 路由。基于 IP region 路由生成的所有 Eroute 也将被删除。



注意：基于 IP region 路由生成的所有 Eroute 作为一个整体存在，管理员不能修改或删除其中的单个 Eroute。

show ipregion route

该命令用于显示所有的 IP region 路由。

clear ipregion route

该命令用于删除所有的 IP region 路由。

show ipregion match <ip_address>

该命令用于在已配置的 IP 域表中查找包含指定 IP 地址的地址段，并显示所有匹配地址段所在的 IP 域表，地址段和相关描述。

ip_address 该参数指定用于匹配的 IP 地址，支持 IPv4 和 IPv6 地址。

ip ipflow {on|off}

该命令用于启用或禁用 IPflow 路由功能。启用 IPflow 路由功能后，当选择一条路由转发报文时，系统会根据一个源/目的 IP 地址对及网关生成一条 IPflow 路由，从而后续的具有相同源和目的地址的流量都会匹配该路由，通过该网关转发。IPflow 路由功能默认是禁用的。

设备上支持的 IPflow 路由的最大数量取决于系统内存的大小，如下表所示。

表12 - 3 IPflow 路由的最大数量

系统内存	IPflow 路由的最大数量
1 GB	10,000
2 GB	20,000
4 GB	1,000,000
8 GB	2,400,000
16 GB	5,000,000
≥32 GB	10,000,000

ip ipflow priority <priority>

该命令用于设置 IPflow 路由的优先级。如果不配置该命令，IPflow 路由的默认优先级为 1000。

priority 该参数指定 IPflow 路由的优先级。取值必须为 1000 到 1999 之间的整数。



注意：

- 由于 Eroute 路由的优先级大于 IPflow 路由的默认优先级，为了使 IPflow 路由功能生效，推荐将 IPflow 路由的优先级设置为大于 1000。
- 当 IPflow 路由达到系统支持的最大数量时，新的 IPflow 路由将会覆盖最早的 IPflow 路由。
- 关于 IPflow 路由和其他路由优先级相同时的匹配顺序，请参见本章开头的描述。

ip ipflow expire <timeout>

该命令用于设置 IPflow 路由的超时时间。如果不配置该命令，IPflow 路由的默认超时时间为 60 秒。如果一条 IPflow 路由被命中，该 IPflow 路由将重新开始计时。如果一条 IPflow 路由在所设置的超时时间内未被命中，该 IPflow 路由将会从系统中删除。如果流量将要触发创建新的 IPflow 路由，但已经存在该 IPflow 路由，则该 IPflow 路由将被更新。

timeout 该参数指定 IPflow 路由的超时时间，单位为秒。取值必须为 1 到 86,400 之间的整数。

show ip ipflow

该命令用于显示系统中生成的所有的 IPflow 路由的所有配置。

clear ip ipflow

该命令用于将 IPflow 路由的所有配置重置为默认值。

ip rts on [all|gateway]

该命令用于启用 RTS 路由功能。启用该功能后，当客户端的请求报文命中设备后，设备将通过反查路由找到客户端请求到达设备的原链路，并自动为该链路创建一条 RTS 路由，确保响应通过原链路返回。

在下面两种情况下设备会创建一条 RTS 路由：

- 设备在反查路由时匹配到大于等于两条相同优先级的路由，并且这些路由的优先级低于 RTS 路由的优先级；
- 设备在反查路由时匹配到一条路由，并且该路由的优先级低于 RTS 路由的优先级，但该路由的网关与到达设备的请求报文的上一跳不一致。

all|gateway 可选，该参数指定 RTS 路由的模式。取值必须为 “all” 或 “gateway”。默认值为 “all”。

- **all**：表示系统使用 “all” 模式。系统记录所有发送者的信息，所有的响应数据报都将沿着请求数据报经过的链路返回。
- **gateway**：表示系统使用 “gateway” 模式。系统只记录来自网关的信息，来自网关的请求的响应数据报会沿着请求数据报经过的链路返回。

注意：参数取值为 “gateway” 时，系统记录的网关应使用命令 “**ip route default**”、“**ip eroute**”、“**ip route static**” 或 “**llb link route**” 定义的网关地址。



注意：

- 为了保证 RTS 路由功能能够正常工作，通过 “**ip eroute**” 命令配置的策略路由必须为普通 Eroute（优先级范围为 1001-1999）。
- 为了保证 RTS 路由功能能够正常工作，请在启用 RTS 路由功能之前确保已经为设备配置了基本的路由信息。
- 当 RTS 路由达到系统支持的最大数量时，新的 RTS 路由将会覆盖最早的 RTS 路由。
- 关于 RTS 路由和其他路由优先级相同时的匹配顺序，请参见本章开头的描述。

设备上支持的 RTS 路由的最大数量取决于系统内存的大小，如下表所示。

表12 - 4 RTS 路由的最大数量

系统内存	RTS 路由的最大数量
1 GB	10,000
2 GB	20,000
4 GB	40,000
8 GB	60,000
16 GB	150,000

32 GB	250,000
>32 GB	400,000

ip rts off

该命令用于禁用 RTS 路由功能。默认情况下，RTS 路由功能是禁用的。

ip rts expire [seconds]

该命令用于设置 RTS 路由的超时时间。如果一条 RTS 路由被命中，该 RTS 路由将重新开始计时；如果一条 RTS 路由在所设置的超时时间内未被命中，该 RTS 路由将会从系统中删除。如果流量将要触发创建新的 RTS 路由，但已经存在该 RTS 路由，则该 RTS 路由将被更新。

seconds 可选，该参数指定 RTS 路由的超时时间，单位为秒。取值必须为 1 到 2,147,483 之间的整数，默认值为 60。

ip rts gateway [ip_address]

该命令用于配置一个 RTS 路由白名单。执行该命令后，只有白名单中存在的 IP 地址可以生成 RTS 路由表项。执行该命令后，对于未在白名单内的 IP 地址生成的 RTS 路由表项，系统将在其超时后删除，其后将不再为该 IP 地址生成 RTS 路由表项。系统支持配置最多 128 个 RTS 路由白名单。

ip_address 该参数指定需要加入 RTS 路由白名单的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

no ip rts gateway [ip_address]

该命令用于删除指定的 RTS 路由白名单。

show ip rts

该命令用于显示 RTS 路由功能的相关配置。

clear ip rts [gateway]

该命令用于将所有 RTS 路由功能的配置重置为默认值，RTS 路由白名单也将会被清除。

gateway 可选。该参数指定是否重置 RTS 路由功能所有配置。取值必须为：

- 空：表示所有 RTS 配置将被重置为默认值。
- gateway：表示清除 RTS 路由白名单所有配置。

默认值为空。

clear droute

该命令用于清除所有直连路由。

12.2 出向链路负载均衡

llb method outbound {rr|wrr|sr}

该命令用于为出向链路负载均衡定义以下算法：

- rr: Round Robin, 轮询算法
- wrr: Weighted Round Robin, 加权轮询算法
- sr: Shortest Response, 最短响应时间算法

默认算法为 rr。



注意：

- sr 算法不能用来对 IP 分片、非 TCP/UDP 报文和重组的 UDP 报文进行链路负载均衡。
- 快速转发功能和 “sr” 算法不能一起使用。

llb method outbound hi [hash_type]

该命令用于为出向链路负载均衡定义 hi (Hash IP, 哈希 IP) 算法。配置该算法后，系统会通过计算 IP 地址的哈希值来实现出向链路负载均衡。

hash_type 可选，该参数指定 hi 算法选择哈希计算的 IP 地址类型。
取值必须为：

- src: 表示源 IP 地址。
- dst: 表示目的 IP 地址。

默认值为 “src”。



注意：使用 hi 算法时，首先需要使用通过 “llb link route” 或者 “ip eroute” 命令指定每条路由的权重。

llb method outbound hip [hash_type]

该命令用于为出向链路负载均衡定义 hip (Hash IP+Port, 哈希 IP 和端口) 算法。配置该算法后，设备会通过计算 IP 地址和端口的哈希值来实现出向链路负载均衡。

hash_type 可选，该参数指定 hip 算法选择哈希计算的 IP 地址和端口类型。取值必须为：

- src: 表示源 IP 地址和端口。

- **dst**: 表示目的 IP 地址和端口。

默认值为 “src”。

llb method outbound lb

该命令用于为出向链路负载均衡定义 lb (Least Bandwith, 最小带宽使用率) 算法。配置该算法后, 设备会选择带宽使用率最小的链路来转发出向流量。

要使用此算法, 管理员需要通过 “**llb link route**” 命令指定链路允许的最大带宽。如果链路未指定允许的最大带宽, 则该算法不会选择此链路。如果所有链路都没有指定允许的最大带宽, 则使用 **wrr** 算法。

llb method outbound lc

该命令用于为出向链路负载均衡定义 lc (Least Connections, 最小连接数) 算法。配置该算法后, 设备会选择连接数最少的出向链路来转发出向流量。

lc 算法建议在所有 LLB 链路都配置 NAT 且 LLB 链路的出向流量都能被 NAT 的情况下使用。如果所有 LLB 链路都没有配置 NAT, lc 算法实际为 **wrr** 算法。其他情况下不建议使用该算法。

llb method outbound dd [netmask] [prefix] [detecting_mode]

该命令用于为出向链路负载均衡定义 dd (Dynamic Detecting, 动态探测) 算法。配置 dd 算法后, 系统将通过不同 LLB 链路向流量目的地址发送 DD 探测报文, 并根据探测结果选择响应时间最短的链路。系统支持对 TCP、UDP 和 ICMP 的流量进行探测。

netmask	可选, 该参数指定 IPv4 目的地址的子网掩码。取值必须为 1 到 32 之间的整数, 默认值为 24。
prefix	可选, 该参数指定 IPv6 目的地址的前缀长度。取值必须为 1 到 128 之间的整数, 默认值为 64。
detecting_mode	可选, 该参数指定 dd 算法的探测模式。取值必须为: • tcp: 表示系统只对 TCP 流量进行动态探测。 • all: 表示系统对 TCP、UDP 和 ICMP 流量进行动态探测。 默认值为 “tcp”。



注意: 在修改 dd 算法的探测模式前, 请先使用命令 “**clear llb dd table**” 清除动态探测表中的信息。

show llb method

该命令用于显示正在使用的出向和入向的链路负载均衡算法。

llb dd static <network_ip> {netmask|prefix}

该命令用来为 dd 算法配置静态探测对象来找到响应时间最短的链路。如果参数“network”与“netmask|prefix”确定了单个 IP 地址，设备会在收到目的地址位于该 IP 地址所属网段的数据包时，对该 IP 地址进行 DD 探测；如果这两个参数确定了一个网段，设备会在收到目的地址属于该网段的数据包时，对该网段进行 DD 探测。系统允许配置最多 1024 个静态探测对象。

network_ip	该参数指定静态探测对象的 IP 地址或网段。取值必须为 IPv4 或 IPv6 地址。
netmask prefix	该参数指定 IP 地址对应的子网掩码或前缀长度。 “netmask”用于配置 IPv4 地址对应的子网掩码，其取值可以是点分地址格式或是一个 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其取值应是一个 0 到 128 之间的整数。

no llb dd static <network_ip> {netmask|prefix}

该命令用于删除指定的静态探测对象。

show llb dd static

该命令用于显示所有的静态探测对象。

clear llb dd static

该命令用于清除所有的静态探测对象。

llb link health remote {enable| disable}

该命令用于启用或禁用基于 dd 算法的健康检查功能。使用该功能前，管理员必须先启用 dd 算法。如果禁用了基于 dd 算法的健康检查功能，当 dd 算法没有探测到可用的链路时，采用 wrr 或 rr 算法转发数据包；如果启用了基于 dd 算法的健康检查功能，则当 dd 算法探测到所有 LLB 链路都不可达（响应超时），系统将丢弃该数据包。默认情况下，系统禁用该功能。

show llb dd table [destination_ip] [mask|prefix]

该命令用于显示动态探测表的详细信息。管理员可以查看指定目的 IP 网段的动态探测信息。如果没有指定目的 IP 网段，则将显示所有动态探测信息。

destination_ip	可选，该参数指定动态探测表中的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。当该参数指定为“0.0.0.0”，将显示所有 IPv4 地址的动态探测信息；当参数指定为“::”，将显示所有 IPv6 地址的动态探测信息。

mask|prefix 可选，该参数指定目的 IP 地址的子网掩码（IPv4 地址）或前缀长度（IPv6 地址）。对于 IPv4 地址，子网掩码的默认值为 255.255.255.255。对于 IPv6 地址，前缀长度的默认值为 128。

示例：

```
Demo(config)#show llb dd table

Table of LLB DD static route
Destination:      10.3.0.10/24, ICMP, Expire:47h59m59s, type:static, Invalid result:0
gateway:          10.8.1.1, response time: 3ms, hits: 0, status: UP.
gateway:          192.168.1.30, response time: Timeout, hits: 0, status:DOWN.

Table of LLB DD route
Destination:      110.3.1.10/24, ICMP, Expire:47h59m22s, type:dynamic, Invalid result:1
gateway:          10.8.1.1, response time: Timeout, hits: 0, status: UP.
gateway:          192.168.1.30, response time: Timeout, hits: 0, status:DOWN.
```

在上述示例中，“response time”表示设备到达目的 IP 地址的时间，“status”表示设备网关的状态。上述示例中“status”状态为“UP”但是“response time”状态为“Timeout”表示设备的流量能够正常达到网关，但是无法到达目的 IP 地址。

clear llb dd table

该命令用于清除动态探测表中的信息。

➤ Rsite

llb rsite health {on|off}

该命令用于启用或禁用 LLB 远程站点可访问性检查。

llb rsite net <rsite_name> <network_ip> {netmask|prefix} <checker_name> [check_ip]

该命令用于定义一个 LLB 远程站点，并将该 LLB 远程站点与一个可访问性检查规则关联。系统支持配置最多 1024 个 LLB 远程站点。每个 LLB 远程站点可以关联 1024 个 IP 地址且每个 IP 地址可以关联 1 个可访问性健康检查规则。

rsite_name 该参数指定 LLB 远程站点的名称。取值必须为最大长度不大于 31 个字节的字符串。如果以数字开头，参数值必须置于双引号内。

network_ip 该参数指定 LLB 远程站点所属的网段或其 IP 地址。取

	值必须为 IPv4 或 IPv6 地址。
netmask prefix	该参数指定 LLB 远程站点所属的网段或其 IP 地址对应的子网掩码或前缀长度。 “netmask”用于配置 IPv4 地址对应的子网掩码，其取值可以是点分地址格式或是一个 1 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其取值应是一个 1 到 128 之间的整数。
checker_name	该参数指定可访问性检查规则的名称。取值必须为命令“llb rsite checker”指定的可访问性检查规则的名称。
check_ip	可选，该参数指定 LLB 远程站点所属网段中要进行可访问性检查规则的 IP 地址。当参数“network_ip”的取值为一个 IP 地址时，不需要指定该参数。



注意：如果一个 LLB 远程站点被删除，将不对该 LLB 远程站点进行探测。

no llb rsite net <rsite_name> [network_ip] [netmask|prefix]

该命令用于删除指定的 LLB 远程站点。如果指定了参数“network_ip”和“netmask|prefix”，仅删除指定 LLB 远程站点的特定 IP 网段。

show llb rsite net [rsite_name]

该命令用于显示指定的 LLB 远程站点。如果不指定参数“rsite_name”，系统将显示所有已经配置的 LLB 远程站点。

clear llb rsite net

该命令用于删除所有已经配置的 LLB 远程站点。

llb rsite checker <checker_name> {tcp|icmp} <port> [interval] [rsite_up] [rsite_down]

该命令用于为 LLB 远程站点定义一个可访问性检查规则。系统支持定义最多 32 个可访问性检查规则。

checker_name	该参数指定可访问性检查规则的名称。取值必须为最大长度不大于 31 个字节的字符串。如果以数字开头，必须将该名称置于双引号内。
tcp icmp	该参数指定可访问性检查规则的类型。
port	该参数指定“tcp”类型的可访问性检查规则的目的端口。

取值必须为 1 至 65535 之间的整数。

当可访问性检查条件类型为“icmp”时，此参数将无效。

interval	可选，该参数指定进行可访问性检查的时间间隔，单位为秒。取值必须为 5 到 300 之间的整数，默认值为 30。如果通过命令“ llb rsite net ”配置了超过 400 个远程站点，则时间间隔应不少于 10 秒；如果配置了超过 800 个远程站点，则时间间隔应不少于 15 秒。
rsite_up	可选，该参数指定标识 LLB 远程站点状态为“UP”需要可访问性检查连续成功的次数。取值必须为 1 到 255 之间的整数。可访问性检查条件默认值为 3。
rsite_down	可选，该参数指定标识 LLB 远程站点状态为“DOWN”需要可访问性检查规则连续失败的次数。取值必须为 1 到 255 之间的整数，默认值为 3。

no llb rsite checker <checker_name>

该命令用于删除指定的可访问性检查规则。

show llb rsite checker [checker_name]

该命令用于显示指定的可访问性检查规则。如果不指定参数“checker_name”，将显示所有的可访问性检查规则。

clear llb rsite checker

该命令用于删除系统中所有的可访问性检查规则。

show llb rsite status [rsite_name]

该命令用于显示指定远程站点在每条 LLB 链路上的状态。如果不指定参数“rsite_name”，系统显示所有远程站点在每条 LLB 链路上的状态。

示例：

Demo(config)#show llb rsite status						
Remote site: Beijing						
net: 10.3.0.10/24						
Gateway	Status	Up Time	Down	Latest Down Event		Down Time
10.8.1.1	UP	10:30:00	0			
10.8.2.1	DOWN	00:00:00	1	Tue May 28 02:28:16 2015		00:05:00
net: 10.3.1.10/24						
Gateway	Status	Up Time	Down	Latest Down Event		Down Time
10.8.1.1	UP	10:30:00		Tue May 28 02:10:16 2015		00:00:00
10.8.2.1	UP	00:00:00	0			

➤ DNS Proxy

12.3 入向链路负载均衡

llb dns host <host_name> <ip> [weight] [port] [link_name]

该命令用于为指定 DNS 域名增加一条用于 LLB 入向 DNS 解析的 A 或 AAAA 记录。系统支持最多 2048 个 DNS 域名。系统允许为每个域名配置最多 128 个资源记录（包括 A 和 AAAA 记录）。

host_name	该参数指定 DNS 域名，格式为“www.xyz.com”。取值必须为最大长度不大于 128 个字节的字符串，该字符串中由“.”分隔的各部分长度不能超过 63 个字节。该参数支持通配符“*”，包含通配符的域名必须置于双引号内，域名不能以“.”结尾。此外，包含通配符“*”的域名，通配符“*”必须在首位。例如，“*.com”或者“*mail.array.com”。当设置参数取值为“*.com”时，所有以“.com”结尾的域名都会被命中，例如“www.abc.array.com”、“www.xyz.com”。
ip	该参数指定 DNS 域名对应服务的 IP 地址，取值必须为 IPv4 地址或 IPv6 地址。在 LLB 与 SLB 配合使用的场景，该参数取值可以为虚拟服务的 VIP。参数“host_name”和“ip”的取值将组成该域名的 A 或者 AAAA 记录。
weight	可选，该参数指定使用 wrr 算法时，该资源记录的权重。取值必须为 1 到 65,535 之间的整数，默认值为 1。
port	可选，该参数指定 DNS 域名对应服务的服务器端口，用于健康检查。在 LLB 与 SLB 配合使用的场景，该参数取值可以为虚拟服务的端口。取值必须为 0 到 65,535 之间的整数，默认值为 0。 如果参数取值为 0，系统将会首先查找 IP 地址与该命令中配置的 IP 相同的第一个虚拟服务；如果没有匹配到合适的虚拟服务，那么系统将会查找 IP 地址与该命令中配置的 IP 相同且后台服务端口为 0（ip/l2ip/l2mac 后台服务）的后台服务；如果仍然没有匹配到，那么系统将会继续查找 IP 地址与该命令中配置的 IP 相同的第一个后台服务。找到后台服务或虚拟服务后，系统将向该服务指定的端口发送数据包进行健康检查。
link_name	可选，该参数指定 LLB 链路名称（通过“llb link route”命令定义）。默认值为空，表示系统将会自动查找已配置的 LLB 链路。



注意：使用该命令配置的 A 或 AAAA 资源记录不能应答该域名的 CNAME (Canonical Name, 别名) 类型的 DNS 解析请求。

no llb dns host <host_name> <ip>

该命令用于删除指定 DNS 域名的一条资源记录。

show llb dns host [host_name]

该命令用于显示指定 DNS 域名的资源记录。如果没有指定参数 “host_name”，将显示所有 DNS 域名的资源记录。

clear llb dns host

该命令用于清除所有 DNS 域名的资源记录。

llb dns ttl <host_name> <seconds>

该命令用于为指定 DNS 域名设置其资源记录的生存时间 (Time to Live, TTL)。如果不配置该命令，DNS 域名的默认 TTL 值为 60 秒。

host_name 该参数指定 DNS 域名。

seconds 该参数指定与 DNS 域名相关的资源记录被缓存的时长，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数。取值为 0 表示资源记录不会被缓存。

show llb dns ttl <host_name>

该命令用于显示指定 DNS 域名的 TTL 配置。

llb dns reply <host_name> <max_rr_count>

该命令用于为指定的 DNS 域名设置其 DNS 响应信息中可返回的最大资源记录数。

host_name 该参数指定 DNS 域名。

max_rr_count 该参数指定 DNS 响应信息中可返回的最大资源记录数。取值必须为 1 到 3 之间的整数。

默认值为 3。

show llb dns reply [host_name]

该命令用于显示指定的 DNS 域名的可返回的最大资源记录数设置。如果没有指定参数 “host_name”，则显示所有 DNS 域名的可返回的最大资源记录数设置。

llb method inbound {rr|wrr|proximity}

该命令用于为入向链路负载均衡定义以下算法：

- rr: Round Robin, 轮询算法
- wrr: Weighted Round Robin, 加权轮询算法
- proximity: 就近性算法

默认算法为 rr。



注意：如果要使用 proximity 算法，需要先进行命令 “ip eroute” 的相关配置。

12.4 链路健康检查

llb link health {on|off}

该命令用于启用或禁用链路负载均衡的健康检查。默认情况下，该功能是禁用的。

以下命令分别可以配置 ICMP、TCP 和 DNS 三种不同类型的健康检查。系统支持为每一条链路配置最多 8 个健康检查。

llb link health checker icmp <link_name> <host> [hc_interval] [timeout] [hc_up] [hc_down]

该命令用于为 LLB 链路配置 ICMP 类型的健康检查。ICMP 类型的健康检查允许设备通过向目的主机发送 ICMP 请求，来检测指定链路的健康状况。

link_name	该参数指定通过命令 “llb link route” 配置的 LLB 链路的名称。
host	该参数指定目的主机的主机名或者 IP 地址。目的主机的 IP 地址必须为 IPv4 或 IPv6 地址。若指定为主机名，对于 IPv4 链路，使用该主机对应的 IPv4 地址进行健康检查；对于 IPv6 链路，使用该主机对应的 IPv6 地址进行健康检查。若指定为 IP 地址，必须置于双引号内。
hc_interval	可选，该参数指定对 LLB 链路健康检查的时间间隔，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 10。
timeout	可选，该参数指定 LLB 链路健康检查的超时时间，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 5。 注意： 超时时间必须小于健康检查的时间间隔。
hc_up	可选，该参数指定标识 LLB 链路的状态为 “UP” 需要的连续健康检查成功的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。

hc_down 可选，该参数指定标识 LLB 链路的状态为 “DOWN” 需要的连续健康检查失败的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。

示例：

```
Demo(config)#llb link health checker icmp "link1" "10.191.2.130" 10 5 3 3
Demo(config)#llb link health checker icmp "link1" "10.191.2.131" 10 5 3 3
```

no llb link health checker icmp <link_name> <host>

该命令用于删除指定 LLB 链路的一个 ICMP 类型的健康检查。

llb link health checker tcp <link_name> <host> <port> [hc_interval] [timeout] [hc_up] [hc_down]

该命令用于为指定 LLB 链路配置 TCP 类型的健康检查。TCP 类型的健康检查允许设备通过尝试与目的主机建立 TCP 连接，来检测指定链路的健康状况。

table
link_name	该参数指定 LLB 链路的名称。
host	该参数指定目的主机的主机名或者 IP 地址。目的主机的 IP 地址可以为 IPv4 或 IPv6 地址。若指定为主机名，对于 IPv4 链路，使用该主机对应的 IPv4 地址进行健康检查；对于 IPv6 链路，使用该主机对应的 IPv6 地址进行健康检查。若指定为 IP 地址，必须置于双引号内。
port	该参数指定健康检查的目的主机的端口，用作 TCP 报文的目的 IP。取值必须为 1 到 65,535 之间的整数。
hc_interval	可选，该参数指定 LLB 链路健康检查的时间间隔，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 10。
timeout	可选，该参数指定 LLB 链路健康检查的超时时间，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 5。 **注意：** 超时时间必须小于健康检查的时间间隔。
hc_up	可选，该参数指定标识 LLB 链路的状态为 “UP” 需要的连续健康检查成功的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。
hc_down	可选，该参数指定标识 LLB 链路的状态为 “DOWN” 需要的连续健康检查失败的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。

示例：


```
Demo(config)#llb link health checker tcp "link1" "www.xyz.com" 80 10 5 3 3
Demo(config)#llb link health checker tcp "link1" "10.191.2.141" 21 10 5 3 3
```

no llb link health checker tcp <link_name> <host> <port>

该命令用于删除指定 LLB 链路的一个 TCP 类型的健康检查。

llb link health checker dns <link_name> <host> <host_name> [interval]
[timeout] [hc_up] [hc_down]

该命令用于为 LLB 链路配置 DNS 类型的健康检查。DNS 类型的健康检查允许设备通过向目的主机发送 DNS 解析请求，来检测指定链路的健康状况。

link_name	该参数指定 LLB 链路的名称。
host	该参数指定目的主机的主机名或者 IP 地址。目的主机 IP 地址可以为 IPv4 或 IPv6 地址。若该参数指定为主机名，对于 IPv4 链路，使用该主机对应的 IPv4 地址进行健康检查；对于 IPv6 链路，使用该主机对应的 IPv6 地址进行健康检查。若指定为 IP 地址，必须置于双引号内。
host_name	该参数指定需要解析的 DNS 域名。取值必须为最大长度不大于 128 个字节的字符串。根据域名解析的结果检测链路的健康状况。
hc_interval	可选，该参数指定 LLB 链路健康检查的时间间隔，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 10。
timeout	可选，该参数指定 LLB 链路健康检查的超时时间，单位为秒。取值必须为 1 到 65,535 之间的整数。默认值为 5。 注意： 超时时间必须小于健康检查的时间间隔。
hc_up	可选，该参数指定标识 LLB 链路的状态为“UP”需要的连续健康检查成功的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。
hc_down	可选，该参数指定标识 LLB 链路的状态为“DOWN”需要的连续健康检查失败的次数。取值必须为 1 到 65,535 之间的整数。默认值为 3。

示例：

```
Demo(config)#llb link health checker dns "link1" 10.191.2.150 www.test.com 20 5 3 3
Demo(config)#llb link health checker dns "link1" "10.191.2.151" "www.test.com" 20 5 3 3
```

no llb link health checker dns <link_name> <host> <host_name>

该命令用于删除指定 LLB 链路的一个 DNS 类型的健康检查。

show llb link health checker [link_name]

该命令用于显示指定 LLB 链路的健康检查配置。如果没有指定参数“link_name”，将显示所有 LLB 链路的健康检查配置。

clear llb link health checker [link_name]

该命令用于清除指定 LLB 链路的所有健康检查。如果没有指定参数“link_name”，将清除所有 LLB 链路的健康检查。

llb link health relation <link_name> <relationship>

该命令用于设置指定链路的所有的健康检查之间的关系。

link_name	该参数指定链路的名称。
relationship	该参数指定链路的所有健康检查之间的关系。取值必须为“and”或“or”，不区分大小写： • and: 所有健康检查都成功时，才认为该链路是可用的。 • or: 任何一个健康检查成功，就认为该链路是可用的。 默认值为“or”。

show llb link health relation [link_name]

该命令用于显示指定链路的“llb link health relation”命令配置。如不指定参数“link_name”，则显示所有链路的“llb link health relation”配置。

12.5 LLB 支持 IP 地址组

ipgroup name <ip_group_name> [group_type]

该命令用于创建一个新的 IP 地址组。系统最多支持 1024 个 IP 地址组。

ip_group_name	该参数指定 IP 地址组的名称。 取值必须是长度不超过 128 个字符的字符串。支持字母、数字和下划线，必须以字母开头。
group_type	可选，该参数指定 IP 地址组的类型。取值必须为“ipv4”或“ipv6”。默认值为“ipv4”。

no ipgroup name <ip_group_name>

该命令用于删除一个指定的 IP 地址组并清空其所包含的 IP 地址段。当一个 IP 地址组包含有被使用的 IP 地址时，该 IP 地址组无法被删除。

show ipgroup name

该命令用于显示所有的 IP 地址组。

clear ipgroup name

该命令用于删除所有的 IP 地址组并清空其所包含的 IP 地址段。当地址组正在被其它功能使用时，无法删除地址组。

show statistics ipgroup [ip_group_name]

该命令用于显示指定 IP 地址组的统计信息。如果没有指定参数“ip_group_name”，系统将显示所有 IP 地址组的统计信息。

clear statistics ipgroup [ip_group_name]

该命令用于清除指定 IP 地址组的统计信息。如果没有指定参数“ip_group_name”，系统将清除所有 IP 地址组的统计信息。

ipgroup address <ip_group_name> <start_ip> [end_ip/mask/prefix]

该命令用于向一个已存在的 IP 地址组内添加地址段。系统支持通过 “IP+掩码/前缀长度” 和 “起始 IP+结束 IP” 两种方式配置 IP 地址段。

同一个地址段可以添加到多个 IP 地址组，但同一个 IP 地址组内的地址段不能有重叠。

group_name	该参数指定已配置的 IP 地址组的名称。
start_ip	该参数指定添加到地址组的 IP 地址段的起始地址。可以为 IPv4 或 IPv6 地址。
end_ip/mask/prefix	可选，该参数指定 IP 地址段的结束地址，或是地址段 IPv4 的掩码或 IPv6 的前缀长度。

系统支持的 IP 地址段数量取决于系统内存的大小，如下表所示：

表12 - 5 最大 IP 地址段数量

规格	内存					
	2G	4G	8G	16G	32G	64G
最大 IP 地址段数量	10,000	20,000	1,000,000	2,000,000	4,000,000	4,000,000

no ipgroup address <ip_group_name> <start_ip> [end_ip/mask/prefix]

该命令用于删除一个指定 IP 地址组的指定地址段。

show ipgroup address [ip_group_name]

该命令用于显示指定 IP 地址组内的所有 IP 地址段。如果没有指定参数“ipgroup_name”，系统将显示所有 IP 地址组内的所有 IP 地址段。

clear ipgroup address [ip_group_name]

该命令用于清除指定 IP 地址组内的所有 IP 地址段。如果没有指定参数“group_name”，系统将清除所有 IP 地址组内的所有 IP 地址段。

ipgroup ipregion <ip_group_name> <ipregion_name>

该命令用于将指定的 IP 域表关联到指定的 IP 地址组上。一个 IP 地址组最多可以关联 64 个 IP 域表，一个 IP 域表可以关联到多个 IP 地址组。

ipgroup_name 该参数指定已配置的 IP 地址组的名称。

ipregion_name 该参数指定已有的 IP 域表名称。管理员可以通过命令“**show ipregion name**”和“**show ipregion geoip**”查看可以关联的 IP 域表。

注意：

- 取值不能是通过命令“**ipregion proximity**”自动生成的域表。
- 取值不能为命令“**show ipregion geoip**”输出的域表中后缀为“.csv”的域表。

**注意：**

- 通过该命令关联的 IP 域表，其中的地址段不能与通过命令“**ipgroup address**”添加的 IP 地址重叠。
- 如果管理员修改或删除该命令配置的 IP 域表，则需要重新关联。

no ipgroup ipregion <ip_group_name> <ipregion_name>

该命令用于删除指定的 IP 地址组和 IP 域表的关联关系。

show ipgroup ipregion [ip_group_name]

该命令用于显示指定的 IP 地址组和 IP 域表的关联关系。如果没有指定参数“ip_group_name”，系统将显示所有 IP 地址组和 IP 域表的关联关系。

clear ipgroup ipregion [ip_group_name]

该命令用于清除指定的 IP 地址组和 IP 域表的关联关系。如果没有指定参数“ip_group_name”，系统将清除所有 IP 地址组和 IP 域表的关联关系。

show ipgroup match <ip_address>

该命令用于查询并显示指定 IP 所归属的所有 IP 地址组和地址段。

12.6 LLB 统计功能

llb link statistics {on|off}

该命令用于启用或禁用 LLB 链路的统计功能。默认情况下，该功能是禁用的。

clear statistics llb link [link_name]

该命令用于清除指定链路的统计信息。如果不指定参数“link_name”，则清除所有链路的统计信息。

show llb link status [detail]

该命令用于显示 LLB 链路的状态和链路健康检查状态的信息。

detail 可选。如果指定参数“detail”，将显示所有 LLB 链路的状态、健康检查的状态及相关的汇总信息，如请求成功次数、请求失败次数等。

show llb link bandwidth

该命令用于显示 LLB 链路的入向与出向带宽统计信息。

show llb link connection

该命令用于显示 LLB 链路连接的统计信息，包括链路名称、网关 IP 地址和链路的当前连接数。

show statistics eroute

该命令用于显示 Eroute 相关的统计信息。具体包括 Eroute、Droute、IPflow 和 LLB 链路路由的统计信息。

clear statistics eroute

该命令用于清除 Eroute 相关的统计信息。具体包括 Eroute、Droute、IPflow 和 LLB 链路路由的统计信息。

show statistics ipflow <ip_address>

该命令用于显示指定 IP 地址的 IPflow 路由统计信息。

ip_address 该参数指定用于过滤 IPflow 统计信息的源 IP 或目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。若指定为“0.0.0.0”，

则显示所有 IPv4 地址的 IPflow 路由统计信息。若指定为“::”，则显示所有 IPv6 地址的 IPflow 路由统计信息。

show statistics rts <ip_address>

该命令用于显示指定的 IP 地址的 RTS 路由的统计信息。

ip_address 该参数指定用于过滤 RTS 路由统计信息的源 IP 地址或目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。若指定为 0.0.0.0，则显示所有 IPv4 地址相关的 RTS 路由统计信息；若该参数指定为::，则显示所有 IPv6 地址相关的 RTS 路由统计信息。

show statistics droute

该命令用于显示直连路由的统计信息。

show statistics llb dd

该命令用于显示动态探测（dd）方法的相关统计信息。

示例：

```
Demo(config)#show statistics llb dd

dd entry num: 3
dd sent packets num: 72
dd probing dstip num: 3
detector ipv4 llb link route num: 3
detector ipv6 llb link route num: 3
daemon detector detect times: 4
filter out RINGQ ipv4 data not into user queue: 0
filter out RINGQ ipv6 data not into user queue: 0
```

show statistics llb rsite [rsite_name]

该命令用于显示指定的 LLB 远程站点的统计数据。如果不指定参数“rsite_name”，系统显示所有 LLB 远程站点的统计数据。

示例：

```
Demo(config)#show statistics llb rsite

Remote site: Beijing
net: 10.3.0.10/24

Gateway          Status  Latest Response Time  Detect Times  UP times  Down Times
10.8.1.1          UP      1ms                   100           98        2
10.8.2.1          DOWN    timeout               100           90        10
net: 10.3.1.10/24
```

Gateway	Status	Latest Response Time	Detect Times	UP times	Down Times
10.8.1.1	UP	2ms	90	89	1
10.8.2.1	UP	1ms	90	87	3

clear statistics llb rsite [rsite_name]

该命令用于清除指定的 LLB 远程站点的统计数据。如果不指定参数“rsite_name”，系统将清除所有 LLB 远程站点的统计数据。

show statistics llb dnsproxy [server_name]

该命令用于显示为 DNS 代理功能配置的指定的 DNS 服务器的统计信息。如果没有指定参数“server_name”，将显示所有为 DNS 代理功能配置的 DNS 服务器的统计信息。

clear statistics llb dnsproxy [server_name]

该命令用于删除为 DNS 代理功能配置的指定的 DNS 服务器的统计信息。如果没有指定参数“server_name”，将删除所有为 DNS 代理功能配置的 DNS 服务器的统计信息。

show statistics llb inbound [host_name]

该命令用于显示指定 DNS 域名的入向链路统计信息，包括 LLB 链路的状态及入向被命中的次数。如果没有指定参数“host_name”，则显示 DNS 域名、A 记录和 AAAA 记录的数量以及所有 DNS 域名的入向链路统计信息。

clear statistics llb inbound

该命令用于清除所有域名的 LLB 入向链路统计信息。执行该命令后，LLB 链路的入向命中次数将会被清零。

12.7 LLB 通用配置

llb probe tcp <source_ip> <source_port> <destination_ip> <destination_port>

该命令用于模拟客户端通过指定源 IP 和源端口发送一个 TCP SYN 报文至目的 IP 地址和目的端口，以检测指定 IP 地址所匹配的流量策略。

source_ip 该参数指定源 IP 地址。

source_port 该参数指定源端口号。

destination_ip 该参数指定目的 IP 地址。

destination_port 该参数指定目的端口号。

llb probe udp <source_ip> <source_port> <destination_ip>
<destination_port>

该命令用于模拟客户端通过指定源 IP 和源端口发送一个 UDP 报文至目的 IP 地址和目的端口，以检测指定 IP 地址所匹配的流量策略。

source_ip 该参数指定源 IP 地址。

source_port 该参数指定源端口号。

destination_ip 该参数指定目的 IP 地址。

destination_port 该参数指定目的端口号。

llb probe icmp <source_ip> <destination_ip>

该命令用于模拟客户端通过指定源 IP 的发送一个 ICMP Request 报文至目的 IP 地址，以检测指定 IP 地址所匹配的流量策略。

source_ip 该参数指定源 IP 地址。

destination_ip 该参数指定目的 IP 地址。

show llb connection [filter_string]

该命令用于显示 NAT 连接中的指定参数的信息。如不指定 “filter_string” 参数，系统将显示 NAT 类型连接的所有信息。显示内容包括协议类型、客户端源 IP 和端口、NAT 转换后的源 IP 和端口、目的 IP、目的端口、路由类型、路由名称、接口名称、网关地址和超时时间。

filter_string 可选，该参数指定需要显示的过滤参数名称。可指定多个过滤参数，参数之间用逗号分隔。

参数格式为 “关键词 1=xxx, 关键词 2=xxx, ...”，例如 “source=10.8.1.1, dport=80, proto=tcp”。系统支持的关键词包括：

- source: 表示客户端 IP 地址。
- local: 表示本地 IP 地址。
- destination: 表示服务端 IP 地址。
- sport: 表示客户端端口号。
- lport: 表示本地端口号。

- dport: 表示服务端口号。
- proto: 表示协议类型, 取值为 “tcp”、“udp”、“icmp” 或 “all”, “all” 表示上述全部协议。

以上关键词及其取值都不区分大小写。默认值为空, 即显示 NAT 连接的所有信息。



注意: 删除 NAT 相关的配置或者 LLB 路由后, 通过该命令显示 NAT 连接信息时, 与该 NAT 连接相关的已建立的 LLB 连接仍然会存在。只有当没有流量命中该 LLB 连接时, 连接超时后该 LLB 连接才会自动删除。

clear llb connection [*filter_string*]

该命令用于清除 NAT 连接中的指定参数的信息。如不指定 “filter_string” 参数, 系统将清除 NAT 类型连接的所有信息。

第13章 全局服务器负载均衡（GSLB）

本章介绍 SDNS（Smart DNS，智能 DNS）功能的相关配置命令以实现 GSLB（Global Server Load Balance，全局服务器负载均衡）。

13.1 基本 SDNS 命令

sdns {on|off}

该命令用于启用或禁用 SDNS 功能。SDNS 功能启用后，系统会监听所有 IP 地址（包括虚拟 IP 地址），可能会导致内存占用率过高。所以推荐管理员在启用该功能前，先通过命令“**sdns listener**”设置 SDNS 服务监听的 IP 地址和端口号。该功能默认是禁用的。使用 SDNS 功能前，请导入包含 GSLB 特性的产品许可密钥。

在 SDNS 模块内的命令不支持加载或同步命令“**sdns on/off**”，不支持加载或同步命令“**sdns on/off**”的命令如下：

```
sdns config file
sdns config scp
sdns sync config to
sdns sync config from
```

在系统级别下的命令允许加载、同步命令“**sdns on/off**”，支持加载或同步命令“**sdns on/off**”的命令如下：

```
config file
config net
config all
synconfig sdns to
synconfig to
synconfig from
ha synconfig bootup on
ha synconfig runtime on
synconfig increment enable
write file
write all
```



注意：

- 当禁用 SDNS 功能时，不允许执行“**sdns dps**”和“**sdns iana**”命令；
- 命令“**sdns config write**”保存 SDNS 配置时会保存命令“**sdns on/off**”，但是通过其他 SDNS 模块的命令加载保存的配置时不会加载命令“**sdns on/off**”；
- SDNS 模块加载配置时，启用 HA 运行时同步，由于命令“**sdns on/off**”没有被加载，所以命令“**sdns on/off**”不会被同步。

- 当禁用 SDNS 功能时，系统会删除所有自动学习到的 SDNS 服务的配置。

sdns reload

该命令用于重新加载 SDNS 服务。

- 执行该命令时，若 SDNS 服务为 off 状态，则命令执行失败。
- 执行该命令时，若 SDNS 服务为 on 状态，则系统将进行如下操作：
 - 重新加载 BIND 服务器的配置文件；
 - 重新关联 IP 域表和 SDNS 区域，生成新的 SDNS IP 域就近性规则（对应“**sdns ipregion proximity** <ipregion_name> <region_name>”命令）；
 - 当后台存在 2 个或 2 个以上 named 进程时，会杀掉所有 named 进程，并重新启动一个 named 进程；
 - 除 **sdns ipregion proximity** 配置外，其他 SDNS 的配置不会重新加载。

show sdns status

该命令用于显示 SDNS 功能的状态，SDNS 递归查询功能的状态，以及 SDNS 数据中心、SDNS 服务 IP、SDNS 池、SDNS 链路、域名、区域、就近性规则、健康检查模板和健康检查实例的使用情况。

例如：

```
Demo(config)#show sdns status
SDNS is ON
SDNS recursion is OFF
Dcs:                2 / 64
Service IPs:        10 / 20000
Pools:              4 / 16000
Links:              1 / 1024
Host names:         2 / 16000
Regions:            10 / 100
Proximities:        100 / 2000000
Monitors:           20 / 1000
Monitor instances:  50 / 25000
```

show sdns all

该命令用于显示 SDNS 功能的全部配置信息。



注意：命令“**show sdns all**”不会显示 SDNS 配置文件。

clear sdns all

该命令用于将 SDNS 功能的全部配置重置为默认值。



注意：当使用“**clear sdns all**”或“**clear config secondary**”命令将 SDNS 配置重置为默认值时，系统将不检查 License 是否对 GSLB 功能进行授权。命令“**clear sdns all**”不会清除 SDNS 配置文件。

show sdns summary [host_name]

该命令用于显示指定域名相关的配置信息。如果不指定参数“host_name”，系统将显示所有域名相关的配置信息。

例如：

```
Demo(config)#show sdns summary "www.1.com"
sdns host name "www.1.com" 60
sdns policy region "p_ct" "www.1.com" "p1" "ct" 0
    sdns region name "ct"
    sdns pool name "p1" 3
    sdns pool method primary "p1" "rr"
    sdns pool health relation "p1" "and"
    sdns pool service "p1" "s1"
        sdns service ip "s1" 1.1.1.1 0
        sdns service health relation "s1" "and"

sdns policy default "www.1.com" "p2"
    sdns pool name "p2" 3
    sdns pool method primary "p2" "rr"
    sdns pool monitor apply "p2" "m1"
    sdns pool monitor apply "p2" "m2"
    sdns pool health mixrelation "p2" "(m1 and m2)"
    sdns pool service "p2" "s2"
        sdns service ip "s2" 2.2.2.2 0
        sdns link service "l1" "s2"
        sdns service monitor apply "s2" "m1"
        sdns service health relation "s2" "and"
    sdns pool service "p2" "s3"
        sdns service ip "s3" 2.2.2.3 0
        sdns service health relation "s3" "and"
```

sdns edns ecs on [mode]

该命令用于为 SDNS 启用 ECS（EDNS Client Subnet）。该功能默认设置为禁用。

mode 可选，该参数指定 ECS 模式。取值必须为：

- “空”：表示系统会在 SDNS 域名转发时在 DNS 请求中插入客户端源 IP 地址。SDNS 域名转发功能通过命令 “sdns host name” 进行配置。
- “resolve”：表示系统在 SDNS 域名解析时对 ECS 进行解析。

取值默认为空。

sdns edns ecs off [mode]

该命令用于为 SDNS 禁用 ECS。

mode 可选，该参数指定 ECS 模式。取值必须为：

- “空”：表示系统在 SDNS 域名转发时不在 DNS 请求中插入客户端源 IP 地址。
- “resolve”：表示系统在 SDNS 域名解析时不对 ECS 进行解析。

取值默认为空。

show sdns edns ecs [mode]

该命令用于显示 ECS 的配置。该命令支持在分区模式下执行。

mode 可选，该参数指定 ECS 模式。取值必须为：

- “空”：表示显示 SDNS 域名转发功能的 ECS 配置。
- “resolve”：表示显示 SDNS 域名解析功能的 ECS 配置。

取值默认为空。

show sdns query match <source_ip> <host_name> [query_type]

该命令用于显示特定 DNS 查询的解析过程。

source_ip 该参数指定 DNS 查询的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。

host_name 该参数指定 DNS 查询中的域名。取值必须为最大长度不大于 128 个字节的字符串，格式为 www.xyz.com。该字符串中由 “.” 分隔的各部分的长度不能超过 63 个字节。参数取值不支持通配符 “*” 和其他特殊字符，并且不能以 “.” 结尾。

query_type 可选，该参数指定 DNS 查询的类型。取值必须为 “A” 或 “AAAA”。默认值为 “A”。

示例：

```
Demo(config)#show sdns query match 10.6.0.166 www.example.com
[1] Check Host Name:
"www.example.com" found.
[2] Check Region Matched:
all
[3] Check Region Policy:
Check region "all" ---> Found region policy "all" with priority 0
Matched Region Policy: "all"
Matched Pool: "pool_default"
Select member from pool "pool_default"
[4] Result:
      A Record: 10.8.6.233
```

sdns resource threshold <indicator_type> <mum>

该命令用于设置指定 SDNS 监控指标的阈值。

indicator_type 该参数指定监控指标类型。取值必须为 “asr”，表示 SDNS 解析成功率。

mum 该参数指定百分比阈值。当参数 “indicator_type” 取值为 asr 时，取值必须为 0 到 100 之间的整数，表示请求解析成功率的下限阈值。例如当取值为 5 时，则系统在一分钟内的请求解析成功率低于 5% 时，系统提示告警。

no sdns resource threshold <indicator_type>

该命令用于删除指定 SDNS 监控指标的阈值

show sdns resource threshold

该命令用于显示 SDNS 监控指标的阈值配置。

clear sdns resource threshold

该命令用于清除已配置的所有 SDNS 监控指标的阈值。

sdns addition section on

该命令用于为 SDNS 启用响应报文带有 A/AAAA 附加资源记录的功能。该功能默认设置为禁用。

sdns addition section off

该命令用于为 SDNS 禁用响应报文带有 A/AAAA 附加资源记录的功能。

show sdns addition section

该命令用于显示响应报文是否带有 A/AAAA 附加资源记录功能的启用状态。

13.2 SDNS 域名

sdns host name <host_name> [ttl] [type]

该命令用于定义一个 SDNS 域名。系统支持最多 16,000 个 SDNS 域名。

host_name

该参数指定 SDNS 域名。取值必须为长度不大于 128 个字节的字符串，格式为 `www.xyz.com`。该字符串中由“.”分隔的各部分长度不能超过 63 个字符。该参数的取值支持通配符“*”、特殊字符“_”和“.”，其他特殊字符均不支持。“.”不能置于起始和结尾位置，“_”不能置于起始位置，取值不允许为系统保留字“default”、“all”或“global”，这些系统保留字不区分大小写。

对于通配符“*”，可以配置为单个“*”或“*”与其他字符的组合。“*”与其他字符组合使用时，“*”必须位于取值的起始位置，后面跟随至少一个其他字符，整个字符串必须置于双引号里，例如“*a”。如果一个域名同时匹配两个通配域名，会根据最长后缀匹配的原则选择域名。需要注意的是，SDNS DNSSEC 和 SDNS 别名（Canonical Name，CNAME）不支持通配域名。

当参数“type”指定为“forward_only”时，SDNS 域名定义为转发域名。转发域名支持配置泛域名，例如 *.com。转发域名不能和 CNAME 池关联。

ttl

可选，该参数指定了与本 SDNS 域名相关的资源记录被缓存的时长。取值必须为 0 到 4,294,967,295 之间的整数，单位为秒。默认值为 60。

type

可选，该参数指定 SDNS 域名的类型。取值必须为：

- **forward_only**: 表示启用 SDNS 域名转发功能，即系统将转发匹配指定域名的 DNS 请求，不进行本地解析。当参数“host_name”指定为泛域名时，查询该域名及其子域名的 DNS 请求都将被转发。需要注意的是当参数“type”取值为“forward_only”时：
 1. 参数“ttl”不生效。
 2. 如果 SDNS 服务池中同时包含 SDNS 服务 IP 为

IPv4 和 IPv6 的 SDNS 服务（且都可用）时，系统既支持使用 IPv4 地址进行转发，也支持使用 IPv6 地址进行转发。

- 空：表示系统对 SDNS 域名进行本地解析。

默认值为空。



注意：如果 SDNS 构造的响应报文中数据部分超过 512 字节，则不会向客户端返回响应报文。

no sdns host name <host_name>

该命令用于删除指定的 SDNS 域名。

show sdns host name

该命令用于显示全部 SDNS 域名。

clear sdns host name

该命令用于清除全部 SDNS 域名。

sdns host persistence <timeout> [host_name] [ipv4_netmask|ipv4_prefix] [ipv6_prefix] [query_type]

该命令用于设置指定 SDNS 域名的会话保持关系的超时时间。配置该命令后，系统将使用客户端 IP 地址和指定的子网掩码或者前缀长度确定一个子网，后续访问该 SDNS 域名的 DNS 请求，系统都将保持会话。如果不指定参数“host_name”，该命令将设置全局的会话保持关系的超时时间。

如果不配置该命令，默认的全局会话保持关系的超时时间为 0 秒，表示不进行会话保持。

timeout	该参数指定会话保持关系的超时时间，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数。
host_name	可选，该参数指定已存在的 SDNS 域名。取值必须为长度不大于 128 个字节的字符串。默认值为“”。
ipv4_netmask ipv4_prefix x	可选，该参数指定 IPv4 地址对应的子网掩码或前缀长度，取值可以是点分地址格式或是 1 至 32 之间的整数。默认值为 32。
ipv6_prefix	可选，该参数指定 IPv6 地址对应的前缀长度，取值必须为 1 至 128 之间的整数。默认值为 128。
query_type	可选，该参数指定 DNS 查询的资源记录类型。取值必须为 A、AAAA、CNAME 或者 MX。默认值为“ALL”，表示系统将设置全部 DNS 资源记录类型的会话保持关

系的超时时间。

no sdns host persistence [*host_name*] [*query_type*]

该命令用于删除指定 SDNS 域名的会话保持关系的超时时间配置。

host_name	可选，该参数指定已存在的 SDNS 域名。 - 如果指定该参数，系统将删除为指定 SDNS 域名配置的会话保持关系的超时时间配置。 - 如果未指定该参数，系统将删除全部 SDNS 域名配置的会话保持关系的超时时间配置。
query_type	可选，该参数指定已存在的 DNS 查询的资源记录的类型。 - 如果指定该参数，系统将删除为指定 DNS 资源记录配置的会话保持关系的超时时间配置。 - 如果未指定该参数，系统将删除全部 DNS 资源记录配置的会话保持关系的超时时间配置。

show sdns host persistence [*host_name*] [*query_type*]

该命令用于显示指定域名的会话保持关系超时时间的配置。

host_name	可选，该参数指定已存在的 SDNS 域名。 - 如果指定该参数，系统将显示为指定 SDNS 域名配置的会话保持关系的超时时间配置。 - 如果未指定该参数，系统将显示为全部 SDNS 域名配置的会话保持关系的超时时间配置。
query_type	可选，该参数指定已存在的 DNS 查询的资源记录的类型。 - 如果指定该参数，系统将显示指定 DNS 资源记录配置的会话保持关系的超时时间配置。 - 如果未指定该参数，系统将显示全部 DNS 资源记录配置的会话保持关系的超时时间配置。

clear sdns host persistence

该命令用于清除所有域名的会话保持关系超时时间的配置。

no sdns session persistence <*host_name*> <*session_id*> [*query_type*]

该命令用于删除指定 SDNS 域名的会话保持关系的配置。

host_name	该参数指定已存在的 SDNS 域名。
session_id	该参数指定 SDNS 域名会话保持关系的会话 ID。取值可以通过命令“show statistics sdns session persistence”查看。
query_type	可选，该参数指定已存在的 DNS 查询的资源记录的类型。 • 如果指定该参数，系统将删除指定 DNS 资源记录配置的会话保持关系。 • 如果未指定该参数，系统将显示全部 DNS 资源记录配置的会话保持关系。

clear sdns session persistence [host_name] [query_type]

该命令用于清除所有 SDNS 域名的会话保持关系的配置。

host_name	可选，该参数指定已存在的 SDNS 域名。 • 如果指定该参数，系统将清除为指定 SDNS 域名配置的会话保持关系。 • 如果未指定该参数，系统将清除为全部 SDNS 域名配置的会话保持关系。
query_type	可选，该参数指定已存在的 DNS 查询的资源记录的类型。 • 如果指定该参数，系统将清除指定 DNS 资源记录配置的会话保持关系。 • 如果未指定该参数，系统将清除全部 DNS 资源记录配置的会话保持关系。

show statistics sdns session persistence [host_name]

该命令用于为指定 SDNS 域名显示当前 SDNS 会话保持关系的统计信息。如果不指定该参数，系统将显示全部 SDNS 会话保持关系的统计信息。

sdns host database import <url>

该命令用于从 HTTP 服务器或 FTP 服务器为系统导入域名数据库。

url	该参数指定加载的 IP 域表文件的 HTTP 或 FTP URL 地址，用于加载 IP 域表。

注意：FTP 类型 URL
(ftp://user:password@host:port/path) 中的“path”需

使用相对路径。

sdns host security policy <database> <policy>

该命令用于为指定的域名数据库配置安全策略。

database 已导入的域名数据库名称。

policy 该参数指定安全策略，取值必须为：

- **NOERROR**：表示无错误条件。
- **FORMERR**：表示域名服务器无法解释查询。
- **SERVFAIL**：表示由于域名服务器问题，无法处理该查询。
- **NXDOMAIN**：表示查询中引用的域名不存在。
- **NOTIMP**：表示域名服务器不支持所请求的查询类型。
- **REFUSED**：表示域名服务器由于策略原因拒绝执行指定的操作。
- **DROP**：表示丢弃请求报文。
- **BIND**：表示将请求报文转发给 bind 处理。

当取值为“NOERROR”、“FORMERR”、“SERVFAIL”、“NXDOMAIN”、“NOTIMP”或“REFUSED”时，系统将返回 DNS 响应码。

该参数取值不区分大小写。

sdns cache on

该命令用于启用 SDNS 缓存。

sdns cache off

该命令用于关闭 SDNS 缓存，默认为关闭。

sdns cache expire [min_seconds] [max_seconds]

该命令用于配置 SDNS 缓存过期时间。

min_seconds 可选，该参数指定 SDNS 缓存过期最小时间，单位为秒。取值必须为 0 至 999,998。取值为 0 时表示配置缓存过期时间为 999,999 秒，缓存过期最小时间必须小于缓存

过期最大时间。默认值为 60 秒。

max_seconds 可选，该参数指定 SDNS 缓存过期最大时间，单位为秒。取值必须为 0 至 999,998。取值为 0 时表示配置缓存过期时间为 999,999 秒，缓存过期最小时间必须小于缓存过期最大时间。默认值为 566,400 秒。

show sdns cache setting

该命令用于显示 SDNS 缓存的配置。

clear sdns cache setting

该命令用于将 SDNS 缓存配置恢复为默认值。

sdns cache prefetch on

该命令用于启用 SDNS 缓存预取。

sdns cache prefetch off

该命令用于关闭 SDNS 缓存预取。

show sdns cache prefetch setting

该命令用于显示 SDNS 缓存预取的配置。

sdns cache prefetch majordn <domain_name>

该命令用于配置 SDNS 缓存预取的重点域名。

domain_name 该参数指定需要缓存预取的重点域名。取值必须为长度不大于 127 个字节的字符串。

no sdns cache prefetch majordn <domain_name>

该命令用于删除指定的 SDNS 缓存预取重点域名的配置。

domain_name 该参数指定需要缓存预取的重点域名。取值必须为长度不大于 127 个字节的字符串。

show sdns cache prefetch majordn

该命令用于显示 SDNS 缓存预取重点域名的配置。

clear sdns cache prefetch majordn

该命令用于清除所有 SDNS 缓存预取重点域名的配置。

show sdns cache content [numbers]

该命令用于显示 SDNS 缓存的内容。

numbers 可选，该参数指定显示 SDNS 缓存内容的数量。取值为 1 至 20,000。默认值为 1,000。

clear sdns cache content

该命令用于清除所有 SDNS 缓存的内容。

13.3 SDNS 监听 IP 地址

sdns listener <ip_address> [sdns_listener_port]

该命令用于设置 SDNS 服务监听的 IP 地址和端口号。配置 SDNS 监听 IP 地址和端口号后，系统只在指定的监听 IP 地址和端口号上提供 SDNS 服务。系统允许配置最多 16 条该命令。

ip_address 该参数指定 SDNS 服务监听的 IP 地址，取值必须为 IPv4 或 IPv6 地址，但不能是广播、多播和环回地址，也不能是 “0.0.0.0” 和 “::”。

sdns_listener_port 可选，该参数指定 SDNS 服务用于监听的端口。取值必须为 1 到 65,000 之间的整数。默认值为 53。

当启用 SDNS 功能时，系统默认监听所有 IPv4 和 IPv6 地址的 53 号端口。

如果只配置 IPv4 类型的 IP 地址，系统对于已配置的 IPv4 地址和端口进行监听，对于 IPv6 类型的全部 IP 地址也进行监听。如果只配置 IPv6 类型的 IP 地址时同理。

如果配置了 IPv4 和 IPv6 类型的 IP 地址和端口，系统只监听已配置的 IP 地址和端口。



注意：

- 执行 “write memory、write file、write all 和 write net” 命令后，系统不会保存 “sdns listener <ip_address> [port]” 中默认端口 53 的配置。
- 该命令不支持配置同步、增量同步、HA 运行时配置同步和 SDNS 运行时配置同步。

no sdns listener <ip_address> [sdns_listener_port]

该命令用于删除指定的 SDNS 监听 IP 地址配置和端口配置。

show sdns listener

该命令用于显示所有的 SDNS 服务监听 IP 地址配置和端口配置。当端口配置为默认值 53 时，端口号不会显示。

clear sdns listener

该命令用于清除所有的 SDNS 监听 IP 地址配置和端口配置。

13.4 SDNS 服务

sdns service ip <service_name> <ip_address> [port] [dc_name] [hc_mode]

该命令用于定义一个 SDNS 服务。该 SDNS 服务的 IP 地址，又称为 SDNS 服务 IP，被用做指定的 SDNS 域名的解析 IP 地址，并将这个 IP 与指定的 SDNS 数据中心关联。系统支持最多 20,000 个 SDNS 服务 IP。

该命令还可以用于修改已有 SDNS 服务的 IP 地址和用于健康检查的端口号。

service_name 该参数指定 SDNS 服务的名称。取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

ip_address 该参数指定 SDNS 服务的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

port 可选，该参数指定 SDNS 服务用于健康检查的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。

dc_name 可选，该参数指定已存在的 SDNS 数据中心的名称。默认为空，表示不与任何数据中心关联。

需要注意的是当 SDNS 服务与 SDNS 链路关联后，需要先解除 SDNS 服务和 SDNS 链路的关联关系（通过命令“**no sdns link service**”），才能修改 SDNS 服务关联的数据中心。

hc_mode 可选，该参数指定 SDNS 健康检查模式，取值必须为：

- 0：表示常规模式（Normal）。在该模式下，系统采用原有行为，即当本地数据中心未收到其他数据中心返回的健康检查实例状态时，系统不会主动探测，直接将该数据中心的健康检查实例状态置为“Down”。
- 1：表示故障切换探测模式（Failover）。在该模式下，当本地数据中心未收到其他数据中心返回的健康检查实例状态时，系统将会主动探测。具体分为如下两种情况：
 - 如果健康检查模板设置了目的 IP 地址，并且设置的目的 IP 与 SDNS 服务 IP 不同，那么将 SDNS

服务与健康检查模板关联后，系统将会创建两个健康检查实例，分别为主实例（Primary Instance）和备实例（Instance）（可以通过命令“**show statistics sdns dc instance**”查看）。

- 当本地数据中心探测到其他数据中心的健康检查实例状态时，主实例健康检查状态标识为探测到的状态，备实例的健康检查状态与主实例的健康检查状态相同。
- 当本地数据中心无法探测到其他数据中心的健康检查实例状态时，主实例的健康检查状态将被标识为 Down，备实例的健康检查状态通过探测 SDNS 服务 IP 获取。
- 如果健康检查模板设置的目的 IP 地址与 SDNS 服务的 IP 相同时，将 SDNS 服务与健康检查模板关联后，系统仅生成一个健康检查实例，且本地数据中心获取健康检查实例状态失败时不进行主动探测。
- 如果健康检查模板未设置目的 IP 地址，将 SDNS 服务与健康检查模板关联后，系统只会生成一个健康检查实例。具体分两种情况：
 - 当本地数据中心收到其他数据中心的健康检查实例状态时，直接使用此状态标识健康检查实例的状态。
 - 当本地数据中心未收到其他数据中心的健康检查实例状态时，系统将主动探测健康检查实例状态。

默认值为 0。

no sdns service ip <service_name>

该命令用于删除指定的 SDNS 服务。

show sdns service ip

该命令用于显示全部 SDNS 服务。

clear sdns service ip

该命令用于清除全部 SDNS 服务。

sdns service {enable|disable} <service_name>

该命令用于启用或禁用指定的 SDNS 服务。在定义一个 SDNS 服务后，该 SDNS 服务默认是启用的。

service_name 该参数指定 SDNS 服务的名称。

show sdns service disable

该命令用于显示全部被禁用的 SDNS 服务。

show sdns service status

该命令用于显示每一个 SDNS 服务的状态，包括 SDNS 服务真实状态、状态的原因、启用状态和命中次数。

当 SDNS 服务关联 SDNS 链路时，只有 SDNS 服务与 SDNS 链路的健康检查都为 UP 状态并且都为 ENABLE 状态，通过该命令显示 SDNS 服务的状态才会显示为 UP；当 SDNS 服务或者 SDNS 链路健康检查为 DOWN 或者为 DISABLE 状态，则通过该命令显示的 SDNS 服务的状态为 DOWN。

SDNS 服务有以下几种状态：SERVICE_UP、SERVICE_DOWN、SERVICE_DISABLE；

SDNS 链路有以下几种状态：LINK_UP、LINK_DOWN、LINK_DISABLE。

例如：

```
Demo(config)#show sdns service status
s1 10.8.6.45 DOWN(SERVICE_UP,LINK_UP,LINK_DISABLE) ENABLE HITS:0
s2 10.8.6.50 UP(SERVICE_UP,LINK_UP) ENABLE HITS:5
```

13.5 SDNS 池

sdns pool name <pool_name> [max_rr_count]

该命令用于定义一个 SDNS 服务池。SDNS 服务池是 SDNS 服务的集合。系统支持最多 16,000 个 SDNS 服务池。

此外，在通过该命令定义 SDNS 服务池时，系统会同时生成同名的 SDNS 应急池。

该命令支持在分区下执行。

pool_name 该参数指定 SDNS 服务池的名称。取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

max_rr_count 该参数指定当该 SDNS 池被命中时，在 DNS 响应信息中返回的最大资源记录数。取值必须为 1 到 3 之间的整

数。默认值为 3。



注意：

- SDNS 功能使用查询到的 SDNS 域名和从被命中的 SDNS 服务池中选择的 SDNS IP 来构建资源记录。
- 如果 SDNS 服务池中同时包含 IPv4 和 IPv6 类型的 SDNS 服务 IP，系统根据请求的类型返回相应的资源记录。例如，假设参数 “max_rr_count” 取值为 3，服务池中 A 记录数为 1，AAAA 记录数为 1。当客户端请求 A 资源时，系统只返回一个 A 资源记录；当客户端请求 AAAA 资源时，系统只返回一个 AAAA 资源记录。

no sdns pool name <pool_name>

该命令用于删除指定的 SDNS 服务池。

此外，在通过该命令删除指定的 SDNS 服务池时，系统会同时删除同名的 SDNS 应急池。

show sdns pool name

该命令用于显示全部 SDNS 服务池。

clear sdns pool name

该命令用于清除全部 SDNS 服务池。

此外，在通过该命令清除 SDNS 服务池时，系统会同时清除同名的 SDNS 应急池。

sdns pool service <pool_name> <service_name>

该命令用于向指定的 SDNS 服务池中添加一个 SDNS 服务。一个 SDNS 服务可以被添加到多个 SDNS 服务池中。系统支持同时添加 SDNS 服务 IP 为 IPv4 和 IPv6 的 SDNS 服务。一个 SDNS 服务池支持同时添加最多 100 个 SDNS 服务 IP 为 IPv4 的 SDNS 服务，和最多 100 个 SDNS 服务 IP 为 IPv6 的 SDNS 服务。

此外，在通过该命令将 SDNS 服务添加到 SDNS 服务池时，系统会同时将 SDNS 服务添加到同名的 SDNS 应急池中。

pool_name 该参数指定 SDNS 服务池的名称。

service_name 该参数指定 SDNS 服务的名称。

no sdns pool service <pool_name> <service_name>

该命令用于从指定的 SDNS 服务池中删除指定的 SDNS 服务。

此外，在通过该命令删除 SDNS 服务池中指定的 SDNS 服务时，系统会同时删除同名的 SDNS 应急池中指定的 SDNS 服务。

show sdns pool service [pool_name]

该命令用于显示指定的 SDNS 服务池中的全部 SDNS 服务。如果不指定参数“pool_name”的值，将显示所有 SDNS 服务池中的全部 SDNS 服务。

clear sdns pool service <pool_name>

该命令用于清除指定的 SDNS 服务池中的全部 SDNS 服务。

此外，在通过该命令清除 SDNS 服务池中的 SDNS 服务时，系统会同时清除同名的 SDNS 应急池中的 SDNS 服务，不在 SDNS 服务池中的 SDNS 应急服务不会从 SDNS 应急池中删除。

sdns pool {enable|disable} <pool_name> [dc_name]

该命令用于启用或禁用指定 SDNS 服务池中指定数据中心下的 SDNS 服务。在定义一个 SDNS 服务池后，默认启用该服务池和服务池下所有数据中心。

pool_name	该参数指定 SDNS 服务池名称。
dc_name	可选，该参数指定 SDNS 数据中心名称。 • 如果不指定该参数，表示启用或禁用指定 SDNS 服务池。 • 如果指定该参数，表示启用或禁用指定服务池的指定数据中心下的 SDNS 服务。

show sdns pool disable

该命令用于显示所有被禁用的 SDNS 服务池和 SDNS 服务池中被禁用的数据中心。

sdns pool method primary <pool_name> <method> [expression] [sorting_mode] [oid_name]

该命令用于从指定的 SDNS 服务池中选择 SDNS 服务 IP 的一级算法或从指定的 SDNS 别名池中选择 SDNS 别名的一级算法。如果一个 SDNS 服务池或者 SDNS 别名池没有配置一级算法，则默认将使用轮询（Round Robin，rr）算法。

当服务池中同时包含 SDNS 服务 IP 为 IPv4 和 IPv6 的 SDNS 服务，系统将为这两类 SDNS 服务分别选择一级算法。例如：如果一级算法为轮询，请求 A 记录资源时仅在 A 记录资源中进行轮询，请求 AAAA 记录时，仅在 AAAA 记录资源中轮询。

pool_name	该参数指定 SDNS 服务池或 SDNS 别名池的名称。
method	该参数指定 SDNS 服务池或 SDNS 别名池使用的一级算法。 对于 SDNS 服务池，参数取值必须为：

- rr: Round Robin, 轮询算法
- grr: Global Round Robin, 全局轮询算法
- wr: Weighted Round Robin, 加权轮询算法
- gwrr: Global Weighted Round Robin, 全局加权轮询算法
- ipo: IP Overflow, IP 优先算法
- hi: Hash IP, 哈希 IP 算法
- hip: Hash IP Port, 哈希 IP Port 算法
- chi: Consistent Hash IP, 一致哈希 IP 算法
- persistence: 会话保持算法
- snmp: Simple Network Management Protocol, SNMP 算法
- drop: 丢弃算法
- bandwidth: 带宽算法
- status: 应用可用性算法
- topology: 拓扑算法
- rtt: Round Trip Time, 最短往返时间算法
- lc: Least Connections, 最少连接数
- pi: Persistent IP, 保持 IP

对于 SDNS 别名池, 参数取值必须为:

- rr: Round Robin, 轮询算法
- wr: Weighted Round Robin, 加权轮询算法
- rtd: Return to DNS, 静态 DNS 解析算法
- mf: Minimum Flow, 最小流量算法
- cpu: CPU 算法

expression

可选, 该参数指定 snmp 算法用来计算 SDNS 服务 IP 的复合权重值的 SNMP 表达式。只有当“method”设置为“snmp”时, 该参数才可用。参数取值必须为已经通过“sdns snmp exp weight”命令配置的 SNMP 表达式名称。

sorting_mode	可选，该参数指定 snmp 算法用来对 SDNS 服务 IP 排序的方式。只有当“method”设置为“snmp”时，该参数才可用。参数取值必须为： - asc: SDNS 服务 IP 按照复合权重值由低到高排序。 - dsc: SDNS 服务 IP 按照复合权重值由高到低排序。 默认值为“asc”。
oid_name	可选，该参数指定一级算法 bandwidth 和 status 用来计算权重的 SNMP OID 名称。只有当参数“method”设置为“bandwidth”、“status”或“lc”时，该参数才生效。取值必须是已经通过“sdns snmp oid”命令配置的 SNMP OID 名称。 默认值为空。

下表列出了 SDNS 服务池和 SDNS 别名池支持的各算法的具体描述。

表13 - 1 SDNS 服务池算法

算法	描述
轮询（rr）	如果 SDNS 服务池中有 3 个 SDNS 服务 IP，参数“max_rr_count”的值为 1，并且采用轮询算法，则 SDNS 服务 IP 将按“1、2、3、1、2、3...”的顺序在 DNS 响应中被返回。该算法在多核 CPU 环境下可能会有误差。
全局轮询（grr）	该算法与轮询算法原理相同。区别在于该算法在多核 CPU 环境下也可以严格运行。
加权轮询（wrr）	加权轮询算法与轮询算法类似。区别在于每个 SDNS 服务都被赋予了一个权重值。只有当第一个 SDNS 服务 IP 被返回的次数达到其权重值时，第二个 SDNS 服务 IP 才会在 DNS 响应中被返回。
全局加权轮询（gwrr）	该算法与加权轮询算法原理相同。区别在于该算法在多核 CPU 环境下也可以严格加权轮询。
IP 优先（ipo）	采用 IP 优先算法时，优先级最高的 SDNS 服务 IP 将总是在 DNS 响应中被返回。
哈希 IP（hi）	采用哈希 IP 算法时，系统会计算源 IP 地址的哈希值。对于源 IP 地址相同的 DNS 查询，系统将返回同一个 SDNS 服务 IP。
哈希 IP Port（hip）	采用哈希 IP Port 算法时，系统会计算源 IP 地址和端口的哈希值。对于源 IP 地址端口相同的 DNS 查询，系统会返回同一个 SDNS 服务 IP。
一致哈希 IP（chi）	采用一致哈希 IP 算法时，系统会计算源 IP 地址的哈希值。对于源 IP 地址相同的 DNS 查询，系统将返回同一个 SDNS 服务 IP；如果该 SDNS 服务 IP 不可用或系统增加了新的 SDNS 服务 IP，chi 算法会根据哈希值选择一个新的 SDNS 服务 IP，后续源 IP 地址相同的 DNS 查询，系统将返回同一个 SDNS 服务 IP。

会话保持 (persistence)	采用会话保持算法时，系统会将首次命中该服务组的客户端请求转发到根据“首次选择算法”选择的应用服务，并会话信息与应用服务对应关系记录下来。当后续会话信息相同的客户端请求命中该服务组时，会话保持算法将客户端请求持续地转发到同一个后台服务。
snmp	采用 snmp 算法时，SDNS 会使用 SNMP 协议从每个 SDNS 服务 IP 收集特定 OID 的数据，根据指定的 SNMP 表达式计算每个 SDNS 服务 IP 的复合权重值 (metric)，并按照指定方式排序。排序最前的 SDNS 服务 IP 将在 DNS 响应中被返回。详细信息，参见设备用户手册中“SNMP 数据收集”小节。
丢弃 (drop)	采用丢弃算法时，系统将直接丢弃 DNS 请求且不返回 DNS 响应。
带宽 (bandwidth)	采用带宽算法时，SDNS 会使用 SNMP 协议从每个 SDNS 服务 IP 收集特定 OID 的数据，获取资源带宽，根据所有 SDNS 服务 IP 的资源带宽，返回最优的 SDNS 服务 IP。
应用可用性 (status)	采用应用可用性算法时，SDNS 会使用 SNMP 协议从每个 SDNS 服务 IP 收集特定 OID 的数据，获取资源状态，根据所有 SDNS 服务 IP 的资源状态，返回最优的 SDNS 服务 IP。
拓扑 (topology)	采用拓扑算法时，SDNS 会根据拓扑算法返回最优的 SDNS 服务 IP。详细信息，参见命令“sdns pool topology”。
最短往返时间 (rtt)	采用最短往返时间算法，系统会根据配置的探测条件，探测本地 DNS 服务器到 SDNS 数据中心的往返时间，往返时间最短的 SDNS 数据中心下的 SDNS 服务 IP 将总是在 DNS 响应中被返回。
最少连接数 (lc)	采用最少连接数算法，SDNS 会使用 SNMP 协议从每个 SDNS 服务 IP 收集特定 OID 的数据，获取应用服务的连接，根据所有 SDNS 服务 IP 的连接数，选择连接数最小的应用服务返回。
保持 IP (pi)	采用保持 IP 算法，SDNS 会将首次命中该服务组的客户端请求转发到根据“首次选择算法”选择的应用服务，并将源 IP 地址的哈希值与应用服务对应关系记录下来。当后续源 IP 地址的哈希值相同的客户端请求命中该服务组时，保持 IP 算法将客户端请求持续地转发到同一个后台服务。
备用 IP (fallbackip)	当首选算法搜索不到可用 IP 时，则该次选或兜底算法会返回自定义配置的 fallback ip 给客户端。自定义 IP 通过命令“sdns pool method secondary”配置。
静态 DNS 解析 (rtd)	跳过动态 DNS 解析，直接将请求交给静态 DNS 解析。
CPU 算法 (cpu)	收集当前各个应用的 CPU 利用率指标，使用当前 CPU 利用率最小的应用服务作为 DNS 请求的回应。
最小流量 (mf)	选择当前处理流量最少的应用服务作为 DNS 请求的回应。



注意：

- 当使用加权轮询算法或者全局加权轮询算法时，如果修改了 SDNS 服务的权重值，将在原有权重完成一轮轮询后生效。
- 该命令支持配置同步、增量同步、HA 运行时配置同步、SDNS 运行时配置同步和 SDNS 配置同步。
- 该命令不支持在分区内使用。
- 使用 RTT 算法时，需要配置 DPS 相关配置和二级算法，并且 “**sdns dps detector**” 命令需配置 “dc_name” 和 “link_name” 这两个参数中的至少一个，如果都未配置，则 RTT 算法不生效。
 - 使用 “**sdns dps detector**” 命令配置 “dc_name” 后，系统会根据本地 DNS 服务器到各 SDNS 数据中心的 RTT，选择最优 RTT 对应的 SDNS 数据中心下的 SDNS 服务 IP。
 - 使用 “**sdns dps detector**” 命令配置 “dc_name” 并配置 “link_name” 后，系统会根据本地 DNS 服务器到各数据中心的 RTT，选择最优 RTT 对应的 SDNS 数据中心及 SDNS 链路下的 SDNS 服务 IP。
- 如果最优 RTT 对应 SDNS 数据中心或 SDNS 链路下无可用 SDNS 服务 IP，则会选择次优 RTT 对应 SDNS 数据中心或 SDNS 链路下的 SDNS 服务 IP。如果系统通过最优 RTT 和次优 RTT 均无法获取到 SDNS 服务 IP，则匹配失败，此时系统使用二级算法匹配。
- 当探测器探测到距离本地 DNS 服务器的最优 RTT 只有一个时，“**show sdns dps path**” 中显示带星号的条目即为最优 RTT 对应的区域；当 DPS 探测器探测到距离本地 DNS 服务器的最优 RTT 有多个时，“**show sdns dps path**” 中显示的多个最优区域中只有一个带星号。当 DPS 探测器探测到新数据时，系统会更新星号标记。

sdns pool method secondary <pool_name> <method> [expression]
[sorting_mode] [oid_name] [fallback_ip4] [fallback_ip6]

该命令用于指定当一级算法不能选出 SDNS 服务 IP 或者别名时，用于从指定的 SDNS 服务池中选择 SDNS 服务 IP 的二级算法或从指定的 SDNS 别名池中选择 SDNS 别名的二级算法。默认情况下，SDNS 服务池和 SDNS 别名池没有配置二级算法。

pool_name	该参数指定 SDNS 服务池或 SDNS 别名池的名称。
method	该参数指定 SDNS 服务池或 SDNS 别名池使用的二级算法。

对于 SDNS 服务池，参数取值必须为：

- rr: Round Robin, 轮询算法
- grr: Global Round Robin, 全局轮询算法
- wr: Weighted Round Robin, 加权轮询算法
- gwrr: Global Weighted Round Robin, 全局加权轮询算法
- ipo: IP Overflow, IP 优先算法
- hi: Hash IP, 哈希 IP 算法
- hip: Hash IP Port, 哈希 IP Port 算法
- chi: Consistent Hash IP, 一致哈希 IP 算法
- persistence: 会话保持算法
- snmp: Simple Network Management Protocol, SNMP 算法
- drop: 丢弃算法
- bandwidth: 带宽算法
- status: 应用可用性算法
- lc: Least Connections, 最少连接数
- pi: Persistent IP, 保持 IP

对于 SDNS 别名池, 参数取值必须为:

- rr: Round Robin, 轮询算法
- wr: Weighted Round Robin, 加权轮询算法
- rtd: Return to DNS, 静态 DNS 解析算法
- mf: Minimum Flow, 最小流量算法
- fallbackip: 备用 IP 算法
- cpu: CPU 算法

expression

可选, 该参数指定 snmp 算法用来计算 SDNS 服务 IP 的复合权重值的 SNMP 表达式。只有当 “method” 设置为 “snmp” 时, 该参数才可用。参数取值必须为已经通过 “**sdns snmp exp weight**” 命令配置的 SNMP 表达式名称。

sorting_mode

可选, 该参数指定 snmp 算法用来对 SDNS 服务 IP 排序的方式。只有当 “method” 设置为 “snmp” 时, 该

参数才可用。参数取值必须为：

- asc: SDNS 服务 IP 按照复合权重值由低到高排序。
- dsc: SDNS 服务 IP 按照复合权重值由高到低排序。

默认值为“asc”。

oid_name

可选，该参数指定二级算法 bandwidth 和 status 用来计算权重的 SNMP OID 名称。只有当参数“method”设置为“bandwidth”或“status”时，该参数才生效。取值必须是已经通过“sdns snmp oid”命令配置的 SNMP OID 名称。

默认值为空。

fallback_ip4

可选，该参数指定二级算法 fallbackip 时的 ipv4 的 ip 地址。默认值为空。只有当“method”设置为“fallbackip”时，该参数才可用，fallback_ip4 和 fallback_ip6 至少需要配置一个。

fallback_ip6

可选，该参数指定二级算法 fallbackip 时的 ipv6 的 ip 地址。默认值为空。只有当“method”设置为“fallbackip”时，该参数才可用，fallback_ip4 和 fallback_ip6 至少需要配置一个。



注意：

- 该命令支持配置同步、增量同步、HA 运行时配置同步、SDNS 运行时配置同步和 SDNS 配置同步。
- 该命令不支持在分区内使用。

no sdns pool method secondary <pool_name>

该命令用于删除指定 SDNS 服务池或 SDNS 别名池的二级算法。



注意：如果删除了 SDNS 服务池的二级算法“ipo”，那么 SDNS 服务池中每个 SDNS 服务的优先级都将被重置为默认值 1。

sdns pool topology <pool_name> <src_region> <dst_region> [priority]

该命令用于为指定的 SDNS 服务池配置基于拓扑算法的区域就近性规则。当收到 DNS 请求时，系统将按照最长前缀匹配方式对源区域关联的就近性规则进行匹配，如果匹配成功，返回源区域关联的目的区域的 SDNS 服务。否则，不返回 SDNS 服务。系统支持配置最多 500 条基于拓扑算法的区域就近性规则。该命令支持在分区下执行。

pool_name	该参数指定已有 SDNS 服务池的名称。
src_region	该参数指定一个已有的 SDNS 区域作为源区域。
dst_region	该参数指定一个已有的 SDNS 区域作为目的区域。
priority	可选，该参数指定基于拓扑算法的区域就近性规则的优先级，取值必须为 0 到 65,535 之间的整数，数值越大，优先级越高。 默认值为 0。

no sdns pool topology <pool_name> <src_region> <dst_region>

该命令用于删除指定的 SDNS 服务池基于拓扑算法的区域就近性规则的配置。该命令支持在分区下执行。

show sdns pool topology [pool_name]

该命令用于显示指定的 SDNS 服务池基于拓扑算法的区域就近性规则的配置。如果不指定参数“pool_name”的值，将显示所有 SDNS 服务池基于拓扑算法的区域就近性规则。该命令支持在分区下执行。

clear sdns pool topology [pool_name]

该命令用于删除指定的 SDNS 服务池基于拓扑算法的区域就近性规则的配置。如果不指定参数“pool_name”的值，将删除所有 SDNS 服务池基于拓扑算法的区域就近性规则的配置。该命令支持在分区下执行。

show sdns pool proximity match <pool_name> <source_ip> [query_type]

该命令用于为指定 SDNS 服务池显示特定 DNS 查询命中的基于拓扑算法的区域就近性规则。

pool_name	该参数指定已有 SDNS 服务池的名称。
source_ip	该参数指定 DNS 查询的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。
query_type	可选，该参数指定 DNS 查询的资源记录类型，取值必须为“A”或“AAAA”。默认值为“A”。

sdns pool member weight <pool_name> <service_name|cname> [weight]

该命令用于为指定的使用 wrr 算法或 gwrr 算法的 SDNS 服务池的 SDNS 服务或 SDNS 别名池的别名设置权重值。

pool_name	该参数指定已有 SDNS 服务池或 SDNS 别名池的名称。
service_name cname	该参数指定已有 SDNS 服务的名称或已有 SDNS 别名。

weight 可选，该参数指定 SDNS 服务的权重值。取值必须为 1 到 4,294,967,295 之间的整数。默认值为 1。



注意：

- 当管理员删除 SDNS 服务池中的指定 SDNS 服务后，该 SDNS 服务池将重新从第一个 SDNS 服务开始使用 wrr 或 gwrr 算法进行轮询。
- 该命令支持配置同步、增量同步、HA 运行时配置同步、SDNS 运行时配置同步和 SDNS 配置同步。
- 该命令不支持在分区内使用。

clear sdns pool member weight <pool_name>

该命令用于将指定的使用 wrr 算法或 gwrr 算法的 SDNS 服务池中全部 SDNS 服务或 SDNS 别名池中全部 SDNS 别名的权重值重置为默认值 1。

sdns pool member priority <pool_name> <service_name> [priority]

该命令用于为指定的使用 ipo 算法的 SDNS 服务池的 SDNS 服务设置优先级。

pool_name 该参数指定 SDNS 服务池的名称。

service_name 该参数指定 SDNS 服务的名称。

priority 可选，该参数指定 SDNS 服务的优先级。取值必须为 1 到 4,294,967,295 之间的整数。参数值越大，优先级越高。默认值为 1。

clear sdns pool member priority <pool_name>

该命令用于将指定的使用 ipo 算法的 SDNS 服务池的全部 SDNS 服务的优先级重置为默认值 1。

sdns pool failover <pool_name> [on|off]

该命令用于为指定的使用 ipo 算法的 SDNS 服务池启用或禁用自动失效切换功能。

启用该功能后，在最高优先级的 SDNS 服务不可用时，系统将自动将当前选择的 SDNS 服务切换到次优先级的 SDNS 服务。默认情况下，每个使用 ipo 算法的 SDNS 服务池的自动失效切换功能都是启用的。

pool_name 该参数指定 SDNS 服务池的名称。

on|off 可选，该参数用于启用或禁用自动失效切换功能。默认值为 “on”。

sdns pool preempt <pool_name> [on|off]

该命令用于为指定的使用 ipo 算法的 SDNS 服务池启用或禁用抢占功能。

该功能启用后,当最高优先级的 SDNS 服务恢复时,系统自动将当前选择的 SDNS 服务切回到最高优先级的 SDNS 服务。默认情况下,每个使用 ipo 算法的 SDNS 服务池的抢占功能都是启用的。

pool_name 该参数指定 SDNS 服务池的名称。

on|off 可选,该参数用于启用或禁用抢占功能。默认值为“on”。

sdns pool ipo reset <pool_name> [priority]

该命令用于手动将当前选择的 SDNS 服务切换到同一 SDNS 服务池中具有指定优先级的 SDNS 服务。执行该命令后,SDNS 服务将被手动切换,但是该操作不能作为配置被保存,在系统重启后失效。

pool_name 该参数指定 SDNS 服务池的名称。

priority 可选,该参数指定 SDNS 服务的优先级。取值必须为 0 到 4,294,967,295 之间的整数。参数值越大,优先级越高。默认值为 0,表示 SDNS 服务池中的最高优先级。



注意: 当自动失效切换功能和抢占功能同时启用时,手动切换将失效。

sdns snmp oid <oid_name> <snmp_oid>

该命令用于定义一个 SNMP OID。系统允许定义最多八个 SNMP OID。

oid_name 该参数指定 SNMP OID 的名称。取值必须为长度不大于 20 个字节的字符串。当参数取值只包含数字时,必须置于双引号内。

snmp_oid 该参数指定 SNMP OID。取值必须为长度是 2 到 895 个字节的字符串。

no sdns snmp oid <oid_name>

该命令用于删除一个已定义的 SNMP OID。

show sdns snmp oid

该命令用于显示所有已定义的 SNMP OID。

clear sdns snmp oid

该命令用于清除所有已定义的 SNMP OID。

show sdns snmp localoid

该命令用于显示系统支持的本地 SNMP OID。

```
Demo(config)#show sdns snmp localoid
Oid Name          Oid
CPU usage         .1.3.6.1.4.1.7564.30.1.0
Memory usage      .1.3.6.1.4.1.7564.4.2.0
New connections   .1.3.6.1.4.1.7564.30.2.0
```

sdns snmp exp weight <expression> <oid1_name> [oid1_weight]
[oid2_name] [oid2_weight] [oid3_name] [oid3_weight]

该命令用于配置用来计算 SDNS 服务 IP 的复合权重值的 SNMP 表达式。每个 SNMP 表达式最少使用一个 SNMP OID 的数据，最多使用三个 SNMP OID 的数据。SNMP 表达式的格式为：

OID1 数据 × OID1 权重 + OID2 数据 × OID2 权重 + OID3 数据 × OID3 权重
expression 该参数指定 SNMP 算法用来计算 SDNS 服务 IP 的复合权重值的表达式的名称。取值必须为长度不大于 20 个字节的字符串。当参数取值只包含数字时，必须置于双引号内。

oid1_name 该参数指定第一个 SNMP OID 的名称。

oid1_weight 可选，该参数指定第一个 SNMP OID 的权重值。取值必须为 0 到 65,535 之间的整数。默认值为 1。

oid2_name 可选，该参数指定第二个 SNMP OID 的名称。

oid2_weight 可选，该参数指定第二个 SNMP OID 的权重值。取值必须为 0 到 65,535 之间的整数。默认值为 1。

oid3_name 可选，该参数指定第三个 SNMP OID 的名称。

oid3_weight 可选，该参数指定第三个 SNMP OID 的权重值。取值必须为 0 到 65,535 之间的整数。默认值为 1。



注意：当某 SDNS 服务池使用配置的 SNMP 表达式时，必须为该表达式中的每个 SNMP OID 配置 SNMP 数据收集模板，并将模板关联到该 SDNS 服务池。

no sdns snmp exp weight <expression>

该命令用于删除指定的 SNMP 表达式。

show sdns snmp exp weight [expression]

该命令用于显示指定的 SNMP 表达式。如果不指定参数“expression”，将显示所有的 SNMP 表达式。

clear sdns snmp exp weight

该命令用于清除所有的 SNMP 表达式。

sdns pool cname <pool_name> <cname>

该命令用于定义一个 SDNS 别名 (Canonical Name, CNAME) 池。SDNS 别名池可以包含最多 200 个别名。当系统收到 CNAME 类型的 DNS 解析请求并且该别名池被命中时，系统将该别名返回给本地 DNS 服务器。当收到 A 或 AAAA 类型的 DNS 解析请求时，系统将进一步将别名解析为 IPv4 或 IPv6 地址。

pool_name 该参数指定 SDNS 服务池的名称，取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

cname 该参数指定一个 CNAME。取值必须为长度不大于 128 个字节的字符串，格式为 www.xyz.com。该字符串中由“.”分隔的各部分长度不能超过 63 个字符。该参数的取值不支持通配符“*”和其他特殊字符，并且不能以“.”结尾。



注意：当待查询的 SDNS 域名关联的服务池是 SDNS 别名池，会根据 SDNS 别名池关联的 CNAME 的取值重新进行 SDNS 查询，最终查询结果只与 CNAME 关联的策略有关。

no sdns pool cname <pool_name>

该命令用于删除一个指定 SDNS 别名池中的指定别名。

show sdns pool cname

该命令用于显示全部 SDNS 别名池。

clear sdns pool cname <pool_name>

该命令用于清除指定 SDNS 别名池。如果指定参数“pool_name”取值为“all”，则清除所有的 SDNS 别名池。

sdns pool resort service <pool_name> <service_name>

该命令用于向指定的 SDNS 应急池添加一个 SDNS 服务。一个 SDNS 服务可以被加入到多个 SDNS 应急池中，一个 SDNS 应急池支持同时添加最多 100 个 SDNS 服务 IP 为 IPv4 的 SDNS 服务，和最多 100 个 SDNS 服务 IP 为 IPv6 的 SDNS 服务。

pool_name 该参数指定一个 SDNS 应急池的名称。取值为通过命令“sdns pool name”定义 SDNS 服务池时同时自动生成的同名的 SDNS 应急池的名称。

`service_name` 该参数指定已有 SDNS 服务的名称。



注意：SDNS 应急池只能通过 SDNS 应急策略与 SDNS 域名关联。

no sdns pool resort service *<pool_name> <service_name>*

该命令用于删除指定 SDNS 应急池中的 SDNS 应急服务。

show sdns pool resort service *[pool_name]*

该命令用于显示指定 SDNS 应急池的所有 SDNS 服务。如果不指定参数“pool_name”，将显示所有 SDNS 应急池的 SDNS 服务。

clear sdns pool resort service *<pool_name>*

该命令用于清除指定的 SDNS 应急池中的全部 SDNS 服务。

sdns pool fallback *<pool_name> <fallback_pool_name>*

该命令用于为指定的 SDNS 服务池配置一个 SDNS 回退池。当指定的 SDNS 服务池中沒有可用的 SDNS 服务时，系统将采用 SDNS 回退池。

`pool_name` 该参数指定 SDNS 服务池的名称。

`fallback_pool_name` 该参数指定 SDNS 回退池的名称。取值可以是一个 SDNS 服务或别名池的名称。



注意：系统允许多个 SDNS 服务池构成一个树形的回退结构。但是不允许存在环回。

no sdns pool fallback *<pool_name>*

该命令用于删除为指定的 SDNS 服务池配置的 SDNS 回退池。

show sdns pool fallback

该命令用于显示全部 SDNS 回退池。

clear sdns pool fallback

该命令用于清除全部 SDNS 回退池。

show sdns pool status *[pool_name]*

该命令用于显示指定的 SDNS 服务真实状态以及状态的原因或别名池的状态。如果不指定参数“pool_name”的值，则将显示全部 SDNS 服务真实状态以及状态的原因和别名池的状态。

当 SDNS 服务关联 SDNS 链路时，只有 SDNS 服务池、SDNS 服务与 SDNS 链路的健康检查都为 UP 状态并且都为 ENABLE 状态，通过该命令显示 SDNS 服务

的状态才会显示为 UP；当 SDNS 服务池健康检查状态为 DOWN 或者 SDNS 服务或者 SDNS 链路健康检查为 DOWN 或者为 DISABLE 状态，则通过该命令显示的 SDNS 服务的状态为 DOWN。当 SDNS 服务未关联 SDNS 链路时，将只显示 SDNS 服务池的健康检查状态以及 SDNS 服务的健康检查状态与启用状态。

SDNS 服务有以下几种状态：SERVICE_UP、SERVICE_DOWN、SERVICE_DISABLE；

SDNS 链路有以下几种状态：LINK_UP、LINK_DOWN、LINK_DISABLE；

SDNS 服务池有以下几种状态：POOL_UP、POOL_DOWN。

当服务池中既包含 SDNS 服务 IP 为 IPv4 的 SDNS 服务又包含 SDNS 服务 IP 为 IPv6 的 SDNS 服务，执行该命令将分别显示不同类型 SDNS 服务的状态。

例如：

```
Demo#show sdns pool status
p1 ipo none HITS:0
    A Record: Available
    1.1.1.1 UP(POOL_UP,SERVICE_UP,LINK_UP) 0
    1.1.1.2 DOWN(POOL_DOWN,SERVICE_UP,LINK_UP) 0
    1.1.1.3
DOWN(POOL_UP,SERVICE_UP,SERVICE_DISABLE,LINK_UP,LINK_DISABLE) 0
    1.1.1.4 DOWN(POOL_DOWN,SERVICE_UP) 0
    AAAA Record: Not Available
    11::1
DOWN(POOL_DOWN,SERVICE_DOWN,SERVICE_DISABLE,LINK_UP,LINK_DISABLE) 0
    11::2
DOWN(POOL_UP,SERVICE_UP,SERVICE_DISABLE,LINK_UP,LINK_DISABLE) 0
```

sdns pool mx <pool_name> <host_name> <priority> [weight]

该命令用于为指定的 SDNS 服务池添加一条 MX 资源记录，用于动态域名解析。系统支持向同一个 SDNS 服务池中添加最多 100 个 MX 资源记录。

pool_name	该参数指定已存在的 SDNS 服务池的名称。
host_name	该参数指定已存在的 SDNS 域名。
priority	该参数指定 MX 资源记录的优先级，取值必须为 0 至 65,535 之间的整数，数字越小，优先级越高。
weight	可选，该参数指定 SDNS 服务池中 MX 资源记录的权重值。取值必须为 1 到 4,294,967,295 之间的整数。默认值为 1。



注意：

- 仅当 SDNS 服务池算法为 RR 或 WRR 时，系统支持使用 MX 资源记录。系统支持为一个 MX 类型请求可返回多个 MX 资源记录。若为 SDNS 服务池配置了除 RR 或 WRR 之外的其他算法，对于 MX 类型请求，SDNS 服务池仍使用 RR 算法来选择 MX 资源记录。
- 该功能支持在分区模式下配置，并且支持配置同步。
- 该功能支持配置同步、增量同步、HA 启动时配置同步、HA 运行时配置同步、SDNS 运行时配置同步、SDNS 配置同步。

no sdns pool mx <pool_name> <host_name>

该命令用于删除指定的 SDNS 服务池中指定的 MX 资源记录。

show sdns pool mx [pool_name]

该命令用于显示指定的 SDNS 服务池中包含的 MX 资源记录。如果不指定参数“pool_name”，将显示所有 SDNS 服务池中包含的 MX 资源记录。

clear sdns pool mx <pool_name>

该命令用于清除指定的 SDNS 服务池中包含的所有 MX 资源记录。

13.6 SDNS 区域

sdns region name <region_name>

该命令用于定义一个 SDNS 区域。系统支持最多 100 个 SDNS 区域。

region_name 该参数指定 SDNS 区域的名称。取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

no sdns region name <region_name>

该命令用于删除一个指定的 SDNS 区域。

执行该命令前，请先启用 SDNS 功能（通过命令“**sdns on**”）。

show sdns region name

该命令用于显示全部 SDNS 区域。

clear sdns region name

该命令用于清除全部 SDNS 区域。

执行该命令前，请先启用 SDNS 功能（通过命令“**sdns on**”）。

sdns region proximity <region1> <region2> [relation]

该命令用于将指定源 SDNS 区域的静态 SDNS 区域就近性规则关联到目的 SDNS 区域。执行该命令后，参数“region1”对应的所有静态 SDNS 区域就近性规则也将关联到“region2”对应的 SDNS 区域。需要注意的是，该命令只支持关联就近性规则匹配关系相同（同为“is”或“not”关系）的 SDNS 区域。

region1	该参数指定一个源 SDNS 区域名称。
region2	该参数指定一个目的 SDNS 区域名称。
relation	可选，该参数指定就近性规则匹配关系。取值必须和指定的源 SDNS 区域以及指定的目的 SDNS 区域的就近性规则匹配关系一致。取值必须为“is”或“not”。默认值为“is”。

no sdns region proximity <region1> <region2> [relation]

该命令用于删除指定源区域的 SDNS 区域就近性规则和指定目的区域的关联关系。

show sdns region proximity

该命令用于显示所有源区域的 SDNS 区域就近性规则和目的区域的关联关系。

clear sdns region proximity

该命令用于清除所有源区域的 SDNS 区域就近性规则和目的区域的关联关系。

13.7 SDNS 策略

sdns policy method <host_name> <policy_type>

该命令用于为指定的域名配置策略类型。系统支持为一个域名配置一条策略。

host_name	该参数指定一个已有的 SDNS 域名。
policy_type	该参数指定策略类型。取值必须为： • rr: Round Robin，轮询策略。 • wr: Weighted Round Robin，加权轮询策略。 • ga: Global Availability，全局可用性策略。 • region: 区域策略。

no sdns policy method <host_name>

该命令用于删除指定域名的 SDNS 策略类型。

show sdns policy method [host_name]

该命令用于显示指定域名的 SDNS 策略类型。如果不指定参数 “host_name”，则显示所有域名的 SDNS 策略类型。

clear sdns policy method

该命令用于清除所有域名的 SDNS 策略类型。

sdns policy member <policy_name> <host_name> <pool_name> [weight/priority] [region_name]

该命令用于为指定域名配置 SDNS 服务池。

policy_name	该参数指定域名策略的名称。取值必须为长度不大于 40 个字节的字符串。 注意： 参数取值不能为 “all”。
host_name	该参数指定一个已有的 SDNS 域名。
pool_name	该参数指定一个已有的 SDNS 服务池。取值可以是一个 SDNS 服务池或别名池的名称。
weight/priority	可选，该参数指定 SDNS 服务池的权重值或者优先级。取值必须为 0 到 65,535 之间的整数。 默认值为 0。
region_name	可选，该参数指定一个 SDNS 区域。仅当参数 “host_name” 所对应的 SDNS 策略为区域策略（通过命令 “sdns policy method” 配置）时，该参数生效。



注意：

- 如果指定 SDNS 域名的 DNS 解析请求匹配多条 SDNS 区域策略，系统仅采用优先级最高的 SDNS 区域策略。
- 同一个 SDNS 域名的多条 SDNS 区域策略的优先级不应相同。

no sdns policy member <policy_name>

该命令用于删除指定域名配置的 SDNS 服务池。

show sdns policy member [host_name]

该命令用于显示指定域名配置的 SDNS 服务池。如果不指定参数 “host_name”，则显示所有域名的 SDNS 服务池。

clear sdns policy member [host_name]

该命令用于清除指定域名的 SDNS 服务池。如果不指定参数 “host_name”，则清除所有域名的 SDNS 服务池。

sdns policy default <host_name> <pool_name>

该命令用于定义一条 SDNS 默认策略。对于每个 SDNS 域名, 仅能配置一条 SDNS 默认策略。

指定的 SDNS 域名的 SDNS 默认策略将在下列任一条件下生效:

- 该 SDNS 域名没有配置任何 SDNS 区域策略, 或没有 SDNS 区域策略被匹配。
- 系统采用优先级最高的 SDNS 区域策略无法为指定的 SDNS 域名选择出可用的 SDNS 服务。

host_name 该参数指定一个已有的 SDNS 域名。

pool_name 该参数指定一个已有的 SDNS 服务池。取值可以是一个 SDNS 服务池或别名池的名称。

no sdns policy default <host_name>

该命令用于删除指定的 SDNS 默认策略。

show sdns policy default

该命令用于显示全部 SDNS 默认策略。

clear sdns policy default

该命令用于清除全部 SDNS 默认策略。

sdns policy resort <host_name> <pool_name>

该命令用于定义一条 SDNS 应急策略, 用于在未命中到区域策略和默认策略时返回关联的应急池中的服务 IP。对于每个 SDNS 域名, 仅能配置一条 SDNS 应急策略。

指定的 SDNS 域名的 SDNS 应急策略将在下面任一条件下生效:

- 管理员没有为该 SDNS 域名配置任何 SDNS 区域策略和默认策略, 或系统未能命中配置的 SDNS 区域策略和默认策略。
- 系统采用优先级最高的 SDNS 区域策略无法为指定的 SDNS 域名选择出可用的 SDNS 服务, 并且系统采用默认策略也无法为指定的 SDNS 域名选择出可用的 SDNS 服务。

需要注意的是当命中 SDNS 应急策略后, 无论关联的应急池中的服务 IP 健康状况如何, 系统都会将该服务 IP 返回。如果仍未能匹配到服务 IP, 系统将从 SDNS 回退池中查找服务 IP。如果系统从回退池也未能匹配到服务 IP, 系统将返回空 DNS 响应。

该命令还可以用于修改已有 SDNS 应急策略的配置。

host_name 该参数指定一个已有的 SDNS 域名。

pool_name 该参数指定一个已有的 SDNS 应急池。取值可以是一个 SDNS 应急池或别名池的名称。



注意：为 SDNS 应急策略关联的应急池默认只能使用全局轮询算法。

no sdns policy resort <host_name>

该命令用于删除指定的 SDNS 应急策略。

show sdns policy resort

该命令用于显示全部 SDNS 应急策略。

clear sdns policy resort

该命令用于清除全部 SDNS 应急策略。

13.8 SDNS Monitor

SDNS monitor 可以用于对 SDNS 服务进行健康检查或者向 SDNS 服务收集 SNMP 数据。要使用 SDNS monitor，管理员必须先定义健康检查模板或数据收集模板，然后将模板与一个 SDNS 服务或 SDNS 服务池关联起来生成 monitor 实例。系统将根据 monitor 实例执行健康检查或者数据收集。

SDNS 支持 ICMP、TCP、UDP、HTTP 和 HTTPS 类型的健康检查模板以及 SNMP 类型的数据收集模板。系统支持最多 1000 个健康检查和数据收集模板。健康检查模板支持 IPv4 和 IPv6 类型。

当模板与一个 SDNS 服务关联起来后，系统将生成一个 monitor 实例；当模板与一个 SDNS 服务池关联起来后，系统将为该服务池中的每个 SDNS 服务生成一个 monitor 实例。基于健康检查模板生成的 monitor 实例称为健康检查实例，基于 SNMP 数据收集模板生成的 monitor 实例称为 SNMP 数据收集实例。系统支持最多 25,000 个 monitor 实例，最多 1024 个 SNMP 数据收集实例。

sdns monitor icmp <template_name> [interval] [timeout] [max_retries] [dst_address] [src_address] [gateway_address] [failure_delay] [probe_timeout]

该命令用于定义一个 ICMP 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

interval 可选，该参数指定健康检查的时间间隔。取值必须为 3

	到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。 超时时间必须小于等于健康检查的时间间隔。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 ICMP 健康检查报文的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
src_address	可选，该参数指定 ICMP 健康检查报文的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数的值，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 ICMP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 ICMP 响应报文，建议配置参数“src_address”和“gateway_address”。
fail_delay	可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为“Down”的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。 默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为“Down”。
prober_timeout	可选，该参数指定健康检查探测的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。取值必须小于参数“timeout”。 默认值为 3。

```
sdns monitor tcp <template_name> [interval] [timeout] [max_retries]  
[dst_address] [dst_port] [src_address] [gateway_address] [fail_delay]  
[prober_timeout]
```

该命令用于定义一个 TCP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为 “all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 TCP 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 TCP 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 TCP 健康检查报文的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 TCP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数 “src_address” 和 “gateway_address”。

fail_delay 可选，该参数指定健康检查的失败延时时间。取值必须是 0 到 86,400 之间的整数，单位为秒。

默认值为 0，表示不延时。

fail_delay 可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为“Down”的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。

默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为“Down”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“sdns service ip”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor udp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [gateway_address] [fail_delay]
[prober_timeout]

该命令用于定义一个 UDP 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

interval 可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

timeout 可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

max_retries 可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。

当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address 可选，该参数指定 UDP 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。

dst_port	可选，该参数指定 UDP 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 UDP 健康检查报文的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 UDP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 UDP 响应报文，建议配置参数“src_address”和“gateway_address”。
fail_delay	可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为“Down”的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。 默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为“Down”。
prober_timeout	可选，该参数指定健康检查探测的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。取值必须小于参数“timeout”。 默认值为 3。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor http <template_name> [request_line] [expected_response]
[flag] [interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address] [fail_delay] [prober_timeout]

该命令用于定义一个 HTTP 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

request_line	可选, 该参数指定 HTTP 请求的请求行, 内容包括 HTTP 请求方法、URL 路径和 HTTP 协议版本。参数取值必须置于双引号内。默认值为 “HEAD / HTTP/1.0\r\n\r\n”。
expected_response	可选, 该参数指定期望的 HTTP 响应。参数取值必须置于双引号内。默认值为 “200 OK”。
flag	可选, 该参数指定 SDNS 服务返回响应包含期望的 HTTP 状态码时的健康检查的结果。取值必须为: • up: 表示标识 SDNS 服务为 Up。 • down: 表示标识 SDNS 服务为 Down。 默认值为 up。
interval	可选, 该参数指定健康检查的时间间隔, 单位为秒。取值必须为 3 到 86,400 之间的整数。默认值为 5。
timeout	可选, 该参数指定健康检查的超时时间, 单位为秒。取值必须为 3 到 86,400 之间的整数。健康检查超时时间必须小于等于健康检查的时间间隔。默认值为 5。
max_retries	可选, 该参数指定判定 SDNS 服务状态所需的健康检查结果连续为 Up 或 Down 的次数。取值必须为 1 到 10 之间的整数。参数取值为 3 时, 系统在连续 3 次健康检查结果都是 Up 时才将 SDNS 服务状态判定为 Up, 或者在连续 3 次健康检查结果为 Down 时将 SDNS 服务的状态判定为 Down。默认值为 3。
dst_address	可选, 该参数指定 HTTP 请求的目的 IP 地址。如果不指定该参数, 则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选, 该参数指定 HTTP 请求的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选, 该参数指定 HTTP 请求的源 IP 地址。取值建议配置系统管理 IP 地址, 包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址, 会导致健康检查失败。如果不指定该参数, 则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选, 该参数指定发送 HTTP 请求的网关的 IP 地址。如果不指定该参数, 则系统将自动选择网关 IP 地址。选在多链路环境中, 为了确保设备可以正确接收 HTTP 响应报文, 建议设置参数 “src_address” 和

“gateway_address”。

fail_delay 可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为 “Down” 的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。

默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为 “Down”。

prober_timeout 可选，该参数指定健康检查探测的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。取值必须小于参数 “timeout”。

默认值为 3。



注意：如果本命令中的参数 “dst_port” 的值是 0，系统将使用在命令 “sdns service ip” 中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数 “dst_port” 的值作为报文的目的端口。

sdns monitor https <template_name> [request_line] [expected_response] [flag] [interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address] [gateway_address] [fail_delay] [prober_timeout]

该命令用于定义一个 HTTPS 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为 “all”。

request_line 可选，该参数指定 HTTP 请求的请求行，内容包括 HTTP 请求方法、URL 路径和 HTTP 协议版本。参数取值必须置于双引号内。默认值为 “HEAD / HTTP/1.0\r\n\r\n”。

expected_response 可选，该参数指定期望的 HTTP 响应。参数取值必须置于双引号内。默认值为 “200 OK”。

flag 可选，该参数指定 SDNS 服务返回响应包含期望的 HTTP 状态码时的健康检查的结果。取值必须为：

- up: 表示标识 SDNS 服务为 Up。
- down: 表示标识 SDNS 服务为 Down。

默认值为 up。

interval 可选，该参数指定健康检查的时间间隔，单位为秒。取

	值必须为 3 到 86,400 之间的整数。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间，单位为秒。取值必须为 3 到 86,400 之间的整数。健康检查超时时间必须小于等于健康检查的时间间隔。默认值为 5。
max_retries	可选，该参数指定判定 SDNS 服务状态所需的健康检查结果连续为 Up 或 Down 的次数。取值必须为 1 到 10 之间的整数。参数取值为 3 时，系统在连续 3 次健康检查结果都是 Up 时才将 SDNS 服务状态判定为 Up，或者在连续 3 次健康检查结果为 Down 时才将 SDNS 服务的状态判定为 Down。默认值为 3。
dst_address	可选，该参数指定 HTTP 请求的目的 IP 地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 HTTP 请求的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 HTTP 请求的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 HTTP 请求的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。选在多链路环境中，为了确保设备可以正确接收 HTTPS 响应报文，建议设置参数“src_address”和“gateway_address”。
fail_delay	可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为“Down”的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。 默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为“Down”。
prober_timeout	可选，该参数指定健康检查探测的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。取值必须小于参数“timeout”。 默认值为 3。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“sdns service ip”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor dns <template_name> [request_line] [expected_response]
[interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address]

该命令用于定义一个 DNS 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不大于 128 个字节的字符串。

request_line 可选，该参数指定 DNS 类型健康检查请求的内容。可指定多个关键词，关键词之间用逗号分隔。健康检查请求与输入的关键词顺序无关。

参数格式为“关键词 1=xxx, 关键词 2=xxx, ...”，长度不超过 512 字节。例如“host=array.com, type=a”。系统支持的关键词包括：

- host: 表示请求的域名。
- type: 表示请求类型。

type 的值支持 a 和 aaaa，或 1~65535 之间的数字。当 request_line 参数不为空时，必须输入 host 关键词，可以不输入 type 关键词。type 默认值为 a。不支持输入多个 host 或 type。以上关键词及其取值都不区分大小写。

expected_response 可选，该参数指定 DNS 类型健康检查响应的内容。可指定多个关键词，关键词之间用逗号分隔。健康检查响应与输入的关键词顺序无关。

参数格式为“关键词 1=xxx, 关键词 2=xxx, ...”，长度不超过 512 字节。例如

“a=1.1.1.1,a=2.2.2.2,aaaa=1::1,rcode=0”。如果健康检查的响应报文包含任意一项资源，且响应报文中的 rcode 与指定 rcode 相同，则认为健康检查成功。

系统支持的关键词包括：

- a: 表示 A 记录。
- aaaa: 表示 AAAA 记录。
- rcode: 表示 DNS 响应中的响应码。

支持最多输入 3 个 A 记录和 3 个 AAAA 记录。rcode 的

取值必须为 0 至 15 之间的整数。不支持输入多个 rcode。
以上关键词及其取值都不区分大小写。

interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 DNS 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 DNS 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 53。
src_address	可选，该参数指定 DNS 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 DNS 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保 APV 设备可以正确接收 DNS 响应报文，建议配置参数“src_address”和“gateway_addres”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“sdns service ip”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor dnstcp <template_name> [request_line] [expected_response]
[interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address]

该命令用于定义一个 DNS-TCP 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不大于 128 个字节的字符串。

request_line	可选，该参数指定 DNS 类型健康检查请求的内容。可指定多个关键词，关键词之间用逗号分隔。健康检查请求与输入的关键词顺序无关。 参数格式为“关键词 1=xxx, 关键词 2=xxx, ...”，长度不超过 512 字节。例如“host=array.com, type=a”。系统支持的关键词包括： • host: 表示请求的域名。 • type: 表示请求类型。 type 的值支持 a 和 aaaa，或 1~65535 之间的数字。当 request_line 参数不为空时，必须输入 host 关键词，可以不输入 type 关键词。type 默认值为 a。不支持输入多个 host 或 type。以上关键词及其取值都不区分大小写。
expected_response	可选，该参数指定 DNS 类型健康检查响应的内容。可指定多个关键词，关键词之间用逗号分隔。健康检查响应与输入的关键词顺序无关。 参数格式为“关键词 1=xxx, 关键词 2=xxx, ...”，长度不超过 512 字节。例如 “a=1.1.1.1,a=2.2.2.2,aaaa=1::1,rcode=0”。如果健康检查的响应报文包含任意一项资源，且响应报文中的 rcode 与指定 rcode 相同，则认为健康检查成功。 系统支持的关键词包括： • a: 表示 A 记录。 • aaaa: 表示 AAAA 记录。 • rcode: 表示 DNS 响应中的响应码。 支持最多输入 3 个 A 记录和 3 个 AAAA 记录。rcode 的取值必须为 0 至 15 之间的整数。不支持输入多个 rcode。以上关键词及其取值都不区分大小写。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置

为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address	可选，该参数指定健康检查报文的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的端口。取值必须为 0 到 65,535 之间的整数。默认值为 53。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保 APV 设备可以正确接收 DNS 响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“sdns service ip”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor ntp*<template_name> <auth_id> <type> <key> [interval] [timeout] [max_retries]*

该命令用于定义一个 NTP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
auth_id	该参数指定身份验证的密钥序号。取值必须为 1 至 65535 之间的整数。
type	该参数指定用于生成身份验证数据摘要的算法。取值必须为：MD5、SHA1、SHA224、SHA256、SHA384、SHA512、MDC2 或 RIPEMD160。
key	该参数指定用于验证客户端身份的密钥。取值必须为长度不大于 64 个字节的字符串。如果长度为 1 至 20 个字节，该参数取值为 ASCII 字符串；如果长度为 21

至 64 字节，该参数取值为十六进制字符串。当该参数取值中包含双引号时，该参数必须使用十六进制格式输入。

interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

health pop3 <template_name> <username> <password> [request] [response] [rows] [cols] [interval] [timeout] [max_retries]

该命令用于定义一个 POP3 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
username	该参数指定登录 POP3 服务器的用户名。取值必须为长度不大于 128 个字节的字符串，必须置于双引号内。
password	该参数指定登录 POP3 服务器的密码。取值必须为长度不大于 128 个字节的字符串，必须置于双引号内。 注意： 使用知名邮箱服务器时，该参数值一般不是邮箱密码，而是开启 POP3 时服务器生成的授权码。
request	该参数指定健康检查请求的内容。取值必须为最大长度为 895 个字节的字符串。当参数取值包含数字或者空格，必须置于双引号内。
response	该参数指定预期的健康检查响应的内容。取值必须为最大长度为 895 个字节的字符串。当参数取值包含数字或者空格，必须置于双引号内。

rows	可选，该参数指定“response”参数值所在的行。取值必须为 1 至 128 之间的整数，默认值为 1。
cols	可选，该参数指定“response”参数值所在的列。取值必须为 1 至 128 之间的整数，默认值为 1。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

sdns monitor halftcp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [src_port] [gateway_address]

该命令用于定义一个 Half-TCP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address	可选, 该参数指定 Half-TCP 健康检查报文的目的地址。如果不指定该参数, 则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选, 该参数指定 Half-TCP 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选, 该参数指定 Half-TCP 健康检查报文的源 IP 地址。如果不指定该参数, 则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
src_port	可选, 该参数指定 Half-TCP 健康检查报文的源端口。如果不指定该参数, 则系统将自动选择源端口。
gateway_address	可选, 该参数指定发送 Half-TCP 健康检查报文的网关的 IP 地址。如果不指定该参数, 则系统将自动选择网关 IP 地址。



注意: 如果本命令中的参数“dst_port”的值是 0, 系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时, 将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor http2 <template_name> [request_line] [expected_response]
[flag] [interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address]

该命令用于定义一个 HTTP2 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串, 支持字母、数字、特殊字符, 名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意: 参数取值不能为“all”。
request_line	可选, 该参数指定 HTTP2 请求的请求行, 内容包括 HTTP2 请求方法、URL 路径和 HTTP2 协议版本。参数取值必须置于双引号内。默认值为“HEAD / HTTP/2 \r\n\r\n”。
expected_response	可选, 该参数指定期望的 HTTP2 响应。参数取值必须置于双引号内。默认值为“200 OK”。

flag	可选，该参数指定 SDNS 服务返回响应包含期望的 HTTP2 状态码时的健康检查的结果。取值必须为： up: 表示标识 SDNS 服务为 Up。 down: 表示标识 SDNS 服务为 Down。 默认值为 up。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 HTTP2 健康检查报文的目的地地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 HTTP2 健康检查报文的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 HTTP2 请求的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 HTTP2 请求的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”

的值作为报文的目的端口。

```
sdns monitor https2 <template_name> [request_line] [expected_response]  
[flag] [interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]  
[gateway_address]
```

该命令用于定义一个 HTTPS2 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

request_line 可选，该参数指定 HTTP 请求的请求行，内容包括 HTTP 请求方法、URL 路径和 HTTP 协议版本。参数取值必须置于双引号内。默认值为“HEAD / HTTP/2 \r\n\r\n”。

expected_response 可选，该参数指定期望的 HTTP 响应。参数取值必须置于双引号内。默认值为“200 OK”。

flag 可选，该参数指定 SDNS 服务返回响应包含期望的 HTTP 状态码时的健康检查的结果。取值必须为：

- up: 表示标识 SDNS 服务为 Up。
- down: 表示标识 SDNS 服务为 Down。

默认值为 up。

interval 可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

timeout 可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

max_retries 可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。

当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address 可选，该参数指定 HTTP2 健康检查报文的目的地址。

如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。

dst_port	可选，该参数指定 HTTP2 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 HTTP 请求的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 HTTP2 请求的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor mysql <template_name> <database_name> <username>
<password> [sql_statement] [expected_result] [rows] [cols] [interval] [timeout]
[max_retries] [dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Mysql 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
database_name	该参数指定 Mysql 数据库服务器的名称，取值必须为不大于 128 字节的字符串。
username	该参数指定登录 Mysql 数据库服务器的用户名称，取值必须为不大于 128 字节的字符串。
password	该参数指定登录 Mysql 数据库服务器的用户密码，取值必须为不大于 128 字节的字符串。当参数取值只包含数字或者包含特殊字符时，必须置于双引号内。
sql_statement	可选，该参数指定健康检查使用的 SQL 语句。取值必

须为置于双引号内的长度不超过 128 个字节的字符串。
仅支持 SELECT 语句。

例如: “select name from student where grade > 8 and age < 16”。

如果不指定该参数, 设备则仅尝试与后台数据库服务器建立连接。默认值为空。

expected_result

可选, 该参数指定执行 SQL 语句后期望返回的结果。
取值必须为长度不大于 128 个字节的字符串。设备检查后台 Mysql 数据库返回的响应值时, 采取部分匹配且不区分大小写。

例如: 参数 “expected_response” 配置为 “zhangsan”, 数据库返回结果为 “ZHANGSAN123”, 系统判定为匹配成功。

如果不指定该参数, 设备仅尝试与后台数据库服务器建立连接。默认值为空。

只有指定了参数 “sql_statement” 时, 才需要指定该参数。当健康检查的目的 IP 地址取值为 IPv6 地址时, 如果管理员配置的行列值超过查询语句实际返回的行列值, 那么 Mysql 健康检查功能将无法正常工作。

rows

可选, 该参数指定 “expected_response” 参数值所在的行。取值必须为 1 至 128 之间的整数, 默认值为 1。

cols

可选, 该参数指定 “expected_response” 参数值所在的列。取值必须为 1 至 128 之间的整数, 默认值为 1。

interval

可选, 该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数, 单位为秒。默认值为 5。

timeout

可选, 该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数, 单位为秒。默认值为 5。

max_retries

可选, 该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。

当取值为 3 时, 如果连续 3 次健康检查的结果都是 Up, 则系统将 SDNS 服务的状态设置为 Up; 如果连续 3 次健康检查的结果都是 Down, 则系统将 SDNS 服务的状态设置为 Down。

dst_address	可选，该参数指定 mysql 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 mysql 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 mysql 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 mysql 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“sdns service ip”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor mssql <template_name> <database_name> <username>
<password> [sql_statement] [expected_result] [rows] [cols] [interval] [timeout]
[max_retries] [dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Mssql 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

database_name 该参数指定 Mssql 数据库服务器的名称，取值必须为不大于 128 字节的字符串。

username 该参数指定登录 Mssql 数据库服务器的用户名称，取值必须为不大于 128 字节的字符串。

password 该参数指定登录 Mssql 数据库服务器的用户密码，取值必须为不大于 128 字节的字符串。当参数取值只包含数字或者包含特殊字符时，必须置于双引号内。

sql_statement	可选，该参数指定健康检查使用的 SQL 语句。取值必须为置于双引号内的长度不超过 128 个字节的字符串。仅支持 SELECT 语句。 例如：“select name from student where grade > 8 and age < 16”。 如果不指定该参数，设备则仅尝试与后台数据库服务器建立连接。默认值为空。
expected_result	可选，该参数指定执行 SQL 语句后期望返回的结果。取值必须为长度不大于 128 个字节的字符串。设备检查后台 Mssql 数据库返回的响应值时，采取部分匹配且不区分大小写。 例如：参数 “expected_response” 配置为 “zhangsan”，数据库返回结果为 “ZHANGSAN123”，系统判定为匹配成功。 如果不指定该参数，设备仅尝试与后台数据库服务器建立连接。默认值为空。 只有指定了参数 “sql_statement” 时，才需要指定该参数。当健康检查的目的 IP 地址取值为 IPv6 地址时，如果管理员配置的行列值超过查询语句实际返回的行列值，那么 Mssql 健康检查功能将无法正常工作。
rows	可选，该参数指定 “expected_response” 参数值所在的行。取值必须为 1 至 128 之间的整数，默认值为 1。
cols	可选，该参数指定 “expected_response” 参数值所在的列。取值必须为 1 至 128 之间的整数，默认值为 1。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状

态设置为 Down。

dst_address	可选，该参数指定 mssql 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 mssql 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 mssql 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 mssql 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor ftp <template_name> [request_line] [interval] [timeout]
[max_retries] [dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 FTP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
request_line	可选，该参数指定健康检查使用的 ftp 命令，如“ftp://user:passwd@1.1.1.1/”，默认为 ftp://加上 dst_address。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的

整数。默认值为 3。

当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address	可选，该参数指定 FTP 健康检查报文的目的地地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 FTP 健康检查报文的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 FTP 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 FTP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数 “src_address” 和 “gateway_address”。

sdns monitor snmp <template_name> [community] [version]

该命令用于定义一个 SNMP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为 “all”。
community	可选，该参数指定 SNMP 网络管理员访问系统的身份验证字符，取值必须为最大长度不大于 32 个字节的字符串。默认值为 “public”。
version	可选，该参数指定 SNMP 的版本，取值必须为 v1 或 v2c。默认值为 v1。

sdns monitor ldap <template_name> [bind_dn] [password] [search_dn] [filter_keyword]

该命令用于定义一个 LDAP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不

超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

- 注意：参数取值不能为 “all”。

bind_dn	可选，该参数指定用于绑定操作的唯一可辨识的名称 DN (Distinguished Name, 辨识名) (类似用户名)。取值必须为最大长度不大于 255 个字节的字符串。默认值为空。
password	可选，该参数指定登录 LDAP 服务器的密码。取值必须为最大长度为 255 个字节的字符串。默认值为空。
search_dn	可选，该参数指定执行搜索操作的 DN 的名称。取值必须为最大长度为 255 个字节的字符串。默认值为空。
filter_keyword	可选，该参数指定搜索 DN 时使用的过滤关键词。取值必须为最大长度为 255 个字节的字符串。通过关键词过滤，LDAP 后台服务可以返回满足过滤条件的结果集。如果该参数值为空，则按照默认的过滤条件返回所有符合参数 “search_dn” 的结果。为了减少网络数据流量，建议指定参数 “search_dn”。默认值为空。

sdns monitor diameter <template_name> [origin_host] [origin_realm]
[host_ip] [vendor_id] [product_name]

该命令用于定义一个 SMTP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为 “all”。
origin_host	可选，该参数指定 Origin-Host AVP 值，标识发起 Diameter 消息的主机。取值必须为长度不大于 128 个字节的字符串。默认值为 “array.hc.diameter.org”。
origin_realm	可选，该参数指定 Origin-Realm AVP 值，标识 Diameter 消息发送者的域。取值必须为长度不大于 128 个字节的字符串。默认值为 “hc.diameter.org”。
host_ip	可选，该参数指定 Host-IP-Address AVP 的值，标识 Diameter 消息发送者的 IP 地址。默认值为 “11.1.11.11”。

vendor_id	可选，该参数指定 Vendor-Id AVP 值，标识 Diameter 设备供应商。取值必须为 0 至 4,294,967,295 之间的整数。默认值为 11。
product_name	可选，该参数指定 Product-Name AVP 值，标识供应商为 Diameter 产品分配的名称。取值必须为长度不大于 128 个字节的字符串。默认值为“HC Interface”。

sdns monitor radius acct <template_name> <secret_string>
[response_code]

该命令用于定义一个 radius-acct 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
secret_string	该参数指定 RADIUS 客户端与 RADIUS 服务器共享的密钥，用于加密用户登录 RADIUS 服务器的密码。
response_code	可选，该参数指定期望 RADIUS 服务器返回的响应码，系统将根据响应码来判断 RADIUS 服务器的健康状态。参数取值为“5”时，表示 RADIUS 服务器开始响应计费请求，如果 RADIUS 服务器返回的响应码为 5，则 RADIUS 服务器状态为“Up”，否则 RADIUS 服务器状态为“Down”。默认值为 5。

sdns monitor radius auth <template_name> <secret_string> <username>
<password> [response_code] [attribute_list]

该命令用于定义一个 radius-auth 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
secret_string	该参数指定 RADIUS 客户端与 RADIUS 服务器共享的密钥，用于加密用户登录 RADIUS 服务器的密码。该密钥应该事先从 RADIUS 服务器获得。取值必须为长度不大于 127 字节的字符串，且必须包含在双引号内。
username	指定登录 RADIUS 服务器的用户名。取值必须为长度不大

	于 31 字节的字符串，且必须置于双引号内。
password	指定登录 RADIUS 服务器的密码。取值必须为长度不大于 31 字节的字符串，且必须包含在双引号内。
response_code	可选，该参数用于设置期望 RADIUS 服务器返回的响应码，系统将根据返回的响应码来判断 RADIUS 服务器的健康状况。取值必须： • 2：表示 RADIUS 服务器接受认证请求。当该参数取值为 2，且提供的用户名和密码都正确时，如果 RADIUS 服务器返回的响应码为 2，则 RADIUS 服务器状态为“Up”，否则 RADIUS 服务器状态为“Down”。 • 3：表示 RADIUS 服务器拒绝认证请求。当该参数取值为 3，且提供的密码错误时，如果 RADIUS 服务器返回的响应码为 3，则 RADIUS 服务器状态为“Up”，否则 RADIUS 服务器状态为“Down”。 默认值为 2。
attribute_list	可选，该参数指定系统支持的 RADIUS 认证的属性列表。取值支持的属性包括“User-Name”、“User-Password”、“NAS-IP-Address”和“NAS-Port”，可以包含最多三个属性，格式为： “attribute-name1=attribute-value1,attribute-name2=attribute-value2”。每个属性字符串的最大长度为不大于 31 字节，且属性字符串之间不允许有空格且必须以逗号（,）分隔。 例如：“NAS-IP-Address=192.168.1.2,NAS-Port=2012”。

sdns monitor siptcp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [src_port] [gateway_address]

该命令用于定义一个 SIP-TCP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 SIP-TCP 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 SIP-TCP 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 SIP-TCP 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
src_port	可选，该参数指定 SIP-TCP 健康检查报文的源端口。如果不指定该参数，则系统将自动选择源端口。
gateway_address	可选，该参数指定发送 SIP-TCP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor sipudp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [src_port] [gateway_address]

该命令用于定义一个 SIP-UDP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 SIP-UDP 健康检查报文的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 SIP-UDP 健康检查报文的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 SIP-UDP 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
src_port	可选，该参数指定 SIP-UDP 健康检查报文的源端口。如果不指定该参数，则系统将自动选择源端口。
gateway_address	可选，该参数指定发送 SIP-UDP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor smtp <template_name> [request_line] [expected_response]
[interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address]

该命令用于定义一个 SMTP 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

request_line	可选，该参数指定健康检查使用的 SMTP 请求，参数取值必须置于双引号内。默认为 NOOP
expected_response	可选，该参数指定期望的 SMTP 响应。参数取值必须置于双引号内。默认值为 “250”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定 SMTP 健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 SMTP 健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定 SMTP 健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送 SMTP 健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数 “src_address” 和 “gateway_address”。



注意：如果本命令中的参数 “dst_port” 的值是 0，系统将使用在命令 “**sdns service ip**” 中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数 “dst_port” 的值作为报文的目的端口。

```
sdns monitor rtsptcp <template_name> [request_line] [expected_response]
[interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address]
[gateway_address]
```

该命令用于定义一个 RTSPTCP 类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为 “all”。
request_line	可选，该参数指定健康检查使用的请求，参数取值必须置于双引号内。默认为 NOOP
expected_response	可选，该参数指定期望的响应。参数取值必须置于双引号内。默认值为 “250”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定健康检查报文的目的地地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数 “src_address” 和 “gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor oracle <template_name> <database_name> <username>
<password> [sql_statement] [expected_result] [rows] [cols] [interval] [timeout]
[max_retries] [dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Oracle 类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

database_name 该参数指定 Oracle 数据库服务器的名称，取值必须为不大于 128 字节的字符串。

username 该参数指定登录 Oracle 数据库服务器的用户名称，取值必须为不大于 128 字节的字符串。

password 该参数指定登录 Oracle 数据库服务器的用户密码，取值必须为不大于 128 字节的字符串。当参数取值只包含数字或者包含特殊字符时，必须置于双引号内。

sql_statement 可选，该参数指定健康检查使用的 SQL 语句。取值必须为置于双引号内的长度不超过 128 个字节的字符串。

仅支持 SELECT 语句。例如：“select name from student where grade > 8 and age < 16”。

如果不指定该参数，设备则仅尝试与后台数据库服务器建立连接。默认值为空。

expected_result 可选，该参数指定执行 SQL 语句后期望返回的结果。取值必须为长度不大于 128 个字节的字符串。设备检查后台 Oracle 数据库返回的响应值时，采取部分匹配且不区分大小写。

例如：参数“expected_response”配置为“zhangsan”，数据库返回结果为“ZHANGSAN123”，系统判定为匹

配成功。

如果不指定该参数，设备仅尝试与后台数据库服务器建立连接。默认值为空。

只有指定了参数“sql_statement”时，才需要指定该参数。当健康检查的目的 IP 地址取值为 IPv6 地址时，如果管理员配置的行列值超过查询语句实际返回的行列值，那么 Oracle 健康检查功能将无法正常工作。

rows	可选，该参数指定“expected_response”参数值所在的行。取值必须为 1 至 128 之间的整数，默认值为 1。
cols	可选，该参数指定“expected_response”参数值所在的列。取值必须为 1 至 128 之间的整数，默认值为 1。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。 在多链接环境中，为了确保设备可以正确接收 TCP 响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor scripttcp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Script-TCP 脚本类型的健康检查模板。

template_name 该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。

注意：参数取值不能为“all”。

interval 可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

timeout 可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。

max_retries 可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。

当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。

dst_address 可选，该参数指定健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。

dst_port 可选，该参数指定健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。

src_address 可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。

gateway_address 可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor scriptudp <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Script-UDP 脚本类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor scripttcps <template_name> [interval] [timeout] [max_retries] [dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个 Script-TCPS 脚本类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns monitor extscript <template_name> [interval] [timeout] [max_retries]
[dst_address] [dst_port] [src_address] [gateway_address]

该命令用于定义一个自定义脚本类型的健康检查模板。

template_name	该参数指定健康检查模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
interval	可选，该参数指定健康检查的时间间隔。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
timeout	可选，该参数指定健康检查的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。默认值为 5。
max_retries	可选，该参数指定设置 SDNS 服务为 Up 或 Down 的连续健康检查次数的最大值。取值必须为 1 到 10 之间的整数。默认值为 3。 当取值为 3 时，如果连续 3 次健康检查的结果都是 Up，则系统将 SDNS 服务的状态设置为 Up；如果连续 3 次健康检查的结果都是 Down，则系统将 SDNS 服务的状态设置为 Down。
dst_address	可选，该参数指定健康检查报文的目的地址。如果不指定该参数，则与健康检查模板绑定的 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定健康检查报文的目的端口。取值必须为 0 到 65,535 之间的整数。默认值为 0。
src_address	可选，该参数指定健康检查报文的源 IP 地址。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_address	可选，该参数指定发送健康检查报文的网关的 IP 地址。如果不指定该参数，则系统将自动选择网关 IP 地址。在多链接环境中，为了确保设备可以正确接收响应报文，建议配置参数“src_address”和“gateway_address”。



注意：如果本命令中的参数“dst_port”的值是 0，系统将使用在命令“**sdns service ip**”中指定的端口。这两个命令中的端口值不能同时为 0。当两个命令中的端口值都不为 0 且端口值不同时，将使用本命令中参数“dst_port”的值作为报文的目的端口。

sdns health import extscript <script_checker_name> <script_checker_url>

该命令用于通过文件导入方式导入 SDNS 健康检查使用的自定义健康检查脚本文件。

script_checker_name 该参数指定导入的自定义健康检查脚本文件的名称。取值必须为长度不大于 128 个字符的字符串。当参数取值包含特殊字符时，必须置于双引号内。（特殊字符包括 '@'、'_'、'-'、'!' 和 '.'）

注:取值不能为 all。

script_checker_url 该参数指定自定义健康检查请求文件的 HTTP 或 FTP 服务器的 URL 地址。

注意：FTP 类型的 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。

sdns health export extscript <script_checker_name> <script_checker_url>

该命令用于通过文件导出方式导出 SDNS 健康检查使用的自定义健康检查脚本文件。

script_checker_name 该参数指定导出的自定义健康检查脚本文件的名称。取值必须为长度不大于 128 个字符的字符串。当参数取值包含特殊字符时，必须置于双引号内。（特殊字符包括 '@'、'_'、'-'、'!' 和 '.'）

注:取值不能为 all。

script_checker_url 该参数指定自定义健康检查导出文件的 HTTP 或 FTP 服务器的 URL 地址。

注意：FTP 类型的 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。

no sdns health import extscript <script_checker_name>

该命令用于删除导入的指定的自定义健康检查脚本文件。

show sdns health import extscript [script_checker_name] [output_mode]

该命令用于显示导入的指定的自定义健康检查脚本文件。

script_checker_name 可选，该参数指定导入的指定自定义健康检查脚本文件的名称。如不指定该参数，则显示所有导入的自定义健康检查脚本文件名称。

output_mode 可选，该参数指定自定义健康检查脚本文件的输出模式。取值必须为：

- **binary**: 表示二进制输出模式。
- **text**: 表示文本输出模式。默认值为“binary”。

clear sdns health import extscript

该命令用于清除所有导入的自定义健康检查脚本文件。

sdns health associate <template_name> <script_checker_name>

该命令用于将指定的健康检查模板与导入的指定的自定义健康检查脚本文件关联起来。

template_name 该参数指定健康检查模板的名称。

script_checker_name 该参数指定已导入的自定义健康检查脚本文件。

no sdns health associate <template_name>

该命令用于删除指定的健康检查模板与导入的自定义健康检查脚本文件的关联关系。

template_name 该参数指定健康检查模板的名称。

show sdns health associate [template_name]

该命令用于显示指定的健康检查模板与导入的自定义请求文件和自定义响应文件的关联关系。如不指定参数，则显示所有模板与导入的自定义请求文件和自定义响应文件的关联关系。

clear sdns health associate

该命令用于删除所有健康检查模板与导入的自定义健康检查脚本文件的关联关系。

sdns monitor snmp collector <template_name> <oid_name> [community] [snmp_version] [interval] [dst_address] [dst_port] [src_address] [gateway_ip] [fail_delay] [prober_timeout]

该命令用于为指定的 SNMP OID 定义一个 SNMP 数据收集模板。

template_name	该参数指定数据收集模板的名称。取值必须为长度不超过 128 个字符的字符串，支持字母、数字、特殊字符，名称必须置于双引号内。参数取值不能包含空格和括号字符。 注意：参数取值不能为“all”。
oid_name	该参数指定 SNMP OID 的名称。取值必须是已经通过“sdns snmp oid”命令配置的 SNMP OID 的名称。
community	可选，该参数指定 SNMP 网络管理员访问系统时的身份验证字符，取值必须为最大长度不大于 32 个字节的字符串。默认值为“public”。
snmp_version	可选，该参数指定 SNMP 协议版本。取值必须为： • v1 • v2c 默认值为“v2c”。
interval	可选，该参数指定数据收集的时间间隔，单位为秒。取值必须为 10 到 86,400 之间的整数。默认值为 60。
dst_address	可选，该参数指定 SNMP 请求的目的 IP 地址。如果不指定该参数，当数据收集模板与 SDNS 服务池绑定后，服务池中每个 SDNS 服务 IP 将被用做目的 IP 地址。
dst_port	可选，该参数指定 SNMP 请求的目的端口。取值必须为 1 到 65,535 之间的整数。默认值为 161。
src_address	可选，该参数指定 SNMP 请求的源 IP 地址。取值建议配置系统管理 IP 地址，包括系统接口 IP、浮动 IP 地址、IP 地址池中的 IP 地址和支持 ARP 协议的虚拟 IP 地址。如果取值不是系统管理 IP 地址，会导致健康检查失败。如果不指定该参数，则系统将选用一个设备接口的 IP 地址作为源 IP 地址。
gateway_ip	可选，该参数指定网关 IP 地址。取值必须为 IPv4 或 IPv6 地址。对于 IPv4 地址，默认值是“0.0.0.0”；对于 IPv6 地址，默认值是“::”。
fail_delay	可选，该参数指定 SDNS 服务的健康检查状态被延迟标记为“Down”的时间。取值必须为 0 到 86,400 之间的整数，单位为秒。 默认值为 0，表示只要健康检查探测失败 SDNS 服务立即被标记为“Down”。

prober_timeout 可选，该参数指定健康检查探测的超时时间。取值必须为 3 到 86,400 之间的整数，单位为秒。取值必须小于参数 “timeout”。

默认值为 3。

no sdns monitor <template_name>

该命令用于删除指定的健康检查模板或数据收集模板。

show sdns monitor all

该命令用于显示全部健康检查模板和数据收集模板。

clear sdns monitor

该命令用于清除全部健康检查模板和数据收集模板。

sdns health import request <file_name> <url>

该命令用于从 HTTP 服务器或 FTP 服务器导入 SDNS 健康检查使用的自定义健康检查请求文件。需要注意的是，当导入的健康检查请求文件的内容是 HTTP 请求时，该文件内容的结尾需多输入两次换行符。系统支持导入最多 1,000 个自定义健康检查请求文件。

file_name 该参数指定导入的自定义健康检查请求文件的名称。取值必须为长度不大于 128 个字符的字符串。支持特殊字符 “@”、“_”、“-”、“!” 和 “.”。当参数取值包含特殊字符时，必须置于双引号内。

注意：

- 取值不能为 “all”。
- 取值可以和命令 “sdns health import response” 中 “file_name” 的取值相同。导入相同文件名的自定义健康检查请求文件时，会覆盖之前导入的文件。

url 该参数指定自定义健康检查请求文件的 HTTP 或 FTP 服务器的 URL 地址。

注意：FTP 类型的 URL

（ftp://user:password@host:port/path）中的 “path” 需使用相对路径。



注意：系统允许导入的自定义健康检查请求文件必须小于 16K，并且不能为空文件。

no sdns health import request <file_name>

该命令用于删除已导入的指定自定义健康检查请求文件。

show sdns health import request [file_name]

该命令用于显示指定的自定义健康检查请求文件的内容。如果不指定参数“file_name”，该命令将显示所有已导入的健康检查请求文件的名称。

clear sdns health import request

该命令用于清除所有已导入的自定义健康检查请求文件。

sdns health import response <file_name> <url>

该命令用于从 HTTP 服务器或 FTP 服务器导入 SDNS 健康检查使用的自定义健康检查响应文件。系统支持导入最多 1,000 个自定义健康检查响应文件。

file_name 该参数指定导入的自定义健康检查响应文件的名称。取值必须为长度不大于 128 个字符的字符串。支持特殊字符“@”、“_”、“-”、“!”和“.”。当参数取值包含特殊字符时，必须置于双引号内。

注意：

- 取值不能为“all”。
- 取值可以和命令“**sdns health import request**”中“file_name”的取值相同。导入相同文件名的自定义健康检查响应文件时，会覆盖之前导入的文件。

url 该参数指定自定义健康检查响应文件的 HTTP 或 FTP 服务器的 URL 地址。

注意： FTP 类型的 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。



注意： 系统允许导入的自定义健康检查响应文件必须小于 16K，并且不能为空文件。

no sdns health import response <file_name>

该命令用于删除已导入的指定自定义健康检查响应文件。

show sdns health import response [file_name]

该命令用于显示指定的自定义健康检查响应文件的内容。如果不指定参数“file_name”，该命令将显示所有已导入的健康检查响应文件的名称。

clear sdns health import response

该命令用于清除所有已导入的自定义健康检查响应文件。

sdns health bind <template_name> <request_file_name>
<response_file_name>

该命令用于为指定的 HTTP 或 HTTPS 类型的健康检查模板关联自定义健康检查请求文件和自定义健康检查响应文件。系统支持为一个健康检查模板关联一个自定义健康检查请求文件和一个健康检查响应文件。

template_name 该参数指定已存在的健康检查模板的名称。
request_file_name 该参数指定已导入的自定义健康检查请求文件。
response_file_name 该参数指定已导入的自定义健康检查响应文件

no sdns health bind <template_name>

该命令用于删除指定的 HTTP 或 HTTPS 类型的健康检查模板与自定义健康检查请求文件和自定义健康检查响应文件的关联关系。

show sdns health bind [template_name]

该命令用于显示指定的健康检查模板与导入的自定义请求文件和自定义响应文件的关联关系。如不指定参数，则显示所有模板与导入的自定义请求文件和自定义响应文件的关联关系。

clear sdns health bind

该命令用于清除所有 HTTP 或 HTTPS 类型的健康检查模板与自定义健康检查请求文件和自定义健康检查响应文件的关联关系。

sdns service monitor apply <service_name> <template_name>

该命令用于为指定的 SDNS 服务关联一个健康检查模板。当为 SDNS 服务关联了一个健康检查模板，系统将为该 SDNS 服务生成一个 monitor 实例。基于健康检查模板生成的实例又称为健康检查实例。一个 SDNS 服务最多可以关联 8 个健康检查模板。

service_name 该参数指定 SDNS 服务的名称。
template_name 该参数指定健康检查模板的名称。



注意：系统只允许 SNMP 数据收集模板与 SDNS 服务池相关联。

no sdns service monitor apply <service_name> <template_name>

该命令用于删除指定 SDNS 服务与指定的健康检查模板之间的关联。

clear sdns service monitor apply [service_name]

该命令用于清除指定 SDNS 服务与健康检查模板之间的关联。如果不指定参数“service_name”，将清除所有 SDNS 服务与健康检查模板之间的关联。

sdns pool monitor apply <pool_name> <template_name>

该命令用于为指定的 SDNS 服务池关联一个健康检查模板或数据收集模板。当为 SDNS 服务池关联了一个健康检查模板，系统将为该 SDNS 服务池中每个与该健康检查模板 IP 类型相同的成员生成一个 monitor 实例，即如果关联的健康检查模板为 IPv4 类型，系统只会为 IPv4 类型的 SDNS 服务生成实例，如果关联的健康检查模板为 IPv6 类型，系统只会为 IPv6 类型的 SDNS 服务生成实例。

一个 SDNS 服务池最多可以关联 16 个健康检查模板或数据收集模板（最多 8 个 IPv4 类型的健康检查模板和最多 8 个 IPv6 类型的健康检查模板）。

pool_name 该参数指定 SDNS 服务池的名称。

template_name 该参数指定健康检查模板或数据收集模板的名称。

no sdns pool monitor apply <pool_name> <template_name>

该命令用于删除指定 SDNS 服务池与指定的健康检查模板或数据收集模板之间的关联。

clear sdns pool monitor apply [pool_name]

该命令用于清除指定 SDNS 服务池与健康检查模板和数据收集模板之间的关联。如果不指定参数“pool_name”的名称，清除所有 SDNS 服务池与健康检查模板和数据收集模板之间的关联。

show sdns monitor instance [monitor_type]

该命令用于显示指定类型的 monitor 实例。

monitor_type 可选，该参数指定 monitor 实例的类型。取值必须为：

- icmp: 表示 ICMP 类型的健康检查实例。
- tcp: 表示 TCP 类型的健康检查实例。
- http: 表示 HTTP 类型的健康检查实例。
- https: 表示 HTTPS 类型的健康检查实例。
- snmp: 表示 SNMP 类型的数据收集实例。
- half-tcp: 表示 Half-TCP 类型的健康检查实例。
- udp: 表示 UDP 类型的健康检查实例。
- http2: 表示 HTTP2 类型的健康检查实例。
- https2: 表示 HTTPS2 类型的健康检查实例。

- ftp: 表示 FTP 类型的数据收集实例。
- ntp: 表示 NTP 类型的健康检查实例。
- pop3: 表示 POP3 类型的健康检查实例。
- smtp: 表示 SMTP 类型的健康检查实例。
- script-tcp: 表示 Script-TCP 类型的健康检查实例。
- diameter-tcp: 表示 Diameter-TCP 类型的数据收集实例。
- script-udp: 表示 Script-UDP 类型的健康检查实例。
- script-tcps: 表示 Script-TCPS 类型的健康检查实例。
- radius-auth: 表示 Radius-Auth 类型的健康检查实例。
- radius-acct: 表示 Radius-Acct 类型的健康检查实例。
- sip-tcp: 表示 SIP-TCP 类型的数据收集实例。
- sip-udp: 表示 SIP-UDP 类型的健康检查实例。
- dns: 表示 DNS 类型的健康检查实例。
- dns-tcp: 表示 DNS-TCP 类型的健康检查实例。
- rtsp-tcp: 表示 RTSP-TCP 类型的健康检查实例。
- ldap: 表示 LDAP 类型的数据收集实例。
- external-script: 表示 External-Script 类型的数据收集实例。
- mysql: 表示 MYSQL 类型的健康检查实例。
- mssql: 表示 MSSQL 类型的健康检查实例。
- oracle: 表示 ORACLE 类型的健康检查实例。

如果不指定该参数，将显示以上所有类型的 monitor 实例。

sdns service health relation <service_name> [relation]

该命令用于设置指定 SDNS 服务的健康检查实例之间的关系。

service_name 该参数指定 SDNS 服务的名称。

relation 可选，该参数指定该 SDNS 服务的健康检查实例之间的关系。取值必须为：

- **and:** 表示只有当 SDNS 服务的所有健康检查实例的结果为 Up 时，系统才标识该 SDNS 服务为 Up。
- **or:** 表示只要 SDNS 服务的任何一个健康检查实例的结果为 Up，系统就标识该 SDNS 服务为 Up。

默认值为 “and”。

show sdns service health relation [service_name]

该命令用于显示指定 SDNS 服务的健康检查实例之间的关系（and 或 or）。如果不指定参数 “service_name”，则将显示每个 SDNS 服务的健康检查实例之间的关系。

sdns pool health relation <pool_name> [relation]

该命令用于设置指定的 SDNS 服务池中每个成员的健康检查实例之间的关系。

当为 SDNS 服务池同时关联了 IPv4 类型的健康检查模板和 IPv6 类型的健康检查模板时，系统将为 SDNS 服务池中 SDNS 服务 IP 为 IPv4 和 IPv6 的 SDNS 服务成员分别设置健康检查实例之间的关系。

pool_name	该参数指定 SDNS 服务池的名称。
relation	可选，该参数指定该 SDNS 服务池中每个成员的健康检查实例之间的关系。取值必须为： • and: 表示只有当 SDNS 服务池中某个成员的所有健康检查实例的结果为 Up 时，系统才标识该成员为 Up。 • or: 表示只要 SDNS 服务池中某个成员的任何一个健康检查实例的结果为 Up，系统就标识该成员为 Up。

默认值为 “and”。



注意：SDNS 服务池中每个成员的 SNMP 数据收集实例的结果不会对该成员的健康检查结果有任何影响。

show sdns pool health relation [pool_name]

该命令用于显示指定 SDNS 服务池中每个成员的健康检查实例之间的关系（and 或 or）。如果不指定参数 “pool_name”，则将显示每个 SDNS 服务中每个成员的健康检查实例之间的关系。

sdns pool health mixrelation <pool_name> <expression>

该命令用于为指定 SDNS 服务池中每个成员的多个健康检查实例设置混合关系。

支持通过该命令修改 SDNS 服务池的混合关系。

pool_name 该参数指定 SDNS 服务池的名称。

expression 该参数指定用于判断 SDNS 服务池中每个成员健康检查状态的关系表达式。表达式必须置于双引号内。表达式结构为: (monitor group1) OR/AND (monitor group2) OR/AND (monitor group3)...

表达式中的一个括号代表一个健康检查模板组，系统最多支持定义 10 个组（最多 5 个 IPv4 类型的健康检查模板组和最多 5 个 IPv6 类型的健康检查模板组），组之间的逻辑关系用 AND 或 OR 连接，如(m1) OR (m2 OR m3) AND (m4)，如 m1 OR m2 或((m1 OR m2) AND m3) 都是不合法的表达式。

每个组中最多支持定义不超过 8 个健康检查模板。不同健康检查模板组中可以使用相同的健康检查模板。

出现在表达式中的健康检查模板应该与服务池关联。如果表达式中的健康检查模板被删除，与该模板相关的设置也将从表达式中删除。

另外，当为 SDNS 服务池同时关联了 IPv4 类型的健康检查模板和 IPv6 类型的健康检查模板时，SDNS 服务池的混合关系需要用 “,” 分隔。例如：sdns pool health mixrelation pool_1 “(m1)OR(m2 OR m3),(m4)AND(m5 OR m6)” 其中，m1、m2 和 m3 为 IPv4 类型的健康检查模板，m4、m5 和 m6 为 IPv6 类型的健康检查模板。该参数取值支持以下几种输入方式：

- “IPv4 类型的健康检查模板组关系，IPv6 类型的健康检查模板组关系”，例如：(m1)OR(m2 OR m3),(m4)AND(m5 OR m6)。
- “IPv4 类型的健康检查模板组关系”，例如：(m1)OR(m2 OR m3)。
- “IPv6 类型的健康检查模板组关系”，例如：(m4)OR(m5 OR m6)。



注意：当为服务池设置了混合关系时，“sdns pool health relation”命令中设置的实例关系（AND 或 OR）将不再生效。

no sdns pool health mixrelation <pool_name>

该命令用于删除指定 SDNS 服务池中每个成员的多个健康检查实例之间的逻辑关系。

show sdns pool health mixrelation [pool_name]

该命令用于显示指定 SDNS 服务池中健康检查实例之间的混合关系。如果不指定参数“pool_name”，则将显示所有 SDNS 服务池的健康检查实例之间的混合关系。

13.9 SDNS 探测池

sdns health pool name <health_pool_name> [method] [numofmeh_probed] [up_num]

该命令用于定义一个 SDNS 探测池。设备支持配置最多 1,000 个 SDNS 探测池。

health_pool_name 该参数指定 SDNS 探测池的名称，取值必须为长度不超过 128 个字节的字符串。

注意：参数取值不能为“all”。

method 可选，该参数指定 SDNS 探测池的算法，取值必须为：

rr: Round Robin，轮训算法。

ga: Global Availability，全局可用性算法。

默认值为：“ga”。

prober_num 可选，该参数指定探测池每次进行健康检查探测的成员的个数。取值必须为 0 到 63 之间的整数。

默认值为 0，表示 SDNS 探测池对所有成员都进行探测。

up_num 可选，该参数指定健康检查探测成功需要的最少成员的数量。取值必须为 1 到 63 之间的整数，取值不能大于参数“prober_num”。

默认值为 1，表示只要探测池成员中有一个健康检查为“UP”，就判定 SDNS 服务状态为“UP”。

no sdns health pool name <health_pool_name>

该命令用于删除指定 SDNS 探测池。

show sdns health pool name

该命令用于显示所有 SDNS 探测池配置。

clear sdns health pool name

该命令用于清除所有 SDNS 探测池配置。

show sdns health pool status [dc_name] [node_name]

该命令用于显示指定 SDNS 数据中心下指定 SDNS 数据中心的探测池状态。

- dc_name 可选。该参数指定已存在的 SDNS 数据中心的名称。
- 如果指定该参数，系统将显示指定 SDNS 数据中心的探测池状态。
 - 如果不指定该参数，即默认为空，系统将显示所有 SDNS 数据中心的探测池状态。

默认值为空。

- node_name 可选。该参数指定已存在的 SDNS 数据中心节点的名称。
- 如果指定该参数，系统将显示指定 SDNS 数据中心节点的探测池状态。
 - 如果不指定该参数，即默认为空，系统将显示所有 SDNS 数据中心节点的探测池状态。

默认值为空。

例如：

Demo(config)#show sdns heal pool status				
Pool_Name	Associated_DC	Node_Name	Weight	Status
p1	dc1	node1	255	offline
p1	dc1	node2	250	offline

sdns health pool member <health_pool_name> <node_name> <weight>

该命令用于向指定的 SDNS 探测池中添加一个 SDNS 数据中心节点。一个 SDNS 探测池支持添加最多 64 个 SDNS 数据中心节点。

- health_pool_name 该参数指定已存在的 SDNS 探测池的名称。
- node_name 该参数指定已存在的 SDNS 数据中心节点的名称。
- weight 该参数指定 SDNS 数据中心节点在探测池中的权重，取值范围必须为 0 到 4,294,967,295 的整数。同一个探测池中的每个节点的权重必须唯一。

no sdns health pool member <health_pool_name> <node_name>

该命令用于从指定 SDNS 探测池中删除指定的 SDNS 数据中心节点。

show sdns health pool member

该命令用于显示所有 SDNS 探测池下的所有 SDNS 数据中心节点。

clear sdns health pool member <health_pool_name>

该命令用于清除指定 SDNS 探测池中的所有 SDNS 数据中心节点。

sdns health pool enable <health_pool_name> [node_name]

该命令用于启用指定的 SDNS 探测池中的指定 SDNS 数据中心节点。

sdns health pool apply <health_pool_name>

<dc_name|service_name|link_name> [mode] [type]

该命令用于为指定的 SDNS 探测池关联指定的 SDNS 数据中心、SDNS 服务或者 SDNS 链路。系统仅支持为一个 SDNS 数据中心、SDNS 服务或者 SDNS 链路的指定模式关联一个 SDNS 探测池。

health_pool_name	该参数指定已存在的 SDNS 探测池的名称。
dc_name service_name link_name	该参数指定已存在的 SDNS 数据中心、SDNS 服务或者 SDNS 链路的名称。
mode	可选，该参数指定 SDNS 探测池的关联模式。取值必须为： • primary: 首选模式。系统将优先使用该模式关联的探测池。 • fallback: 备选模式。仅在首选探测池不可用时，系统使用该模式关联的探测池。 默认值为“primary”。
type	可选，该参数指定 SDNS 探测池关联的资源类型。取值不区分大小写，取值必须为： • DC: 表示该探测池将关联到 SDNS 数据中心。 • LINK: 表示该探测池将应用到 SDNS 链路。 • SERVICE: 表示该探测池将应用到 SDNS 服务。 默认值为“DC”。

no sdns health pool apply <health_pool_name>

<dc_name|service_name|link_name> [mode]

该命令用于解除指定的 SDNS 探测池与指定的 SDNS 数据中心、SDNS 服务或 SDNS 链路的关联关系。如不指定参数“mode”，则为指定的 SDNS 数据中心的首选模式取消应用 SDNS 探测池。

show sdns health pool apply

该命令用于显示所有 SDNS 探测池与所有的 SDNS 数据中心、SDNS 服务或 SDNS 链路的关联关系。。

clear sdns health pool apply [health_pool_name]

该命令用于为指定的 SDNS 探测池清除与所有的 SDNS 数据中心、SDNS 服务或 SDNS 链路的关联关系。如不指定参数 “health_pool_name”，则为所有 SDNS 探测池清除与所有的 SDNS 数据中心、SDNS 服务或 SDNS 链路的关联关系。

13.10 SDNS 静态和 IP 域表就近性规则

sdns proximity <source_ip> <netmask|prefix> <region_name> [relation]

该命令用于为指定的 SDNS 区域添加一条静态 SDNS 就近性规则。静态 SDNS 就近性规则（包括 IP region 就近性规则）的优先级高于动态就近性规则。系统最多支持配置 2,000,000 条 SDNS 就近性规则（包括所有静态和动态就近性规则）。

source_ip	该参数指定源子网的 IP 地址。其取值可以为 IPv4 或 IPv6 地址。
netmask prefix	该参数指定源子网的掩码或前缀长度。参数 “source_ip” 和 “netmask prefix” 共同确定一个子网。 “mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。 “prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。
region_name	该参数指定一个已有的 SDNS 区域。
relation	可选，该参数指定静态 SDNS 就近性规则匹配关系。取值必须为： - is: 表示“是”关系，即源子网匹配了该静态 SDNS 就近性规则时，系统将返回该 SDNS 区域关联的 SDNS 服务。 - not: 表示“非”关系，即源子网不匹配了该静态 SDNS 就近性规则时，系统将返回该 SDNS 区域关联的 SDNS 服务。 默认值为 “is”。



注意：

- SDNS 采用最长前缀匹配规则来选择与本地 DNS 服务器的 IP 地址最相匹配的 SDNS 区域。
- 由参数 “source_ip” 和 “netmask|prefix” 确定的子网可以用于多个 SDNS 区域的

静态 SDNS 就近性规则。但是为了确保对于一个 SDNS 域名仅有一条优先级最高的 SDNS 区域策略被命中, 需要为 SDNS 域名关联的 SDNS 区域策略配置不同的优先级。

no sdns proximity <source_ip> <netmask|prefix> <region_name> [relation]

该命令用于删除指定的静态 SDNS 就近性规则。

show sdns proximity static

该命令用于显示全部静态 SDNS 就近性规则。

clear sdns proximity

该命令用于清除全部静态 SDNS 就近性规则。

sdns ipregion proximity <ipregion_name/ipregion_expression>
<region_name> [relation]

该命令用于将指定的 IP 域表或者域表关系表达式和 SDNS 区域关联。当一个 IP 域表或者域表关系表达式和 SDNS 区域关联后, 系统会批量生成 SDNS IP 域就近性规则。系统支持最多 1000 条 IP 域就近性规则。该命令支持在分区下执行。

ipregion_name|ipregion_ 该参数指定一个已有的 IP 域表的名称或域表关系表达式。
expression 域表关系表达式必须置于双引号内。如果该参数取值非域表关系表达式, 默认为 IP 域表名称。

域表关系表达式结构为:

“China_IP Version” 或

“China_State_IP Version” 或

“China_ISP_IP Version” 或

“China_State_city_IP Version” 或

“China_State_ISP_IP Version” 或

“China_NOT_State_IP Version” 或

“China_NOT_ISP_IP Version” 或

“China_State_city_ISP_IP Version” 或

“China_State_NOT_city_IP Version” 或

“China_State_NOT_ISP_IP Version” 或

“China_NOT_State_ISP_IP Version” 或

“China_State_NOT_city_ISP_IP Version” 或

“China_State_city_NOT_ISP_IP Version”。

其中：

- “China”：代表中国，为固定取值。
- “State”：代表省级或者直辖市。取值应首字母应大写，其他字母小写。
- “city”：代表市级。取值应市级所有字母都应小写。
- “ISP”代表网络服务运营商。取值可以为 CMCC（中国移动）、CUCC（中国联通）、CTCC（中国电信）、CTT（中国铁通）和 CERNET（中国教育网）。
- “IP Version”：代表版本协议，系统支持使用 IPv4 或者 IPv6 类型的协议。

另外，当域表关系表达式表达不属于关系时，表达式中需要用“NOT”进行表达。该参数取值支持以下几种输入方式：

- “China_NOT_State_IP Version”：表示除了这个省以外的国内的所有省。
- “China_State_NOT_city_IP Version”：表示除了这个市以外的省内的所有市。
- “China_State_city_NOT_ISP_IP Version”：表示除了这个运营商以外的其它的所有运营商。

注意：

- 如果域表关系表达式中的省市级名称和已有的 IP 域表名称相同，则使用已有的 IP 域表。
- 域表关系表达式中不支持直辖市的区，如：北京市朝阳区。

region_name

该参数指定一个已有的 SDNS 区域。

relation

可选，该参数指定 IP 域或者域表就近性规则匹配关系。取值必须为：

- is：表示“是”关系，即 IP 域表或者域表匹配了该静态 SDNS 就近性规则时，系统将返回该 SDNS 区域关联的 SDNS 服务。
- not：表示“非”关系，即 IP 域表或者域表不匹配

了该静态 SDNS 就近性规则时，系统将返回该 SDNS 区域关联的 SDNS 服务。

默认值为“is”。



注意：该命令不支持在分区内使用。

no sdns ipregion proximity <ipregion_name> <region_name> [relation]

该命令用于删除该参数指定的 SDNS IP 域表和 SDNS 区域之间的关联。该命令支持在分区下执行。

show sdns ipregion proximity

该命令用于显示全部 SDNS IP 域表和 SDNS 区域之间的关联。

clear sdns ipregion proximity

该命令用于清除全部 SDNS IP 域表和 SDNS 区域之间的关联。

show sdns proximity ipregion

该命令用于显示全部 SDNS IP 域就近性规则。

show sdns proximity match <local_dns_ip>

该命令用于手动查询一个本地 DNS 服务器将会匹配的 SDNS 区域。

local_dns_ip 该参数指定本地 DNS 服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

13.11 SDNS 动态就近性探测系统

sdns dps {on|off}

该命令用于启用或禁用动态就近性探测系统（Dynamic Proximity System，DPS）功能。该功能默认设置为禁用。

动态就近性探测系统由 DPS 服务器和 DPS 探测器组成。

DPS 服务器的主要功能如下：

- 收集本地 DNS 服务器的 IP 地址列表并将列表发送给 DPS 探测器供探测采用。
- 从 DPS 探测器收集就近性探测结果并根据结果生成动态就近性探测规则。

DPS 探测器的主要功能如下：

- 接收来自 DPS 服务器的本地 DNS 服务器的 IP 地址列表。

- 向本地 DNS 服务器发送探测报文以获取三类就近性信息：往返时间（Round Trip Time, RTT）、丢包率（Packet Loss Rate, PLR）和路由跳数。
- 向 DPS 服务器报告就近性探测结果。

DPS 功能启用后，设备会作为一台 DPS 服务器工作，并仅向在同一台设备上配置的 DPS 探测器发送本地 DNS 服务器的 IP 地址列表。

sdns dps interval send [interval]

该命令用于设置 DPS 服务器向 DPS 探测器发送本地 DNS 服务器的 IP 地址列表的时间间隔。

interval 可选，该参数指定时间间隔。取值必须为 1 到 2,147,483,647 之间的整数，单位为秒。默认值为 120。

sdns dps interval query [interval]

该命令用于设置 DPS 服务器从 DPS 探测器收集就近性探测结果的时间间隔。

interval 可选，该参数指定时间间隔。取值必须为 1 到 2,147,483,647 之间的整数，单位为秒。默认值为 1200。

sdns dps detector <region_name> <ip_address> [dps_port] [detect_interval] [cache_time] [dc_name] [link_name]

该命令用于为指定的 SDNS 区域配置 DPS 探测器。每个 SDNS 区域只能配置一个 DPS 探测器。系统支持配置最多 128 个 DPS 探测器。

region_name 该参数指定一个已有的 SDNS 区域。

ip_address 该参数指定 DPS 探测器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

如果该参数的取值为设备上一个接口的 IP 地址，则设备将作为指定的 SDNS 区域的 DPS 探测器。在此之前，需要先运行“**sdns dps localdetector**”启动 DPS 探测器进程。

dps_port 可选，该参数指定 DPS 探测器用于与 DPS 服务器通信的端口。取值必须为 1 到 65,535 之间的整数。默认值为 44,544。

detect_interval 可选，该参数指定 DPS 探测器的探测间隔。取值必须为 5 到 2,147,483,647 之间的整数，单位为秒。默认值为 900。

cache_time 可选，该参数指定从 DPS 服务器获取的 DNS IP 地址列表在 DPS 探测器上被缓存的时长。取值必须为 1 到 2,147,483,647 之间的整数，单位为秒。默认值为 172,800。

dc_name 可选, 该参数指定一个已存在的 SDNS 数据中心的名称。该参数只需要在一级算法指定为 RTT 时配置。默认值为空。

link_name 可选, 该参数指定一个已存在的 SDNS 链路名称。该参数只需要在一级算法指定为 RTT 时配置。默认值为空。



注意: 如果命令 “**sdns dps localdetector**” 中的参数 “ip_address” 的值为 “0.0.0.0” 或 “::”, 则本命令中参数 “ip_address” 的值应设置为一个接口的 IP 地址, 才能使用本地 DPS 探测器进程作为 DPS 探测器。

no sdns dps detector <region_name>

该命令用于删除指定的 SDNS 区域的 DPS 探测器。

show sdns dps detector

该命令用于显示全部 DPS 探测器。

clear sdns dps detector

该命令用于清除全部 DPS 探测器。

sdns dps localdetector <detector_name> <ip_address> [detect_port] [dps_port] [detect_timeout] [gateway_ip] [dps_ip] [type]

该命令用于在设备上启动一个本地 DPS 探测器进程。系统支持启动最多 8 个本地 DPS 探测器进程。

detector_name 该参数指定本地 DPS 探测器进程的名称。取值必须为长度不大于 128 个字节的字符串。

注意: 参数取值不能为 “all”。

ip_address 该参数指定本地 DPS 探测器进程监听的 IP 地址。取值必须为一个接口的 IP 地址。“0.0.0.0”表示监听全部 IPv4 地址; “::”表示监听全部 IPv6 地址。

detect_port 可选, 该参数指定本地 DPS 探测器进程向本地 DNS 服务器发送探测报文采用的源端口。取值必须为 1025 到 65,535 之间的整数。默认值为 53,455。

dps_port 可选, 该参数指定本地 DPS 探测器进程与 DPS 服务器通信时采用的监听端口。取值必须为 1025 到 65,535 之间的整数。默认值为 44,544。

detect_timeout 可选, 该参数指定探测本地 DNS 服务器的超时时间。取值必须为 1 到 2,147,483,647 之间的整数。默认值为 30。

gateway_ip	可选，该参数指定转发探测报文的网关的 IP 地址。取值必须为 IPv4 或 IPv6 地址。默认值是“0.0.0.0”或“::”，表示设备将自动选择网关。
dps_ip	可选，该参数指定 DPS 探测器用于和 DPS 服务器通信的 IP 地址。当指定该参数时，“ip_address”中指定的 IP 地址将只负责探测本地 DNS 服务器，该参数中指定的 IP 地址将负责与 DPS 服务器通信。当不指定该参数时，“ip_address”中的 IP 将同时负责探测本地 DNS 服务器和与 DPS 服务器的通信，即该参数的默认值与“ip_address”参数的取值相同。 当启用本地 DPS 探测器时，“sdns dps detector”命令中的“ip_address”参数应该与此命令中的“dps_ip”相同。
type	可选，该参数指定本地 DPS 探测器的探测协议类型，取值必须为： - icmp：表示本地 DPS 探测器的探测协议为 icmp。 - udp：表示本地 DPS 探测器的探测协议为 udp。 - tcp：表示本地 DPS 探测器的探测协议为 tcp。 默认值为“icmp”。



注意：

- 该命令中“detect_port”和“dps_port”参数值不能相同。
- 该命令中“dps_port”参数值必须与对应的“sdns dps detector”配置中的“dps_port”参数值相同。
- 每个本地 DPS 探测器进程的“detect_port”和“dps_port”参数值在所有的本地 DPS 探测器进程中是唯一的。

no sdns dps localdetector <detector_name>

该命令用于停止指定的本地 DPS 探测器进程。

show sdns dps localdetector

该命令用于显示全部本地 DPS 探测器进程。

clear sdns dps localdetector

该命令用于停止全部已经启动的本地 DPS 探测器进程。

sdns dps method <method> [weight_of_rtt] [weight_of_plr] [weight_of_hops]

该命令用于配置 DPS 算法。DPS 服务器采用 DPS 算法计算本地 DNS 服务器和每个 SDNS 区域(DPS 探测器)之间路径的“metric”。DPS 服务器为路径的“metric”最小的本地 DNS 服务器和 SDNS 区域创建一条动态就近性规则。

method	该参数指定 DPS 算法。取值必须为： • rtt: metric 等于探测报文往返时间(Round Trip Time, RTT)。 • plr: metric 等于探测丢包率(Packet Loss Rate, PLR)。 • hops: metric 等于路由跳数(hops)。 • mix: DPS 服务器将按照(权重 x 往返时间 + 权重 x 丢包率 + 权重 x 路由跳数)计算一个路径的 metric 值。 默认值为“rtt”。
weight_of_rtt	可选，该参数指定报文往返时间的权重值。只有当 DPS 算法为 mix 时才能设置该参数。其取值范围为 0 到 9 之间的整数。默认值为 1。
weight_of_plr	可选，该参数指定丢包率的权重值。只有当 DPS 算法为 mix 时才能设置该参数。其取值范围为 0 到 9 之间的整数。默认值为 1。
weight_of_hops	可选，该参数指定路由跳数的权重值。只有当 DPS 算法为 mix 时才能设置该参数。其取值范围为 0 到 9 之间的整数。默认值为 1。



注意：参数“weight_of_rtt”、“weight_of_plr”和“weight_of_hops”的值不能同时为 0。

show sdns dps method

该命令用于显示 DPS 算法。

show sdns proximity dynamic

该命令用于显示全部动态就近性规则。

clear sdns dps history

该命令用于清除 DPS 的历史数据，包括动态就近性规则和从 DPS 探测器接收到的就近性结果。

sdns dps expire [expire_time]

该命令用于设置动态就近性规则的失效时间。系统将清除到达失效时间的动态就近性规则。

interval 可选，该参数指定动态就近性规则的失效时间。取值必须为 5 到 2,147,483,647 之间的整数，单位为秒。默认值为 1500。

show sdns dps expire

该命令用于显示动态就近性规则的失效时间。

sdns dps write proximity file <file_name>

该命令用于将全部动态就近性规则保存到一个位于设备上的本地文件中。

file_name 该参数指定保存动态就近性规则的本地文件的名称。

sdns dps write proximity scp {remote_server_ip|name} <user_name> <file_path> <file_name>

该命令用于将全部动态就近性规则保存到一个位于远端 SCP 服务器的文件中。

remote_server_ip|name 该参数指定远端 SCP 服务器的 IP 地址或名称。取值必须置于双引号内。

user_name 该参数指定访问远端 SCP 服务器的用户名。输入用户名后，系统将提示输入密码。

file_path 该参数指定远端 SCP 服务器上保存全部动态就近性规则的文件所在的路径。

file_name 该参数指定远端 SCP 服务器上保存全部动态就近性规则的文件名称。

sdns dps write proximity tftp <remote_server_ip> <file_name>

该命令用于将全部动态就近性规则保存到一个位于远端 TFTP 服务器的文件中。

remote_server_ip 该参数指定远端 TFTP 服务器的 IP 地址。

file_name 该参数指定远端 TFTP 服务器上保存全部动态就近性规则的文件名称。

show sdns dps path [local_dns_ip]

该命令用于显示指定的本地 DNS 服务器与每个 DPS 探测器（SDNS 区域）之间的报文往返时间、丢包率和路由跳数。

local_dns_ip 可选，该参数指定本地 DNS 服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。“0.0.0.0”表示全部 IPv4

的本地 DPS；“::”表示全部 IPv6 的本地 DPS。如不指定参数值，则将显示全部本地 DNS 服务器和 DPS 探测器两两之间的报文往返时间、丢包率和路由跳数。

show sdns dps status

该命令用于显示 DPS 服务器和设备上的本地 DPS 探测器的状态。

例如：

```
Demo(config)#show sdns dps status
```

```
SDNS DPS service is ON
```

Local Detector	Status
detect1	UP
detect2	UP

show sdns dps all

该命令用于显示全部 SDNS DPS 的配置信息。

clear sdns dps all

该命令用于将全部 SDNS DPS 的配置重置为默认值。

13.12 DNS 资源记录

表13 - 2 DNS 资源记录数量限制

规格	内存			
	<4G	≥4G	≥32G	≥128G
DNS 区域	0	5000	10000	20000
IP 类型资源记录	0	10000	20000	40000
CNAME 类型资源记录	0	10000	20000	40000
MX 类型资源记录	0	10000	20000	40000
NS 类型资源记录	0	10000	20000	40000
SRV 类型资源记录	0	10000	20000	40000
SOA 类型资源记录	0	10000	20000	40000
PTR 类型资源记录	0	10000	20000	40000
TXT 类型资源记录	0	10000	20000	40000
SPF 类型资源记录	0	10000	20000	40000

sdns record ip <record_name> <domain_name> <ip_address> [ttl]

[expiration_date] [expiration_action] [autopttr]

该命令用于为指定的域名添加一条 A 或 AAAA 资源记录，并为该资源记录定义名称。该命令还可以用于修改已有资源记录的 IP 地址和 TTL。

record_name	该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。 注意： - 参数取值不能为 “all”。 - 由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。
domain_name	该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。
ip_address	该参数指定域名对应的 IP 地址，取值必须为 IPv4 或 IPv6 地址。
ttl	可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。
expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式，其中，“yyyy” 表示年份，“mm” 表示月份，而 “dd” 表示日。比如：“20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： block：表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 delete：表示系统将删除该资源记录。 默认值为 block。
autoptr	可选，该参数指定是否启用 PTR 记录联动，取值必须为 on：表示启用 PTR 资源记录联动，即当管理员添加 A 或 AAAA 资源记录时，系统将同时自动生成相应的 PTR 区域和一条 PTR 资源记录。且当管理员将该条 A 或 AAAA 资源记录与 DNS 区域绑定时，自动生成的 PTR 资源记录也将与该 DNS 区域绑定。 off：表示禁用 PTR 记录联动。 默认值为 off。



注意：自动生成的 PTR 记录不可手动改修，当 IP 记录更改记录类型不为 A 或 AAAA 时，删除相应的自动 PTR 记录，关闭 IP 记录联动功能时，删除不使用的 zone 和关联的 PTR 记录。IP 记录的 zone 和联动 PTR 记录的 zone 在同一视图下。zone 的命名格式为 ip 前缀，记录命名格式为“autoptr_ip_id”，如果该 zone 已存在，则直接使用该 zone。修改了 A 或 AAAA 资源记录后，相应的联动 PTR 资源记录会自动修改。

sdns record cname <record_name> <domain_name> <cname> [ttl]
[expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 CNAME 资源记录，CNAME 记录可以让一个域名成为另一个域名的别名，最终解析到一个主机的真实地址。该命令还可以用于修改已有记录的别名和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name 该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

cname 该参数指定域名的别名，取值必须是长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date 可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action 可选参数，指定资源记录过期时的处理动作，取值必须为：

- **block**：表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。

- **delete:** 表示系统将删除该资源记录。

默认值为 block。

sdns record dname <record_name> <domain_name1> <domain_name2>
[ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 DNAME 资源记录。DNAME 称为委托名称记录，用于用一条资源记录重定向多个子域，并将它们指向另一个域。该命令还可以用于修改已有资源记录的要解析的 DNS 域名、要重定向到的权威 DNS 域名和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意:

- 参数取值不能为 “all”。
- 由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name1 该参数指定要解析的 DNS 域名，取值必须为长度不超过 128 个字节的字符串，格式为 “xyz.com”，支持以点号或冒号结束。

domain_name2 该参数指定要重定向到的权威 DNS 域名，取值必须为长度不超过 128 个字节的字符串，格式为 “xyz.com”，支持以点号或冒号结束。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 8,6400。

expiration_date 可选参数，该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式，其中，“yyyy” 表示年份，“mm” 表示月份，而 “dd” 表示日。比如：“20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action 可选参数，指定资源记录过期时的处理动作，取值必须为：

- **block:** 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。

- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record hinfo <record_name> <domain_name> <cpu_type> <os_type> [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 HINFO 资源记录，通过 HINFO 记录，域名系统可以提供一个主机所使用的计算机硬件类型和操作系统的简要描述。该命令还可以用于修改已有记录的域名、CPU 信息、操作系统信息和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为 “all”。
- 由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name 该参数指定要解析的 DNS 域名，取值必须长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。

cpu_type 该参数指定实际提供域名解析服务的 DNS 服务器的 CPU 信息。取值必须长度不超过 255 个字节的字符串。

os_type 该参数指定实际提供域名解析服务的 DNS 服务器的操作系统信息。取值必须长度不超过 255 个字节的字符串。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 8,6400。

expiration_date 可选参数，该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式，其中，“yyyy” 表示年份，“mm” 表示月份，而 “dd” 表示日。比如：“20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action 可选参数，指定资源记录过期时的处理动作，取值必须为：

- block: 表示系统将禁用该资源记录，即该资源记录

在解除禁用前将不能再使用。

- **delete:** 表示系统将删除该资源记录。

默认值为 block。

sdns record https <record_name> <domain_name1> <domain_name2>
<priority> [value] [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 HTTPS 资源记录,HTTPS 资源记录即 Type65 记录,方便查找连接到网络服务所需的信息,通过一次 DNS 查询来加速通信连接过程。该命令还可以用于修改已有记录的域名、优先级、键值对和 TTL。

record_name 该参数指定资源记录名称,取值必须为长度不大于 128 个字节的字符串。

注意:

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步,所以该参数取值不能包含该前缀。

domain_name1 该参数指定要解析的 DNS 域名,取值必须长度不超过 128 个字节的字符串,格式为“xyz.com”,支持以点号或冒号结束。

domain_name2 该参数指定要重定向到的权威 DNS 域名,取值必须长度不超过 128 个字节的字符串,格式为“xyz.com”,支持以点号或冒号结束。

priority 该参数指定资源记录的优先级,取值必须为 0 到 65,535 之间的整数。其中:

- 0 表示别名模式,用于绑定根域名。
- 大于 0: 表示服务模式,用于返回服务参数。

value 可选参数,取值必须为长度不超过 512 个字符的字符串,格式为键值对“key=value”,键值对不可使用引号,多个键值对之间以分号作分隔,最多配置 10 条键值对。默认值为空。关于 key 的取值范围,详见 RFC 9460。

ttl 可选参数,该参数指定资源记录的 TTL,单位为秒。取值必须为 0 到 4,294,967,295 之间的整数,默认值为 86,400。

expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示2010年1月29日。其中“yyyy”的取值应该为2,000至2,037之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： • block：表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 • delete：表示系统将删除该资源记录。 默认值为 block。

sdns record ns <record_name> <domain_name1> <domain_name2> [ttl]
[expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 NS 资源记录，并为该记录定义名称。NS 资源记录定义了解析指定域名（domain_name1）的权威 DNS 服务器

（domain_name2），因此权威 DNS 服务器上必须存在相应的 A 或 AAAA 资源记录。该命令还可以用于修改已有资源记录的 DNS 域名、权威 DNS 服务器域名和 TTL。

record_name	该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name1	该参数指定 DNS 域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，支持以点号或冒号结束。

domain_name2	该参数指定权威 DNS 服务器的域名。

ttl	可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示

2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action

可选参数，指定资源记录过期时的处理动作，取值必须为：

- block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。
- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record ptr <record_name> <ip_address> <domain_name> [ttl]
[expiration_date] [expiration_action]

该命令用于为指定的 IP 地址添加一条 PTR 资源记录，并为该记录定义名称。PTR 资源记录用于执行反向域名解析，即将 IP 地址解析为域名。该命令还可以用于修改已有资源记录的 IP 地址、DNS 域名和 TTL。

record_name

该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

ip_address

该参数指定域名对应的 IP 地址，取值必须为 IPv4 或 IPv6 地址。不支持缩写形式。

domain_name

该参数指定 DNS 域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

ttl

可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date

可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action

可选参数，指定资源记录过期时的处理动作，取值必须为：

- block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。
- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record mx <record_name> <domain_name1> <domain_name2>
<priority> [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 MX 资源记录，并为该资源记录定义名称。MX 资源记录用于将以该域名 (domain_name1) 为结尾的电子邮件指向对应的邮件服务器 (domain_name2) 进行处理。该命令还可以用于修改已有资源记录的邮件服务器所在域、邮件服务器的域名、优先级和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为 “all”。
- 由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name1 该参数指定邮件服务器所在的域。

domain_name2 该参数指定邮件服务器的域名。

priority 该参数指定 MX 资源记录的优先级，取值必须为 0 至 65535 之间的整数，数字越小，优先级越高。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date 可选参数，该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式，其中，“yyyy” 表示年份，“mm” 表示月份，而 “dd” 表示日。比如：“20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action 可选参数，指定资源记录过期时的处理动作，取值必须为：

- block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。
- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record srv <record_name> <domain_name> <target_server>
<target_port> <priority> <weight> [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名创建一条 SRV 记录，并为该资源记录定义名称。该命令还可以用于修改已有记录的目标服务器、目标服务器端口、优先级、权重和 TTL。

record_name	该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。 注意： 参数取值不能为 “all”。 由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。
domain_name	该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。
target_server	该参数指定 SRV 记录的目标服务器域名，取值必须是长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。
target_port	该参数指定目标服务器的端口。取值必须为 0 到 65,535 之间的整数。
priority	该参数指定 SRV 资源记录的优先级，取值必须为 0 至 65,535 之间的整数，数字越小，优先级越高。
weight	该参数指定 SRV 记录的权重。取值必须为 0 到 65,535 之间的整数。
ttd	可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。
expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式，其中，“yyyy” 表示年份，“mm” 表示月份，而 “dd” 表示日。比如：“20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： • block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 • delete: 表示系统将删除该资源记录。 默认值为 block。

```
sdns record soa <record_name> <domain_name> <master_server>  
<email_contact> <serial_number> [refresh_interval] [retry_interval]  
[expiration_interval] [negative_ttl] [ttl] [expiration_date] [expiration_action]
```

该命令用于为指定的域名创建一条 SOA 记录，并为该资源记录定义名称。该命令还可以用于修改已有记录的主服务器、邮箱、序列号、刷新闻隔、重试间隔、过期间隔、最小 TTL 和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

参数取值不能为 “all”。

由于 “IP 地址_” 前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name 该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。

master_server 该参数指定 SOA 记录的主服务器域名，取值必须是长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。

email_contact 该参数指定 SOA 记录的邮箱，取值必须是长度不超过 128 个字节的字符串，格式为 “xyz.com”，不能以 “.” 结束。

serial_number 该参数指定 SOA 记录的序列号。取值必须为 0 到 4,294,967,295 之间的整数。

refresh_interval 可选，该参数指定 SOA 记录的刷新闻隔，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数。默认值为 3,600。

retry_interval 可选，该参数指定 SOA 记录的重试间隔，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数。默认值为 1,800。

expiration_interval 可选，该参数指定 SOA 记录的过期间隔，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数。默认值为 1,209,600。

negative_ttl 可选参数，该参数指定失败的 DNS 查询对应的 SOA 记录的生存时间，单位为秒。取值必须为 0 到 4294967295 之间的整数。默认值为 86,400。

ttl	可选参数，该参数指定成功的 DNS 查询对应的 SOA 资源记录的生存时间，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。
expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： • block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 • delete: 表示系统将删除该资源记录。 默认值为 block。

sdns record txt <record_name> <domain_name> <description1>
[description2] [description3] [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 TXT 资源记录，并为该资源记录定义名称。TXT 资源记录是基于文本的 DNS 记录，以 TXT 的格式存储于 DNS 区域文件中，用于检索有关域名的信息。

一个 DNS 区域支持配置多条 TXT 资源记录，不支持为 PTR 类型的 DNS 区域添加 TXT 资源记录。

要使 TXT 资源记录生效，管理员需要在 DNS 区域里面添加至少有一个 NS 记录和一个 A/AAAA 记录。并且仅当 DNS 区域内 NS/MX 记录的域名与 A/AAAA 域名相同时，才能向区域中添加 A/AAAA 记录。使用 TXT 记录功能前需要启用 SDNS 功能（通过命令“sdns on”）以及 SDNS 全域名功能（通过命令“sdns fulldns on”）。该命令还可以用于修改已有资源记录域名、内容和 TTL。

record_name	该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。 注意： • 参数取值不能为“all”。 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。
domain_name	该参数指定 TXT 资源记录对应的域名，取值必须为长度不超过 128 个字节的字符串，格式为“xyz.com”。

	注意: 该参数必须为 DNS 区域名称(通过命令“sdns zone name”) 或者为 DNS 区域的子域, 支持多级子域名。
description1	该参数指定 TXT 记录的内容, 取值必须为长度 1-200 个字节的字符串(空格也是字符, 其长度也计算在内)。取值支持数字、大小写字母和特殊字符。当取值只包含数字或包含特殊字符时, 必须置于双引号内。 该参数仅支持以下特殊字符: “.”、“*”、“/”、“-”、“:”、“_”、“?”、“=”、“@”、“,”、“\”、“ ”。 注意: • 当参数取值为包含 “\单个数字” 的字符串 (这里的单个数字指 0 到 9), 会导致该 DNS 区域包含该配置在内的后续所有配置都不生效。重启 SDNS 服务后, 该 DNS 区域内的所有配置仍然不生效, 只有删除该配置, SDNS 才能正常工作。所以推荐用户不要将参数取值配置为包含 “\单个数字” 的字符串。 • 参数不能以 “\” 结尾。
description2	可选, 该参数指定 TXT 记录的内容。具体描述见参数 “description1”。默认值为空。 注意: 当参数 “description3” 不为空时, 该参数取值也不能为空, 即: 不可以执行命令 “sdns record txt txt1 www.abc.com “d1” “” “d3””。
description3	可选, 与参数 “description2” 的取值一致。
ttl	可选参数, 该参数指定资源记录的 TTL, 单位为秒。取值必须为 0 到 4,294,967,295 之间的整数, 默认值为 86,400。
expiration_date	可选参数, 该参数指定资源记录的失效日期。取值必须为 “yyyymmdd” 格式, 其中, “yyyy” 表示年份, “mm” 表示月份, 而 “dd” 表示日。比如: “20100129” 表示 2010 年 1 月 29 日。其中 “yyyy” 的取值应该为 2,000 至 2,037 之间的整数。默认值为空, 表示永不到期。
expiration_action	可选参数, 指定资源记录过期时的处理动作, 取值必须为: • block: 表示系统将禁用该资源记录, 即该资源记录在解除禁用前将不能再使用。

- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record spf <record_name> <domain_name> <description> <ttl>
<expiration_date> <expiration_action>

该命令用于为指定的域名添加一条 SPF 资源记录，SPF 记录用于指定一个域名允许哪些 IP 地址或邮件服务器发送电子邮件。这意味着，如果某个邮件服务器不是授权的服务器之一，当该服务器试图以该域名发送邮件时，接收服务器就可以识别并拒绝该邮件，从而避免伪造邮件和垃圾邮件。该命令还可以用于修改已有记录的域名、内容和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name 该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

description 该参数指定 SPF 记录的内容，取值必须为长度不大于 600 个字节的字符串。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date 可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。

expiration_action 可选参数，指定资源记录过期时的处理动作，取值必须为：

- block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。

- delete: 表示系统将删除该资源记录。

默认值为 block。

sdns record ds <record_name> <domain_name> <key_tag> <algorithm>
<digest_type> <digest> [ttl] <expiration_date> <expiration_action>

该命令用于为指定的域名添加一条 DS 资源记录，DS 资源记录是 DNSSEC 协议中的一种记录类型，用于支持 DNS 区域的数字签名和验证。它用于在父域与子域之间的 DNS 安全委托，确保 DNS 数据的完整性和真实性。DS 记录是 DNSSEC 中的一个重要组成部分，帮助验证 DNS 数据是否未被篡改。该命令还可以用于修改已有记录的域名、密钥标记、密钥算法、摘要和 TTL。

record_name 该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name 该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

ket_tag 该参数指定密钥标记，取值必须为 0 到 65,535 之间的整数。

algorithm 该参数指定密钥算法。取值必须为 0 到 255 之间的整数。

digest_type 该参数指定摘要类型，取值必须为：

- 1: 表示 SHA-1 摘要类型。
- 2: 表示 SHA-256 摘要类型。

digest 该参数指定摘要。

- SHA-1 摘要类型需要 20 字节的摘要值长度。
- SHA-256 摘要类型需要 32 字节的摘要值长度。

ttl 可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。

expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示2010年1月29日。其中“yyyy”的取值应该为2,000至2,037之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： • block：表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 • delete：表示系统将删除该资源记录。 默认值为 block。

sdns record naptr <record_name> <domain_name> <order> <preference> [flags] [service] [regexp] [replacement] [ttl] [expiration_date] [expiration_action]

该命令用于为指定的域名添加一条 NAPTR 资源记录，NAPTR 记录允许 DNS 服务器根据某个查询返回相关的服务信息，特别是在需要根据一个标识符查找服务的场景中，NAPTR 通常用于将一个服务的请求映射到一个特定的 URI，端口或协议。该命令还可以用于修改已有记录的域名、顺序、权重、标志、服务、正则表达式和 TTL。

record_name	该参数指定资源记录名称，取值必须为长度不大于 128 个字节的字符串。

注意：

- 参数取值不能为“all”。
- 由于“IP 地址_”前缀用于 DNS 区域主从同步，所以该参数取值不能包含该前缀。

domain_name	该参数指定域名，取值必须长度不超过 128 个字节的字符串，格式为“xyz.com”，不能以“.”结束。

order	该参数指定 NAPTR 记录的顺序。顺序按照数值从小到大排序。取值必须为 0 到 65,535 之间的整数。

preference	该参数指定参数“order”值相同的 NAPTR 记录的权重，数值越小的记录权重越大。取值必须为 0 到 65,535 之间的整数

flags	可选参数，该参数指定包含控制记录字段重写和解释方面的标志。标志是来自集合[A-Z]和[0-9] 的单个字符。目前仅支持“S”、“A”、“U”、“P”和“”，不区分大小写。 “S”标志：表示下一个查找的应该是 SRV 记录。 “A”标志：表示下一个查找的应该是 A、AAAA 或 A6 记录。 “U”标志：表示下一步不是 DNS 查找，而是 Regexp 字段的输出是一个 URI。 “P”标志：表示应用程序侧算法的其余部分应以特定协议的方式进行。新的规则集为参数 services 字段中指定的协议标识。 “空”：参数 replacement 指向的是另外一个 NAPTR 记录。 默认值为空。
service	可选参数，该参数指定在 NAPTR 记录中用于指定沿着重写路径可用的服务，以及与这些服务通信时使用的特定协议。取值为不超过 255 个字节的字符串。该参数默认值为空。常见的标识符如下所示： - E2U：表示 E.164 到 URI 的映射。 - I2L：表示从标识符到定位器的映射。 - I2C：表示从标识符到联系信息的映射。 - I2R：表示从标识符到资源的映射。 - z3950：表示 Z39.50 协议。 - rcds：表示 RCDS 协议。 - http：表示 HTTP 协议。 - sip：表示 SIP 协议。 - tcp：表示 TCP 协议。 - udp：表示 UDP 协议。
regexp	可选参数，该参数指定原域名替换的正则表达式，根据原域名生成新域名或 URI 规则。取值为长度不超过 255 个字节的字符串。当参数取值和 参数“replacement”取

值都不为空时，NAPTR 记录会先使用正则表达式匹配输入的字符串，如果匹配成功，则将匹配的部分替换成参数“replacement”指定的内容，从而实现对请求的重定向或转换。默认值为空。

replacement	可选参数，该参数指定下一个要查询的域名，该域名必须是一个完全合格的域名。具体查询的记录类型（NAPTR、SRV 或地址记录）取决于参数“flags”的值。取值必须为长度不超过 128 字节的字符串。默认值为“.”。
ttd	可选参数，该参数指定资源记录的 TTL，单位为秒。取值必须为 0 到 4,294,967,295 之间的整数，默认值为 86,400。
expiration_date	可选参数，该参数指定资源记录的失效日期。取值必须为“yyyymmdd”格式，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。其中“yyyy”的取值应该为 2,000 至 2,037 之间的整数。默认值为空，表示永不到期。
expiration_action	可选参数，指定资源记录过期时的处理动作，取值必须为： • block: 表示系统将禁用该资源记录，即该资源记录在解除禁用前将不能再使用。 • delete: 表示系统将删除该资源记录。 默认值为 block。

sdns record enable <record_name>

该命令用于启用一条资源记录。

sdns record disable <record_name>

该命令用于禁用一条资源记录。

sdns record checkinterval [interval]

该命令用于设置资源记录过期天数检测的时间间隔。

interval	可选参数，该参数指定资源记录过期天数检测的时间间隔，单位为分钟。取值必须为 1 至 1440 之间的整数。默认值为 1440。

no sdns record <record_name>

该命令用于删除指定的资源记录。

show sdns record [record_name]

该命令用于显示特定已添加的资源记录。如果不指定参数“record_name”，则显示所有的已添加的资源记录。

clear sdns record all

该命令用于清除所有已添加的资源记录。

13.13 DNS 区域

13.13.1 基本设置

sdns zone name <zone_name> [zone_type] [view_name]

该命令用于在指定 SDNS 视图下创建一个 DNS 区域。

zone_name 该参数指定 DNS 区域名称，取值必须为一个 DNS 域名或 IP 前缀，长度不大于 128 个字节。取值为域名时，字符串中由“.”分隔的各部分长度不能超过 63 个字符。非 PTR 类型的 DNS 区域必须使用域名定义，例如“www.a.com”。PTR 类型的 DNS 区域必须使用 IP 前缀定义，如果使用 IPv4 前缀，必须为点分十进制格式，以点号（“.”）结尾，例如“10.8.6.”；如果使用 IPv6 前缀，必须为冒号分隔的十六进制格式，以冒号结尾（“:”），例如“fff:”。

zone_type 可选，该参数指定 DNS 区域的类型，取值不区分大小写，取值必须为：

- MASTER：表示主要区域。
- SLAVE：表示辅助区域。
- STUB：表示存根区域。
- STATICSTUB：表示静态存根区域。

默认值为“MASTER”。

view_name 可选，该参数指定已存在的视图名称。默认值为“default”。

no sdns zone name <zone_name> [view_name]

该命令用于删除指定 SDNS 视图下的指定 DNS 区域。如果不指定参数“view_name”，系统将删除“default”视图下的 DNS 区域。

show sdns zone name [view_name]

该命令用于显示指定 SDNS 视图下的 DNS 区域。如果不指定参数“view_name”，则显示所有 SDNS 视图下的 DNS 区域。

clear sdns zone name all

该命令用于清除所有的 DNS 区域。

clear sdns zone name view <view_name>

该命令用于清除指定 SDNS 视图下所有的 DNS 区域。

sdns zone record <zone_name> <record_name> [view_name]

该命令用于将指定的资源记录添加到指定 SDNS 视图的指定 DNS 区域。每个 DNS 区域必须包含至少一个 NS、一个 A 或一个 AAAA 资源记录。

zone_name	该参数指定已存在的 DNS 区域名称。
record_name	该参数指定已存在的 DNS 资源记录名称，添加到 DNS 区域内的资源记录必须为 DNS 区域的子域名或者子网掩码更长的 IP 地址。
view_name	可选，该参数指定已存在的 SDNS 视图的名称，如果不指定该参数，系统将添加指定资源记录到“default”视图下的 DNS 区域。默认值为“default”。



注意：如果在 PTR 类型的 DNS 区域里添加 NS 资源记录，定义该 NS 资源记录的“sdns record ns”命令中“domain_name1”参数的值必须和 DNS 区域名称一致。

no sdns zone record <zone_name> <record_name> [view_name]

该命令用于从指定 SDNS 视图的 DNS 区域里删除一条资源记录。如果不指定参数“view_name”，系统将从“default”视图的 DNS 区域里删除一条资源记录。

show sdns zone record [zone_name] [view_name]

该命令用于显示指定的 DNS 区域包含的资源记录。

zone_name	可选，该参数指定已存在的 DNS 区域名称。如果不指定该参数，取值为“all”，系统将显示所有 DNS 区域包含的资源记录。 默认值为“all”。

view_name 可选，该参数指定已存在 SDNS 视图的名称。如果不指定该参数，取值为“all”，系统将显示所有 SDNS 视图包含的资源记录。

默认值为“all”。

clear sdns zone record <zone_name> [view_name]

该命令用于清除指定 SDNS 视图中指定区域包含的资源记录。

zone_name 可选，该参数指定已存在的 DNS 区域名称。如果不指定该参数，取值为“all”，系统将清除所有 DNS 区域包含的资源记录。默认值为“all”。

view_name 可选，该参数指定已存在 SDNS 视图的名称。如果不指定该参数，取值为“all”，系统将清除所有 SDNS 视图包含的资源记录。默认值为“all”。

sdns zone tsigkey <tsigkey_name> <algorithm> [secret]

该命令用于配置 TSIG（Transaction Signature，事务签名）密钥。TSIG 是一种用于保护 DNS 消息安全的机制，主要用于区域传输、动态更新和其他 DNS 消息之间的身份验证和完整性保护。TSIG 使用共享的密钥和哈希算法对 DNS 消息进行签名和验证，从而确保消息的真实性和完整性。设备支持配置最多 1,000 个 TSIG 密钥。

name 该参数指定 TSIG 密钥的名称，取值必须为长度不大于 128 个字节的字符串。

algorithm 该参数指定 TSIG 密钥的算法，取值必须为“hmac-md5”、“hmac-sha1”或“hmac-sha256”。

secret 可选，该参数指定 TSIG 密钥的内容。默认值为空，表示自动生成 TSIG 密钥。

no sdns zone tsigkey <tsigkey_name>

该命令用于删除指定的 TSIG 密钥。

show sdns zone tsigkey

该命令用于显示全部的 TSIG 密钥配置。

clear sdns zone tsigkey

该命令用于清除全部的 TSIG 密钥配置。

sdns nameserver name <ns_name> <ns_ip_address> [port] [tsigkey_name]

该命令用于创建一个远端 SDNS 域名服务器。设备允许配置最多 1,000 个远端域名 SDNS 服务器。

ns_name	该参数指定远端 SDNS 域名服务器的名称。
ns_ip_address	该参数指定远端 SDNS 域名服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。
port	可选，该参数指定远端 SDNS 域名服务器的端口。取值必须为 0 到 65,535 之间的整数。 默认值为 53。
tsigkey_name	可选，该参数指定已存在的 TSIG 密钥名称。 默认值为空。

no sdns nameserver name <ns_name>

该命令用于删除指定的远端 SDNS 域名服务器配置。

show sdns nameserver name

该命令用于显示全部的远端 SDNS 域名服务器配置。

clear sdns nameserver name

该命令用于清除全部的远端 SDNS 域名服务器配置。

sdns zone nameserver <zone_name> <ns_name> [view_name]

该命令用于为指定的 DNS 区域配置域名服务器。一个视图下的一个区域支持添加最多 5 个域名服务器。

- 当区域类型为主要区域时，该命令用于配置主要区域的辅助域名服务器；
- 当区域类型为辅助区域时，该命令用于配置辅助区域的主要域名服务器；
- 当区域类型为存根区时，该命令用于配置存根区域的主要域名服务器；
- 当区域类型为静态存根区时，该命令用于配置静态存根区的域名服务器。

zone_name	该参数指定已存在的 DNS 区域名称。
ns_name	该参数指定已存在的远端 SDNS 域名服务器名称。
view_name	可选，该参数已存在的视图名称。默认值为“default”。

no sdns zone nameserver <zone_name> <ns_name> [view_name]

该命令用于删除指定视图下指定 DNS 区域的域名服务器，如果未配置参数“view_name”，则删除“default”视图下指定 DNS 区域的域名服务器。

show sdns zone nameserver [zone_name] [view_name]

该命令用于显示指定视图下指定 DNS 区域的域名服务器配置。

- zone_name 可选。该参数指定已存在的 DNS 区域名称。
- 如果指定该参数，系统将显示指定 DNS 区域的域名服务器配置。
 - 如果不指定该参数，即参数为空，系统将显示所有 DNS 区域的域名服务器配置。

默认值为空。

- ns_name 可选。该参数已存在的视图名称。
- 如果指定该参数，系统将显示指定视图下的域名服务器配置。
 - 如果不指定该参数，即参数为空，系统将显示所有视图下的域名服务器配置。

默认值为空。

clear sdns zone nameserver [zone_name] [view_name]

该命令用于清除指定视图下指定 DNS 区域的域名服务器配置。

- zone_name 可选。该参数指定已存在的 DNS 区域名称。
- 如果指定该参数，系统将清除指定 DNS 区域的域名服务器配置。
 - 如果不指定该参数，即参数为空，系统将清除所有 DNS 区域的域名服务器配置。

默认值为空。

- ns_name 可选。该参数已存在的视图名称。
- 如果指定该参数，系统将清除视图下的域名服务器配置。
 - 如果不指定该参数，即参数为空，系统将清除所有视图下的域名服务器配置。

默认值为空。

13.13.2 SDNS 转发

sdns zone forward name <zone_name> <nameserver> [view_name]

该命令用于为指定 SDNS 视图下的 DNS 区域配置 SDNS 转发功能。配置命令后，系统将转发匹配指定区域的 DNS 请求，不进行本地解析。

zone_name	该参数指定已存在的 DNS 区域的名称。该参数取值支持“空”，表示全局转发，系统将对所有静态域名都进行转发。
nameserver	该参数指定域名服务器的 IP 地址和端口。其中，IP 地址取值必须为 IPv4 或 IPv6 地址，端口取值必须为 0 到 65,535 之间的整数，若不指定端口，默认端口为 53。该参数的格式为“IP 地址 1%端口 1,IP 地址 2%端口 2”，例如：“1.1.1.1%53, 2.2.2.2, 2001:4860:4860::8888%666”。该参数支持最多配置 5 个域名服务器。
view_name	可选，该参数指定已存在的 SDNS 视图的名称。如果不指定该参数，则为“default”视图下的 DNS 区域配置 SDNS 转发功能。默认值为“default”。

no sdns zone forward name <zone_name> [view_name]

该命令用于删除指定 SDNS 视图下 DNS 区域的 SDNS 转发功能的配置。如果不指定参数“view_name”，则删除“default”视图下 DNS 区域的 SDNS 转发功能的配置。

show sdns zone forward name [view_name]

该命令用于显示指定 SDNS 视图下 DNS 区域配置的 SDNS 转发功能的配置。如果不指定参数“view_name”，则显示所有 SDNS 视图下 DNS 区域的 SDNS 转发功能的配置。

clear sdns zone forward name

该命令用于清除为所有的 DNS 区域配置的 SDNS 转发功能的配置。

clear sdns zone forward view <view_name>

该命令用于清除指定 SDNS 视图下 SDNS 转发功能的配置。

sdns zone forward enable <zone_name>

该命令用于为指定的 DNS 区域启用 SDNS 转发功能。DNS 区域的 SDNS 转发功能默认是启用的。

`zone_name` 该参数指定已存在的 DNS 区域的名称。

sdns zone forward disable <zone_name>

该命令用于为指定的 DNS 区域禁用 SDNS 转发功能。DNS 区域的 SDNS 转发功能默认是启用的。

`zone_name` 该参数指定已存在的 DNS 区域的名称。

show sdns zone forward disable

该命令用于显示全部被禁用的 SDNS 转发区域。

show sdns zone forward status [zone_name]

该命令用于显示指定 DNS 区域的 SDNS 转发功能的状态。如果不指定参数“zone_name”，将显示所有 DNS 区域的 SDNS 转发功能的状态。

13.14 SDNS 全域名

sdns fulldns {on|off}

该命令用于启用或禁用 SDNS 全域名功能。该功能的默认设置为启用。

禁用该功能后，系统仅支持解析 A、AAAA、CNAME 和 DNSKEY 类型的域名，对于无法解析的域名，系统会回复错误码。

启用该功能后，系统支持解析所有类型的域名。对于无法解析的域名，如果配置了“sdns recursion on”，系统会将请求转发给 BIND 服务器解析。

sdns recursion {on|off}

该命令用于启用或禁用 SDNS 递归查询功能。该功能仅在启用了 SDNS 全域名功能后生效。默认情况下，该功能是禁用的。

sdns recursion randport [min_port] [max_port]

该命令用于配置 SDNS 递归或转发的源端口范围。如果不配置该命令，系统默认的最小源端口为 32,768，最大源端口为 60,999。

`min_port` 可选。该参数指定 SDNS 递归或转发的最小源端口，取值必须为 1,024 到 65,535 的整数。

默认值为 32,768。

`max_port` 可选。该参数指定 SDNS 递归或转发的最大源端口，取

值必须为 1,024 到 65,535 的整数，取值不能小于参数“min_port”。

默认值为 60,999。



注意：端口范围应避免系统保留端口和其他应用可能使用的端口，以避免端口冲突。

show sdns recursion randport

该命令用于显示 SDNS 递归或转发的源端口范围。

clear sdns recursion randport

该命令用于恢复 SDNS 递归或转发的源端口范围为缺省配置。

sdns recursion randid on

该命令用于启用 SDNS 递归或转发的随机事务 ID 功能。启用该功能后，设备的 DNS 解析的随机事务 ID 是随机的。该功能默认启用且不能被禁用。

show sdns recursion randid

该命令用于显示 SDNS 递归或转发的随机事务 ID 功能的启用状态。

sdns recursion root server <root_server_ip>

该命令用于定义一个根节点服务器。系统支持最多 16 个根节点服务器。

root_server_ip 该参数指定根节点服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。



注意：自定义根节点服务器后，13 个公网根服务器会被禁用，防止自定义根节点与公网结果不一致，导致冲突。

no sdns recursion root server <root_server_ip>

该命令用于删除指定的根节点服务器。

show recursion root server

该命令用于显示全部根节点服务器。

clear sdns recursion root server

该命令用于清除全部根节点服务器。

sdns recursion timeout [recursion_timeout]

该命令用于设置递归超时时间。在指定的递归超时时间内如果客户端未收到响应，则中断连接。

recursion_timeout 可选，该参数指定递归超时时间。取值必须为 10,000 到 30,000 之间的整数。默认值为 10,000，单位为毫秒。

show sdns recursion timeout

该命令用于显示设置的递归超时时间。

sdns recursion aggregation [aggregation_num]

该命令用于设置递归聚合的聚合数量。

aggregation_num 可选，该参数指定递归聚合的聚合数量。取值必须为 0 到 4,294,967,295 之间的整数。默认取值为 0，表示不进行递归聚合。

show sdns recursion aggregation

该命令用于显示设置的递归聚合的聚合数量。

sdns view name <view_name> <priority>

该命令用于创建一个 SDNS 视图，用于为不同的 DNS 查询来源配置不同的 DNS 解析策略。系统默认会创建一个“default”视图，该视图不可删除和修改。

该命令还可以用于修改已有 SDNS 视图的优先级。

view_name 该参数指定 SDNS 视图的名称。取值必须为长度不大于 128 个字节的字符串。

priority 该参数指定 SDNS 视图的优先级。取值必须为 1 到 65,535 之间的整数。参数值越大，优先级越高。

设备上支持的“sdns view name”条目的最大数量取决于系统内存的大小，如下表所示。

表 19 - 3 “sdns view name”条目最大数量

系统内存	“sdns view name”条目最大数量
大于等于 4GB 并且小于 32 GB	5,000
大于等于 32GB 并且小于 128 GB	10,000
大于等于 128 GB	20,000

no sdns view name <view_name>

该命令用于删除指定的 SDNS 视图。

show sdns view name

该命令用于按照优先级顺序显示所有的 SDNS 视图。

clear sdns view name

该命令用于清除所有的 SDNS 视图。

sdns view acl <view_name> <region_name>

该命令用于为指定 SDNS 视图配置 ACL 规则。配置该命令后，仅源地址匹配该 ACL 规则的请求，可访问 SDNS 视图。如果不配置该命令，默认所有的客户端都可以访问 SDNS 视图。

系统支持为一个 SDNS 视图配置最多 10 条 ACL 规则。

view_name 该参数指定已存在的 SDNS 视图的名称。

region_name 该参数指定源地址所属的 SDNS 区域的名称。取值支持配置为 “none”，表示则该视图下所有资源都不可访问。



注意：“default”视图的 ACL 规则为 “any”，表示所有客户端都可以访问该视图。该规则不可更改。

no sdns view acl <view_name> <region_name>

该命令用于删除指定 SDNS 视图下的 ACL 规则。

show sdns view acl [view_name]

该命令用于显示指定 SDNS 视图下的 ACL 规则。如果不指定参数 “view_name”，显示所有 SDNS 视图下的 ACL 规则。

clear sdns view acl [view_name]

该命令用于清除指定 SDNS 视图下的 ACL 规则。如果不指定参数 “view_name”，清除所有 SDNS 视图下的 ACL 规则。

sdns zone acl query <zone_name> <region_name> [view_name]

该命令用于为指定 SDNS 视图下的指定 DNS 区域配置一条 ACL 规则。如果没有为 DNS 区域配置 ACL 规则，则允许所有客户端访问。对于同一个视图下的一个 DNS 区域，系统支持配置最多 10 条 ACL 规则。

zone_name 该参数用于已存在的 DNS 区域的名称。

region_name 该参数指定客户端源地址所属的 SDNS 区域的名称。

view_name 可选，该参数指定 SDNS 视图的名称。如果不指定该参数，则表示为 “default” 视图下指定 DNS 区域配置 ACL 规则。默认值为 “default”。

no sdns zone acl query <zone_name> <region_name> [view_name]

该命令用于删除指定 SDNS 视图下指定 DNS 区域的一条 ACL 规则。如果不指定参数 “view_name”，则删除 “default” 视图下指定 DNS 区域的一条 ACL 规则。

show sdns zone acl query [zone_name] [view_name]

该命令用于显示指定 SDNS 视图的指定 DNS 区域的 ACL 规则。

zone_name	可选，该参数指定已存在的 DNS 区域名称。如果不指定该参数，则表示显示所有 DNS 区域的 ACL 规则。默认值为空。
view_name	可选，该参数指定已存在的 SDNS 视图的名称，如果不指定该参数，则表示显示所有视图下的 ACL 规则。默认值为空。

clear sdns zone acl query [zone_name] [view_name]

该命令用于清除指定 SDNS 视图下指定 DNS 区域的所有 ACL 规则。

zone_name	可选，该参数指定已存在的 DNS 区域名称。如果不指定该参数，则表示清除所有 DNS 区域的 ACL 规则。默认值为空。
view_name	可选，该参数指定已存在的 SDNS 视图的名称，如果不指定该参数，则表示清除所有视图下的 ACL 规则。默认值为空。

**sdns view record sort <view_name> <region_name> <region2_name>
<priority>**

该命令用于为指定 SDNS 视图配置资源记录排序规则。一个 SDNS 视图下最多配置 100 条资源记录排序规则。

- 如果配置了该规则，在指定 DNS 区域的 ACL 规则（通过命令“**sdns zone acl query**”配置）匹配成功后，系统会继续匹配该资源记录排序规则，即首先将客户端源地址与参数“region_name”进行匹配，如果匹配，再继续将静态资源记录的 IP 地址与参数“region2_name”进行匹配。匹配该规则成功后，系统会返回该静态资源记录。
- 如果未配置该规则，在 ACL 规则匹配成功后，系统会直接返回资源记录。

view_name	该参数指定已存在的 SDNS 视图的名称。
region_name	该参数指定请求源地址所属的 SDNS 区域名称。
region2_name	该参数指定作为响应返回的静态资源记录的地址所属的 SDNS 区域名称。
priority	该参数指定资源记录排序的优先级。取值必须为 0 到 65,535 之间的整数。该值越大，优先级越高。

no sdns view record sort <view_name> <region_name> <region2_name>

该命令用于为指定 SDNS 视图删除指定的资源记录排序规则。

show sdns view record sort [view_name]

该命令用于显示指定 SDNS 视图的资源记录排序规则的配置。如果不指定参数“view_name”，则默认显示所有 SDNS 视图下的资源记录排序规则。

clear sdns view record sort [view_name]

该命令用于清除指定 SDNS 视图的资源记录排序规则配置。如果不指定参数“view_name”，默认清除所有 SDNS 视图下的资源记录排序规则。

13.15 RPZ 防火墙

sdns rpz record <rpz_record_name> <type> <src><action> [local_data]

该命令用于添加一条 RPZ（Response Policy Zone）记录。RPZ 记录包括 RPZ 触发器和 RPZ 动作。配置该命令后，如果收到的 DNS 请求匹配配置的 RPZ 记录，则系统会根据配置对请求或响应进行拦截，并执行相应的 RPZ 动作。系统支持添加最多 100 条 RPZ 记录。

该命令还可以用于修改已有 RPZ 记录的触发器类型、触发器取值、RPZ 的动作、自定义解析结果。

rpz_record_name 该参数指定 RPZ 记录的名称。取值必须为长度不大于 128 字节的字符串。

type 该参数指定 RPZ 触发器的类型。取值必须为：

- “Client IP Address”：表示用于匹配发起请求的客户端 IP 地址，支持 IPv4 和 IPv6。在 RPZ 记录输出显示中该触发器以.rpz-client-ip 结尾。
 - 对于 IPv4 地址段，假如 IPv4 地址为“B1.B2.B3.B4/prefix”，在 RPZ 记录的书写格式中显示为“prefix.B4.B3.B2.B1”；
 - 对于 IPv6 地址段，假如 IPv6 地址为“B1:B2:B3:B4:B5:B6:B7:B8/prefix”，在 RPZ 记录的书写格式中显示为“prefix.B8.B6.B6.B5.B4.B3.B2.B1”。如同 IPv6 地址中可以使用双冒号进行缩写，在 RPZ 记录的书写格式中 IPv6 地址的省略部分也可以被 zz 代替，如“2001::6:180/128”会被表示为“128.180.6.zz.2001”。
- “QDNAME”：表示用于匹配请求或响应报文请求

记录中域名字段的域名（可带通配符）。例如触发器为“*.array.com”，当请求记录中域名字段包含“array.com”时，将会触发 RPZ 触发器。

- “Response IP Address”：表示用于匹配响应报文应答记录中 IP 地址字段的 IP 地址。在 RPZ 记录输出显示中该触发器以“.rpz-ip”结尾。支持 IPv4 和 IPv6。IP 地址段的格式与“Client IP Address”中描述一致。
- “NSDIP”：表示用于匹配响应报文附加资源记录中 NS（权威域名服务器）的 IP 地址。在 RPZ 记录输出显示中该触发器以“.rpz-nsdip”结尾。例如 RPZ 记录格式的触发器“24.0.49.101.180.rpz-nsdip”，当响应报文中包含的 NS 记录对应的 IP 地址为 180.101.49.0/24 网段时，可以触发 RPZ 触发器。
- “NSDNAME”：表示用于匹配响应报文应答记录中 NS（权威域名服务器）的名字。在 RPZ 记录输出显示中该触发器以“.rpz-nsdname”结尾。例如 RPZ 记录格式的触发器“ns.example.com.rpz-nsdname”，当响应报文中包含“ns.example.com”的 NS 记录时，可以触发 RPZ 触发器。

src 该参数指定 RPZ 触发器的取值。取值必须为域名或网段。

action 该参数指定 RPZ 的动作。取值必须为：

- “NXDOMAIN”：表示系统回复 NXDOMAIN 类型的响应。
- “NODATA”：表示系统回复 NODATA 类型（rcode 为 noerror，但应答服务个数为 0）的响应。
- “PASSTHRU”：表示透传，即该记录列入 RPZ 白名单，不对客户端请求做 RPZ 处理。
- “DROP”：表示丢弃，即系统对客户端请求不做响应。
- “TCPACTION”：表示系统将响应报文中 TC 标志置为 1，强制客户端发起 TCP 类型的 DNS 请求，用于攻击防护。
- “LOCALDATA”：表示系统回复管理员自定义配

置的解析结果。

local_data 可选，该参数用于指定自定义解析结果。取值必须为网段、域名或空。只有当参数“action”取值为“LOCAL DATA”时，可设置此参数。该参数默认取值为空。

例如：

```
Demo(config)#sdns rpz record r1 "Client IP Address" "10.210.0.111/32" "DROP"
```

以上命令配置表示配置一条 RPZ 记录。触发器类型为客户端 IP 地址；触发器的取值为 10.210.0.111/32 网段；RPZ 的动作为 DROP，即丢弃 IP 为 10.210.0.111/32 网段的客户端发送到设备的 DNS 请求报文。

no sdns rpz record <rpz_record_name>

该命令用于删除指定的 RPZ 记录。

show sdns rpz record [rpz_record_name]

该命令用于显示指定的 RPZ 记录。如果不指定参数“rpz_record_name”，则显示所有 RPZ 记录。

clear sdns rpz record

该命令用于清除所有 RPZ 记录。

13.16 SDNS DNSSEC

sdns dnssec {on|off}

该命令用于为 SDNS 启用或禁用 DNSSEC 功能。该功能默认为关闭。



注意：SDNS DNSSEC 功能目前只支持对 A 和 AAAA 类型的资源记录进行加密，暂不支持对 CNAME 资源记录的加密。

sdns dnssec keygen <host_name> <type> [algorithm] [size]

该命名用于为指定 SDNS 域名生成 ZSK（Zone Signing Key，根区签名密钥）或 KSK（Key Signing Key，根区密钥签名密钥）签名密钥。ZSK 将对所有的资源记录进行签名，KSK 只对 ZSK 进行签名。

host_name 该参数指定一个已存在的 SDNS 域名。生成 ZSK 或者 KSK 将该域名的 DNS 资源记录进行加密。

type 指定生成的签名密钥的类型。取值必须为：

	• ZSK: 根区签名密钥 • KSK: 根区密钥签名密钥
algorithm	可选参数, 指定签名密钥所采用的签名算法。取值必须为: • RSASHA1 • RSASHA256 • NSEC3RSASHA1 默认值为 RSASHA1。
size	该参数指定生成密钥的长度, 单位为位。取值必须为 1024 到 4096 之间的整数。 默认长度为 1024 位。

no sdns dnssec keygen [*host_name*]

该命令用于删除指定 SDNS 域名的 DNSSEC 签名密钥。当不指定域名时, 将删除所有 SDNS 域名的签名密钥。

show sdns dnssec keygen [*host_name*]

该命令用于显示指定 SDNS 域名的 DNSSEC 签名密钥。当不指定 SDNS 域名时, 将显示所有 SDNS 域名的签名密钥。

sdns dnssec keypub <*host_name*> <*type*> <*keyfile_name*> [*rollover_time*] [*expiration_time*] [*TTL*]

该命令用于将 ZSK 或 KSK 签名密钥发布到 DNS 服务器 (设备) 的指定 SDNS 域名根区。签名密钥发布之后, 指定 SDNS 域名的资源记录 (Resource Record) 就可以使用该签名密钥进行签名。

host_name	该参数指定一个已存在的 SDNS 域名。
type	该参数指定生成的签名密钥的类型。取值必须为: • ZSK: 根区签名密钥 • KSK: 根区密钥签名密钥
keyfile_name	该参数指定待发布的签名密钥文件 (可通过 “ show sdns dnssec keygen ” 命令查看)。参数值必须置于双引号内。
rollover_time	可选参数, 指定系统自动更新 ZSK 签名密钥的周期, 单位为天。 默认 ZSK 的更新周期为 25 天。

expiration_time	可选参数，指定 ZSK 签名密钥的失效时间，单位为天。到达失效时间后，系统将自动删除失效的 ZSK 签名密钥。为保证签名密钥的顺利更新，密钥失效时间需大于密钥更新周期。建议将 ZSK 的失效时间设置为 30 天。 默认 ZSK 的失效时间为 30 天。
TTL	可选参数，指定签名密钥的缓存失效时间，单位为分钟。为避免密钥产生冲突，设置的缓存失效时间必须小于“rollover_time”和“expiration_time”参数之间的差值。 默认的缓存失效时间为 60 分钟。

no sdns dnssec keypub [host_name]

该命令用于取消将 ZSK 或 KSK 签名密钥发布到 DNS 服务器(设备)的指定 SDNS 域名根区。如果不指定参数“host_name”，发布到所有 SDNS 域名根区的 ZSK 或 KSK 签名密钥都将被取消。

show sdns dnssec keypub [host_name]

该命令用于显示已发布到 DNS 服务器中指定 SDNS 域名的 ZSK 或 KSK 签名密钥。如果不指定参数“host_name”时，将显示发布到 DNS 服务器所有 SDNS 域名根区的 ZSK 或 KSK 签名密钥。

sdns dnssec zonesign <host_name>

该命令用于对指定 SDNS 域名的资源记录执行签名操作。执行签名操作后，系统将使用签名私钥为每一条资源记录生成对应的 RRSIG 记录。

host_name 该参数指定一个已存在的 SDNS 域名。

no sdns dnssec zonesign [host_name]

该命令用于删除指定 SDNS 域名的所有 RRSIG 签名记录和签名密钥。当不指定 SDNS 域名时，将删除所有 SDNS 域名的 RRSIG 签名记录和所有签名密钥。

show sdns dnssec zonesign [host_name]

该命令用于显示指定 SDNS 域名的资源签名信息。当不指定 SDNS 域名时，将显示所有已执行签名操作的 SDNS 域名。

show sdns dnssec ds import [host_name]

该命令用于显示为指定 SDNS 域名导入的 DS (Delegation Signer, 授权签名者) 文件。DS 文件用于验证签名公钥的合法性，需存放在上级 DNS 服务器中，用于建立 DNSSEC 信任链。当不指定“host_name”参数时，将显示设备上导入的所有 DS 文件。

host_name 可选，该参数指定一个已存在的 SDNS 域名。

show sdns dnssec ds generate [host_name]

该命令用于显示为指定 SDNS 域名生成的 DS (Delegation Signer, 授权签名者) 文件。当不指定 “host_name” 参数时，将显示设备上生成的所有 DS 文件。

host_name 可选，该参数指定一个已存在的 SDNS 域名。

sdns dnssec export ds <filename> <url>

该命令用于将指定 DS 文件导出到指定 URL 地址。

filename 该参数指定需要导出的 DS 文件名称(可通过“**show sdns dnssec ds**”命令查看)。参数值必须置于双引号内。

URL 该参数指定用于储存 DS 文件的 URL 地址(只支持 FTP 地址)。

注意: FTP 类型 URL (ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

sdns dnssec import ds <host_name> <url>

该命令用于从指定 URL 地址导入 DS 文件。

host_name 该参数指定需要导入 DS 文件的对应域名。参数值必须置于双引号内。

URL 该参数指定 DS 文件所在的 URL 地址(只支持 FTP 或 HTTP 地址)。



注意: 导入的 DS 文件暂时不支持再次导出和删除。

sdns dnssec export key <type> <keyfile_name> <url>

该命令用于将签名密钥导出指定 URL 地址。DNSSEC 签名密钥采用公钥加密技术，所以签名密钥在导出时需要分别导出其公钥和私钥。

type 该参数指定签名密钥的类型。取值必须为：

- ZSK: 根区签名密钥
- KSK: 根区密钥签名密钥

keyfile_name 该参数指定待导出的签名密钥名称(可通过“**show sdns dnssec keygen**”命令查看)。参数需置于双引号内。

在签名密钥名称后添加 “.key” 后缀即指定导出其公钥，

添加 “.private” 后缀即指定导出其私钥。例如，要导出名为 “Kwww.xyz.com.+005+46666+zsk+RSASHA1+1024” 的 ZSK 公钥，需将名称指定为 “Kwww.xyz.com.+005+46666+zsk+RSASHA1+1024.key”。

URL 该参数指定签名密钥的 URL 导出地址（只支持 FTP 地址）。

注意: FTP 类型 URL (ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

sdns dnssec import key <type> <keyfile_name> <url>

该命令用于从指定的 URL 地址导入签名密钥。

type 该参数指定签名密钥的类型。取值必须为：

- ZSK: 根区签名密钥
- KSK: 根区密钥签名密钥

keyfile_name 该参数指定待导入的签名密钥文件名。参数值必须置于双引号内。

URL 该参数指定签名密钥的 URL 导入地址（只支持 FTP 和 HTTP 地址）。

注意: FTP 类型 URL (ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

show sdns dnssec all

该命令用于显示所有 SDNS DNSSEC 相关的配置信息。

clear sdns dnssec all

该命令用于删除所有 SDNS DNSSEC 相关的配置。

show sdns dnssec status <host_name>

该命令用于显示指定域名的 DNSSEC 状态信息。

示例：

```
Demo(config)#show sdns dnssec status "www.abc.com"
host status flags: HOST_PUBLISH|HOST_KEY|HOST_SIGN
ttl: 60(s)
zsk key counter: 1
ksk key counter: 1
```

```
ZSK key(1):
    keyfile: Kwww.abc.com.+005+43368+zsk+RSASHA1+1024
    keyid: 43368
    type: ZSK
    algorithm: RSASHA1
    status_flags: KEY_PUBLISH|KEY_SIGN| KEY_TIMER
    ttl: 1(hour)
    ex_time: 2(days)
    ro_time: 1(days)
KSK key(0):
    keyfile: Kwww.abc.com.+005+07177+ksk+RSASHA1+1024
    keyid: 7177
    type: KSK
    algorithm: RSASHA1
    status_flags: KEY_PUBLISH| KEY_SIGN |NO
    ttl: 1(hour)
    ex_time: 30(days)
    ro_time: 25(days)
```

命令行输出信息中的“host status flags”项用来显示指定域名的 DNSSEC 信息，参数含义如下：

- HOST_PUBLISH：表示签名密钥已在该域名中发布。
- HOST_KEY：表示该域名上已存在 DNSKEY 资源记录。
- HOST_SIGN：表示该域名的资源已存在 RRSIG 签名记录。

签名密钥信息中的“status_flags”项的参数含义如下：

- KEY_PUBLISH：表示这个该签名密钥已被发布。
- KEY_SIGN：表示已用该签名密钥执行完签名。
- KEY_TIMER：表示该签名密钥有更新周期。

13.17 SDNS 数据中心同步

sdns dc name <dc_name>

该命令用于定义一个 SDNS 数据中心。系统支持定义最多 64 个数据中心。

dc_name 该参数指定 SDNS 数据中心的名称，取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

no sdns dc <dc_name>

该命令用于删除指定 SDNS 数据中心。

show sdns dc name

该命令用于显示所有 SDNS 数据中心的配置。

例如：

```
Demo(config)#show sdns dc name
sdns dc name "dc1"
sdns dc name "dc2"
```

clear sdns dc name

该命令用于清除指定的 SDNS 数据中心配置。

show sdns dc status [dc_name]

该命令用于显示指定的 SDNS 数据中心所有节点的状态。如不指定参数“dc_name”，则显示所有 SDNS 数据中心的所有节点的状态。

例如：

```
Demo#show sdns dc status
DC Name      DC Type      Resource_Type  Name      IP          Port      Priority  Type      Status
dc1          local        Node           node1     10.210.2.154 65517     255      Local|Master|Center Offline
dc2          remote       Node           node2     10.210.2.110 65517     250      Remote|Center Offline
```

sdns node name <node_name> <dc_name> <priority> <node_ip> [node_port]

该命令用于定义一个 SDNS 数据中心节点，并将其与指定 SDNS 数据中心绑定。设备支持最多定义 64 个 SDNS 数据中心节点，每个数据中心可绑定最多 32 个 SDNS 数据中心节点。

node_name 该参数指定 SDNS 数据中心节点的名称，取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

dc_name 该参数指定已存在的 SDNS 数据中心名称。

priority 该参数指定节点的优先级，取值必须为 0 到 255 之间的整数。取值越大，优先级越高。优先级最高的为主 SDNS 数据中心节点，其余节点为备 SDNS 数据中心节点。每个 SDNS 数据中心节点的优先级必须唯一。

node_ip 该参数指定 SDNS 数据中心节点的 IP 地址。取值可以为 IPv4 或 IPv6 地址。

node_port 可选，该参数指定 SDNS 数据中心节点的监听端口，取值必须为 65,391 至 65,535 之间的整数。

默认值为 65,517。

no sdns node name <node_name>

该命令用于删除指定 SDNS 数据中心节点。

show sdns node name

该命令用于显示所有 SDNS 数据中心节点配置。

SDNS 数据中心节点 SDNS 数据中心节点

clear sdns node name

该命令用于清除所有 SDNS 数据中心节点配置。

show sdns node status [node_name]

该命令用于显示指定的 SDNS 数据中心状态，如不指定参数 “node_name”，则显示所有 SDNS 数据中心的状态。

例如：

Demo#show sdns node status					
Name	IP	Port	Priority	Type	Status
node1	10.210.2.154	65517	255	Local Master Center	Offline
node2	10.210.2.110	65517	250	Remote Center	Offline

sdns node enable <node_name>

该命令用于启用指定 SDNS 数据中心节点，该功能默认为启用。

node_name 该参数指定已存在的 SDNS 数据中心的名称。

注意：参数取值不能为 “all”。

sdns node disable <node_name>

该命令用于禁用指定 SDNS 数据中心节点。

sdns dc proximity <dc_name> <region_name> [relation]

该命令用于将指定 SDNS 数据中心的就近性规则关联到指定 SDNS 区域

dc_name 该参数指定已存在的 SDNS 数据中心。

region_name 该参数指定已存在的 SDNS 区域。

relation 可选，该参数指定就近性规则匹配关系。取值必须和指定的 SDNS 区域的就近性规则匹配关系一致。取值必须为 “is” 或 “not”。默认值为 “is”。

no sdns dc proximity <dc_name> <region_name> [relation]

该命令用于删除指定 SDNS 数据中心的就近性规则和指定 SDNS 区域的关联关系。

show sdns dc proximity

该命令用于显示所有 SDNS 数据中心的就近性规则和 SDNS 区域的关联关系。

clear sdns dc proximity

该命令用于清除所有 SDNS 数据中心的就近性规则和 SDNS 区域的关联关系。

sdns sync status [interval] [timeout]

该命令用于设置 SDNS 数据中心本地节点请求获取其他数据中心节点健康检查实例状态的时间间隔和接收响应报文的超时时间。

interval	可选，该参数指定本地数据中心节点请求获取其他数据中心节点健康检查实例状态的时间间隔，单位为秒，取值必须为 1 至 86,400 之间的整数。默认值为 3。
timeout	可选，该参数指定数据中心本地节点接收其他数据中心节点健康检查实例状态时的超时时间，单位为秒，取值必须为 1 至 86,400 之间的整数。默认值为 2。 注意：该参数的取值必须小于或等于“interval”参数的值。

show sdns sync status

该命令用于显示 SDNS 本地数据中心节点请求获取其他数据中心节点健康检查实例状态的时间间隔和接收响应报文的超时时间。

sdns sync heartbeat [interval] [down_check_times]

该命令用于设置本地数据中心节点向其它数据中心节点发送心跳包的间隔。本地数据中心节点会按照设置的发送间隔，向其它数据中心节点发送心跳包。如果连续多次（由参数“down_check_times”确定）都没收到对端节点的心跳响应，则断开与远端数据中心节点的连接。

interval	可选，该参数指定本地数据中心节点发送心跳包的时间间隔，单位为秒。取值必须为 1 至 10 之间的整数，默认值为 1。
down_check_times	可选，该参数指定连续没有收到远端数据中心节点的心跳响应的次数。取值必须为 3 至 1,000 之间的整数，默认值为 15。

show sdns sync heartbeat

该命令用于显示本地数据中心节点向其他数据中心节点发送心跳包的间隔。

sdns sync config to <dc_name>

该命令用于将本地 SDNS 数据中心的配置同步至指定的远端数据中心。

dc_name	该参数指定远端数据中心名称，取值必须为： • 数据中心名称：表示同步至该数据中心 • all：表示同步至所有远端数据中心的所有节点，取值为“all”时，参数“node_ip”不生效。
node_ip	可选，该参数指定远端数据中心节点 IP，取值必须为： • IP：表示同步至指定数据中心的指定节点。 • all：表示同步至指定数据中心的所有节点。

默认值为“all”。



注意：在为 SDNS 数据中心配置 HA 主备模式时，在本地 SDNS 数据中心执行该命令时，需要在远端数据中心上配置本地数据中心作为同步节点（通过命令“**synconfig peer**”），且同步节点的 IP 必须为本地数据中心的 IP。

sdns sync config from <dc_name> <node_ip>

该命令用于将指定远端 SDNS 数据中心节点的配置同步至本地数据中心节点。

dc_name	• 该参数指定远端数据中心名称，取值必须为数据中心名称，表示同步至该数据中心。
node_ip	• 该参数指定远端数据中心节点 IP，取值必须为节点 IP，表示同步至指定数据中心的指定节点。



注意：在为 SDNS 数据中心配置 HA 主备模式时，在本地 SDNS 数据中心执行该命令时，需要在远端数据中心上配置本地数据中心作为同步节点（通过命令“**synconfig peer**”），且同步节点的 IP 必须为本地数据中心的 IP。

show statistics sdns dc instance [dc_name]

该命令用于显示指定的数据中心所有节点和其包含的健康检查实例的统计信息。如不指定参数“dc_name”，则显示所有数据中心所有节点和其包含的健康检查实例的统计信息。

sdns sync group name <sync_group_name>

该命令用于配置 SDNS 同步组名称。配置该命令后，仅同步组名称相同的 SDNS 设备间可以进行 SDNS 运行时配置同步。启用该功能前，请先禁用 SDNS 运行时配置同步功能。

如果不配置该命令，系统默认的 SDNS 同步组为“default”，表示设备仅与 SDNS 同步组名称为“default”的设备进行同步。

sync_group_name 该参数指定 SDNS 同步组名称。取值必须为长度不大于 128 个字节的字符串。

show sdns sync group name

该命令用于显示 SDNS 同步组名称配置。

sdns sync config bootstrap on

该命令用于启用 SDNS 功能启动时配置同步。启用该功能后，系统将远端 SDNS 设备的配置信息同步至本地 SDNS 设备。该功能默认为禁用。

该功能不会同步的配置项列表如下：

```
sdns on
sdns off
sdns listener
sdns dps localdetector
```

sdns sync config bootstrap off

该命令用于禁用 SDNS 功能启动时配置同步。

sdns sync config runtime on

该命令用于为 SDNS 启用运行时配置同步功能。启用该功能后，当一个数据中心的配置发生改变时，该数据中心的这些配置将实时同步到其他数据中心。该功能只同步功能启用后变动的配置。该功能默认是禁用的。

只有在本地和远端数据中心都启用该功能时，才能在数据中心间进行实时的配置同步。对于不需要同步的 SDNS 配置项，系统通过一个黑名单管理。启用运行时配置同步功能后，除黑名单以外的所有配置项都会被同步。下表列出了黑名单里的所有配置项：

```
show
clear sdns all
sdns dc
no sdns dc
clear sdns dc
sdns dnssec
```

```
no sdns dnssec
clear sdns dnssec
sdns dps
no sdns dps
clear sdns dps
sdns listener
no sdns listener
clear sdns listener
sdns sync config
sdns on
sdns off
sdns config
no sdns config
clear sdns config
clear sdns sync log
sdns dps write proximity
```



注意：

- 启用运行时配置同步功能后，只在一台数据中心主机上进行配置才能同步全部命令。如果在多台数据中心主机上同时进行命令同步，运行时配置同步会产生冲突，最终同步的命令不完整；
- SDNS 运行时配置同步功能与增量同步功能不能同时启用。
- 当 TCP 最大分段大小 (MSS) 的值小于 216 时，设备会丢弃 TCP 报文，导致该功能失效。

sdns sync config runtime off

该命令用于禁用 SDNS 运行时配置同步功能。

show sdns sync config

该命令用于显示 SDNS 运行时配置同步功能的配置。

show sdns sync log [dc_name] [filter_string]

该命令用于显示 SDNS 运行时配置同步日志的信息。

show sdns sync log [dc_name] [node_ip] [filter_string]

该命令用于显示 SDNS 运行时配置同步日志的信息。

dc_name

可选，该参数指定 SDNS 数据中心的名称，取值必须为长度不大于 128 个字节的字符串或者“all”，默认值为“all”。

- 如果该参数不为“all”，系统将显示指定 SDNS 数据中心的运行时配置同步日志的信息，并详细显示

同步成功 (success)、同步命令未执行 (failed) 或同步失败 (loss) 的每一条命令。

- 如果指定该参数为 “all”，系统将显示所有 SDNS 数据中心的运行时配置同步日志的信息，只显示同步成功、同步命令未执行或同步失败的命令的数量。

node_ip

可选，该参数指定 SDNS 数据中心的节点 IP，取值可以为 “all”，表示显示指定 SDNS 数据中心的所有节点的同步日志。

默认值为 “all”。

filter_string

可选，该参数指定 SDNS 运行时配置同步日志的过滤字符串，支持关键字 “success”、“loss” 和 “failed”。

- 如果指定该参数，系统将显示所有与该字符串匹配 SDNS 运行时配置同步的信息。
 - 如果参数取值为关键字 “success”、“loss” 或 “failed”，将只对应显示同步成功、同步命令未执行或同步失败的命令。
 - 如果指定该参数为非以上关键字的字符串，则按配置 SDNS 命令的顺序显示 “success” 和 “failed” 的命令。
- 如果不指定该参数，系统将显示每一个远端数据中心同步命令的统计信息。



注意：如果在启用运行时配置同步功能后添加新的数据中心，启用运行时配置同步功能后的所有的命令都将被统计到该新数据中心的 “loss” 部分。

配置示例如下：

SDNS 运行时配置同步

```
Demo(config)#sdns sync config runtime on
Demo(config)#show sdns sync config
sdns sync config runtime on
Demo(config)#show sdns sync status
sdns sync status 3 2
```

SDNS 运行时配置同步日志分析

```
Demo(config)#show sdns sync log
dc name: dc2(192.168.93.200)
```

```
Total failed : 2
Total loss   : 0
Total success: 65
Failed cli command:
no sdns service ip "resorts1"
Service name "resorts1" not found.
Failed tp execute "no sdns service ip" "resorts1"
no sdns service ip "resorts2"
Service name "resorts2" not found.
Failed tp execute "no sdns service ip" "resorts2"
dc name: dc22(182.16.8.222)
Total failed : 0
Total loss   : 2
Total success: 65
Loss cli command:
no sdns service ip "resorts1"
no sdns service ip "resorts2"
Demo(config)#show sdns sync log dc2 pool
192.168.63.200:sdns pool name "a1" 3
192.168.63.200:sdns pool method primary "a1" rr
192.168.63.200:sdns pool name "a2" 3
192.168.63.200:sdns pool method primary "a2" rr
192.168.63.200:sdns pool name "a3" 3
192.168.63.200:sdns pool method primary "a3" rr
```

clear sdns sync log

该命令用于清除所有的 SDNS 运行时配置同步日志。

show sdns sync diff [dc_name] [node_ip]

该命令用于显示本地数据中心与指定远端数据中心的指定节点之间的 SDNS 配置的差异。

在执行该命令前必须配置：

- 配置本地数据中心主机和至少一个远端数据中心主机；
- 配置 Challenge Code（通过命令“**synconfig challenge**”）；
- 如果在本地数据中心执行该命令，则需要远端数据中心配置同步节点 IP 为本地数据中心的 IP 地址；如果在远端数据中心执行该命令，则需要在本本地数据中心配置同步节点 IP 为远端数据中心的 IP 地址。

该命令不支持显示数据中心和数据中心备机之间的 SDNS 配置差异。

dc_name	可选，该参数指定已存在的远端数据中心的名称。默认为“all”，表示显示本地数据中心与所有远端数据中心之间的 SDNS 配置的差异。
node_ip	可选，该参数指定已存在的远端数据中心节点的 IP 地址。默认为“all”，表示显示本地数据中心与指定数据中心所有节点之间的 SDNS 配置的差异。



注意：在为 SDNS 数据中心配置 HA 主备模式时，在本地 SDNS 数据中心执行该命令时，需要在远端数据中心上配置本地数据中心作为同步节点（通过命令“**synconfig peer**”），且同步节点的 IP 必须为本地数据中心的 IP。

对于无法通过执行该命令显示的配置差异，系统通过一个黑名单管理。下表列出了黑名单里的所有配置项：

```
no(no sdns pool resort service 除外)
show
clear
sdns dc
sdns dnssec
sdns dps
sdns listene
sdns sync config
sdns on
sdns off
sdns config
```

13.18 SDNS 链路

sdns link name <link_name> <gateway_ip> <dc_name> [hc_mode]

该命令用于为指定的数据中心创建一条 SDNS 链路，创建 SDNS 链路后，系统将默认启用该 SDNS 链路。系统支持为所有数据中心总共创建最多 1024 条 SDNS 链路。

对于已存在的 SDNS 链路，该命令支持修改 SDNS 链路关联的网关 IP 地址，修改前后的 IP 地址类型需要保持一致。

link_name 该参数指定 SDNS 链路的名称，SDNS 链路的名称必须唯一。取值必须为长度不大于 128 个字节的字符串。

注意：参数取值不能为“all”。

gateway_ip 该参数指定 SDNS 链路的网关 IP 地址。取值必须为 IPv4

或者 IPv6 地址。对于不同的 SDNS 链路，其网关 IP 地址可以相同。

dc_name

该参数指定已存在的数据中心的名称。

hc_mode

该参数指定 SDNS 链路健康检查模式。取值必须为：

- 0：表示常规模式（Normal）。在该模式下，系统采用原有行为，即当本地数据中心未收到其他数据中心返回的链路健康检查实例状态时，系统不会主动探测，直接将该数据中心的链路健康检查实例状态置为“Down”。
- 1：表示故障切换探测模式（Failover）。在该模式下，当本地数据中心未收到其他数据中心返回的链路健康检查实例状态时，系统将会主动探测。具体分为如下几种情况：
 - 如果健康检查模板设置了目的 IP 地址，并且设置的目的 IP 与 SDNS 链路网关 IP 地址不同，那么将 SDNS 链路与健康检查模板关联后，系统将会创建两个健康检查实例，分别为主实例（Primary Instance）和备实例（Instance）（可以通过命令“**show statistics sdns dc instance**”查看）。
 - 当本地数据中心探测到其他数据中心的健康检查实例状态时，主实例健康检查状态标识为探测到的状态，备实例的健康检查状态与主实例的健康检查状态相同。
 - 当本地数据中心无法探测到其他数据中心的健康检查实例状态时，主实例的健康检查状态将被标识为 Down，备实例的健康检查状态通过探测 SDNS 链路网关 IP 地址获取。
 - 如果健康检查模板设置的目的 IP 地址与 SDNS 链路网关 IP 地址相同时，将 SDNS 链路与健康检查模板关联后，系统仅生成一个健康检查实例，且本地数据中心获取健康检查实例状态失败时不进行主动探测。
 - 如果健康检查模板未设置目的 IP 地址，将 SDNS 链路与健康检查模板关联后，系统只会生成一个健康检查实例。具体分两种情况：
 - 当本地数据中心收到其他数据中心的健康检查实例状态时，直接使用此状态标识健康检查实例

的状态。

- 当本地数据中心未收到其他数据中心的健康检查实例状态时，系统将主动探测健康检查实例状态。

默认值为 0。

no sdns link name <link_name>

该命令用于删除指定的 SDNS 链路的配置。

show sdns link name [link_name]

该命令用于显示指定的 SDNS 链路的配置。如果不指定参数 “link_name”，系统将显示所有的 SDNS 链路的配置。

clear sdns link name

该命令用于清除所有 SDNS 链路的配置。

sdns link monitor apply <link_name> <template_name>

该命令用于为指定的 SDNS 链路关联一个健康检查模板。为 SDNS 链路关联健康检查模板后，系统会生成相应的 SDNS 链路的健康检查实例（通过命令 “**show statistics sdns link**” 或者命令 “**show statistics sdns dc instance**” 查看）。

一个 SDNS 链路最多可以关联 8 个健康检查模板。

link_name 该参数指定 SDNS 链路的名称。

template_name 该参数指定健康检查模板的名称，不支持数据收集类型的健康检查模板。



注意：与 SDNS 链路关联的健康检查模板如果是 TCP、HTTP 和 HTTPS 等需要目的端口类型的模板，则在定义模板时需要指定目的端口号。

no sdns link monitor apply <link_name> <template_name>

该命令用于解除指定 SDNS 链路与健康检查模板之间的关联关系。

show sdns link monitor apply [link_name]

该命令用于显示指定 SDNS 链路与健康检查模板之间的关联关系。如果不指定参数 “link_name”，将显示所有 SDNS 链路与健康检查模板之间的关联关系。

clear sdns link monitor apply [link_name]

该命令用于清除指定 SDNS 链路与健康检查模板之间的关联关系。如果不指定参数 “link_name”，将清除所有 SDNS 链路与健康检查模板之间的关联关系。

sdns link health relation <link_name> [relation]

该命令用于设置指定的 SDNS 链路的健康检查实例之间的关系。

link_name	该参数指定 SDNS 链路的名称。
relation	可选，该参数指定 SDNS 链路的健康检查实例之间的关系。取值必须为： • and: 表示只有当 SDNS 链路的所有健康检查实例的结果为“Up”时，系统才标识该 SDNS 链路为“Up”。 • or: 表示只要 SDNS 链路的任何一个健康检查实例的结果为“Up”，系统就标识该 SDNS 链路为“Up”。 默认值为 “and”。

show sdns link health relation [link_name]

该命令用于显示指定的 SDNS 链路的健康检查实例之间的关系。如果不指定参数 “link_name”，则将显示所有 SDNS 链路的健康检查实例之间的关系。

sdns link health mixrelation <link_name> <expression>

该命令用于为指定 SDNS 链路的多个健康检查实例设置混合关系。

link_name	该参数指定 SDNS 链路的名称。
expression	该参数指定用于判断 SDNS 链路的健康检查状态的关系表达式。表达式必须置于双引号内。表达式结构为： (monitor group1) OR/AND (monitor group2) OR/AND (monitor group3)... 表达式中的一个括号代表一个健康检查模板组，系统最多支持定义 5 个组，组之间的逻辑关系用 AND 或 OR 连接，如(m1) OR (m2 OR m3) AND (m4)。 每个组中最多支持定义不超过 8 个健康检查模板。不同健康检查模板组中可以使用相同的健康检查模板。 出现在表达式中的健康检查模板应该与链路关联。如果表达式中的健康检查模板被删除，与该模板相关的设置也将从表达式中删除。



注意： 当为 SDNS 链路配置混合关系后，通过命令 “sdns link health relation” 为该 SDNS 链路设置的与或关系将不再生效。

no sdns link health mixrelation <link_name>

该命令用于删除指定的 SDNS 链路中多个健康检查实例之间的混合关系。

show sdns link health mixrelation [link_name]

该命令用于显示指定的 SDNS 链路健康检查实例之间的混合关系。如果不指定参数 “link_name”，则将显示所有 SDNS 链路的健康检查实例之间的混合关系。

sdns link service <link_name> <service_name>

该命令用于将指定的 SDNS 服务关联到指定的 SDNS 链路。一个 SDNS 服务只能关联一个 SDNS 链路，一个 SDNS 链路可以与最多 20,000 个 SDNS 服务关联。

link_name 该参数指定已存在的 SDNS 链路的名称。

service_name 该参数指定已存在的 SDNS 服务的名称。该 SDNS 服务的 IP 地址类型必须与 SDNS 链路的网关 IP 地址类型一致，并且该 SDNS 服务必须和参数 “link_name” 指定的 SDNS 链路属于同一个数据中心。

no sdns link service <link_name> <service_name>

该命令用于解除指定的 SDNS 服务与指定的 SDNS 链路之间的关联关系。

show sdns link service [link_name]

该命令用于显示指定 SDNS 链路上关联的 SDNS 服务。如果不指定参数 “link_name”，将显示所有 SDNS 链路上关联的 SDNS 服务。

clear sdns link service [link_name]

该命令用于清除指定 SDNS 链路与 SDNS 服务的关联关系。如果不指定参数 “link_name”，将清除所有 SDNS 链路与 SDNS 服务的关联关系。

sdns link enable <link_name>

该命令用于启用指定的 SDNS 链路。

link_name 该参数指定已存在的 SDNS 链路的名称。

sdns link disable <link_name>

该命令用于禁用指定的 SDNS 链路。链路禁用后，所有与该链路关联的 SDNS 服务都将不可用。

link_name 该参数指定已存在的 SDNS 链路的名称。

show sdns link status [link_name]

该命令用于显示指定链路的状态信息，包括链路名称、所属数据中心、启用状态和链路是否可用等。

show statistics sdns link [link_name]

该命令用于显示指定的 SDNS 链路的统计信息。

13.19 DNS 响应码重写

sdns settings rcodeconvert <origin_rcode> <new_rcode> [host_name]

该命令用于为指定 SDNS 域名配置 DNS 响应码重写规则。配置该命令后，系统将接收到的 DNS 响应与已有配置进行匹配，匹配的顺序为先匹配指定 SDNS 域名的 DNS 响应码重写规则，再匹配全局的 DNS 响应码重写规则，只有匹配成功，重写才会生效。该命令支持在分区下执行。

origin_rcode

该参数指定原有的 DNS 响应码，取值必须为：

- FORMERR: 表示域名服务器无法解释查询。
- SERVFAIL: 表示由于域名服务器问题，无法处理该查询。
- NXDOMAIN: 表示查询中引用的域名不存在。
- NOTIMP: 表示域名服务器不支持所请求的查询类型。
- REFUSED: 表示域名服务器由于策略原因拒绝执行指定的操作。

该参数取值不区分大小写。

new_rcode

该参数指定改写后的 DNS 响应码。取值必须为：

- NOERROR: 表示无错误条件。
- FORMERR: 表示域名服务器无法解释查询。
- SERVFAIL: 表示由于域名服务器问题，无法处理该查询。
- NXDOMAIN: 表示查询中引用的域名不存在。
- NOTIMP: 表示域名服务器不支持所请求的查询类型。
- REFUSED: 表示域名服务器由于策略原因拒绝执行指定的操作。

该参数取值不区分大小写。且参数取值不能和参数“origin_rcode”取值相同。

host_name

可选。该参数指定已存在的 SDNS 域名。分区模式下，不支持配置为空。

默认值为空，表示为全局配置 DNS 响应码重写规则。



注意：当前 DNS 响应码重写规则支持 SDNS 域名和 DNS 区域。不支持 SDNS 域名转发、DNS 区域转发和 SDNS 全域名功能。

no sdns settings rcodeconvert [host_name]

该命令用于删除为指定 SDNS 域名配置的 DNS 响应码重写规则，如果不指定参数“host_name”，将删除为全局配置的 DNS 响应码重写规则。该命令支持在分区下执行。

show sdns settings rcodeconvert [host_name]

该命令用于显示为指定 SDNS 域名配置的 DNS 响应码的重写规则。该命令支持在分区下执行。

host_name 可选。该参数指定已存在的 SDNS 域名。如果不指定该参数，即取值为空时，表示显示为全局和所有 SDNS 域名配置的 DNS 响应码重写规则。

分区模式下，取值为空时，表示显示该分区下为所有 SDNS 域名配置的 DNS 响应码重写规则。

默认值为空。

clear sdns settings rcodeconvert

该命令用于清除为全局以及所有 SDNS 域名配置的 DNS 响应码重写规则。该命令支持在分区下执行。分区模式下，该命令用于清除该分区下为所有 SDNS 域名配置的 DNS 响应码重写规则。

13.20 SDNS 解析失败自定义应答策略

sdns settings failaction <action> [host_name] [record_type]

该命令用于为指定 SDNS 域名配置解析失败应答策略。配置该命令后，如果 SDNS 解析失败，系统将接收到 DNS 请求与已有配置进行匹配，匹配顺序为先匹配指定 SDNS 域名的解析失败应答策略，再匹配全局的解析失败应答策略，只有匹配成功，解析失败应答策略才会生效。系统支持为同一 SDNS 域名配置一条同一资源记录类型的解析失败应答策略。系统支持为全局配置每种资源记录类型的解析失败应答策略各一条。该命令支持在分区下执行。

action 该参数指定解析失败应答策略，取值必须为：

- **NOERROR**：表示无错误条件。
- **FORMERR**：表示域名服务器无法解释查询。

- **SERVFAIL**: 表示由于域名服务器问题, 无法处理该查询。
- **NXDOMAIN**: 表示查询中引用的域名不存在。
- **NOTIMP**: 表示域名服务器不支持所请求的查询类型。
- **REFUSED**: 表示域名服务器由于策略原因拒绝执行指定的操作。
- **DROP**: 表示丢弃请求报文。
- **BIND**: 表示将请求报文转发给 bind 处理。

当取值为“NOERROR”、“FORMERR”、“SERVFAIL”、“NXDOMAIN”、“NOTIMP”或“REFUSED”时, 系统将返回 DNS 响应码。

该参数取值不区分大小写。

host_name

可选。该参数指定已存在的 SDNS 域名。分区模式下, 不支持配置为空。

默认值为空, 表示为全局配置失败应答策略。

record_type

可选。该参数指定资源记录的类型。取值必须为: “A”、“AAAA”、“SOA”、“NS”、“MX”、“CNAME”、“SRV”、“PTR”、“TXT”、“DNAME”、“NAPTR”、“SPF”、“HINFO”、“HTTPS”或“ALL”。非“ALL”类型和“ALL”类型可以同时配置。匹配时, 先匹配指定资源记录类型的解析失败应答策略, 再匹配“ALL”类型的解析失败应答策略。

默认值为“ALL”, 表示不区分类型。

该参数取值不区分大小写。



注意:

当前 SDNS 解析失败自定义应答策略支持 SDNS 域名和 DNS 区域。不支持 SDNS 域名转发、DNS 区域转发和 SDNS 全域名功能。

no sdns settings failaction [host_name] [record_type]

该命令用于删除为指定 SDNS 域名配置的解析失败应答策略。

host_name

可选。该参数指定已存在的 SDNS 域名。

- 如果指定该参数, 表示删除为指定 SDNS 域名配置

的解析失败应答策略。

- 如果不指定该参数，即取值为空时，表示删除为全局配置的解析失败应答策略。

分区模式下，不支持配置为空。

默认值为空。

record_type

可选。该参数指定资源记录的类型。

- 如果指定该参数，表示删除指定资源记录类型的解析失败应答策略。
- 如果不指定该参数，即取值为空时，表示删除所有资源记录类型的解析失败应答策略。

默认值为空。

show sdns settings failaction [host_name]

该命令用于显示为指定 SDNS 域名配置的解析失败应答策略。该命令支持在分区下执行。

host_name

可选。该参数指定已存在的 SDNS 域名。如果不指定该参数，即取值为空时，表示显示为全局和所有 SDNS 域名配置的解析失败应答策略。

分区模式下，取值为空时，表示显示该分区下为所有 SDNS 域名配置的解析失败应答策略。

默认值为空。

clear sdns settings failaction [host_name]

该命令用于清除为全局以及所有 SDNS 域名配置的解析失败应答策略。该命令支持在分区下执行。

host_name

可选。该参数指定已存在的 SDNS 域名。如果不指定该参数，即取值为空时，表示清除为全局和所有 SDNS 域名配置的解析失败应答策略。

分区模式下，不支持配置为空。

默认值为空。

13.21 TCP DNS

sdns settings tcpdns [max_connection] [timeout] [idle|duration]

该命令用于设置 TCP DNS 连接的最大并发连接数、超时时间和超时模式。如果未配置该命令，系统默认的 TCP DNS 连接的最大连接数为 10,000，超时时间为 120 秒，超时模式为 “idle”。

max_connection	可选，该参数指定 TCP DNS 后台服务允许的最大并发连接数。取值必须为 0 到 4,294,967,295 之间的整数。取值为 0 时表示没有最大并发连接数限制。 默认值为 10,000。 最大并发连接数的设置取决于提供 TCP DNS 后台服务的服务器的性能。如果设置的最大并发连接数超出服务器所支持的范围，超出部分的连接将无法建立。
timeout	可选，该参数指定 TCP DNS 连接的超时时间，单位为秒。取值必须为 30 到 7,200 之间的整数。 默认值为 120。
idle duration	可选，该参数指定 TCP DNS 会话保持关系的超时模式。取值必须为： • idle: 表示在超过设置的超时时间内没有使用会话保持关系时，设备将会删除该会话保持关系。 • duration: 表示当会话保持关系已建立的时间超过设置的超时时间，设备将会删除该会话保持关系。 默认值为 “idle”。

show sdns settings tcpdns

该命令用于显示 TCP DNS 连接的最大并发连接数、超时时间和超时模式的设置。

13.22 DOH

slb real dns <real_service> <ip> [port] [max_connection] [hc_type] [hc_up] [hc_down] [timeout]

该命令用于配置一个使用 UDP 协议进行数据传输的 DNS 类型的后台服务，该后台服务在 WebUI 上显示为 DNS UDP 类型。

real_service	该参数指定后台服务的名称。取值必须为长度不大于最大长度为 128 个字节的字符串，区分大小写。当参数取值包含特殊字符时（特殊字符包括 '@'、'!'、'~'、'_'、':'、'-'、'.'），必须置于双引号内。参数取值不能包含空格，且不允许为系统保留字 “default”、“all” 或

“global”，这些系统保留字不区分大小写。

注意：后台服务的名称不能和已有虚拟服务的名称相同。

ip	该参数指定后台服务的 IP 地址。取值必须为 IPv4 或 IPv6 地址。
port	可选，该参数指定后台服务监听客户端请求的端口号。取值必须为 0 到 65,535 之间的整数。如果参数取值为“0”，表示该后台服务在所有端口监听客户端请求，且参数“hc_type”的取值只能为“icmp”或“none”。 默认值为 53。
max_connection	可选，该参数指定后台服务允许的最大并发连接数。取值必须为 0 到 4,294,967,295 之间的整数。取值为 0 时表示没有最大并发连接数限制。 最大并发连接数的设置取决于提供后台服务的服务器的性能。如果设置的最大并发连接数超出服务器所支持的范围，超出部分的连接将无法建立。 默认值为 0。
hc_type	可选，该参数指定基本健康检查的类型。取值必须为“dns”、“icmp”、“udp”、“script-udp”、“snmp”、“external-script”或“none”。 • 如果参数“port”的取值为 0，该参数的取值只能为“icmp”和“none”。 • 如果参数取值为“none”，表示不对后台服务进行基本健康检查。 默认值为“dns”。
hc_up	可选，该参数指定标识后台服务的状态为“Up”需要的连续健康检查成功的次数。取值必须为 1 到 255 之间的整数。 默认值为 3。
hc_down	可选，该参数指定标识后台服务的状态为“Down”需要的连续健康检查失败的次数。取值必须为 1 到 255 之间的整数。

默认值为 3。

timeout 可选，该参数指定后台服务连接的超时时间，单位为秒。
取值必须为 1 到 1,000,000 之间的整数。

默认值为 60。

no slb real dns <real_service>

该命令用于删除特定协议类型的指定后台服务。

show slb real dns [real_service]

该命令用于显示特定协议类型的指定后台服务。如果不指定参数“real_service”，系统将显示特定协议类型的所有后台服务。

clear slb real dns

该命令用于删除特定协议类型的所有后台服务。

slb group method <group_name> [method]

该命令用于创建一个后台服务组，并为其设置负载均衡算法。

group_name 该参数指定后台服务组的名称。取值必须为长度不大于 128 个字节的字符串。如果参数取值只包含数字或者包含特殊字符时（特殊字符包括‘@’、‘!’、‘~’、‘_’、‘:’、‘-’、‘.’），必须置于双引号内。

注意：在分区模式下，由于配置的后台服务组名称被处理成“group_name@@segment_name”的形式，所以在系统模式下配置的后台服务组名称中不能包含“@@”，否则系统会报错。

method 可选，该参数指定用来对后台服务组内的后台服务进行负载均衡的服务组算法。取值必须为：

- rr: Round Robin, 轮询
- grr: Global Round Robin, 全局轮询
- sr: Shortest Response, 最短响应时间
- lc: Least Connections, 最少连接数*
- lb: Least Bandwidth, 最小带宽使用率*
- snmp: SNMP, 简单网络管理协议*
- pi: Persistent IP*

- pto: Persistent TCP Option*
- hi: Hash IP*
- hip: Hash (IP+Port)*
- chi: Consistent Hash IP*
- hh: Hash Header*
- chh: Consistent Hash Header*
- ph: Persistent Hostname*
- pu: Persistent URL*
- hq: Hash Query*
- ic: Insert Cookie*
- hc: Hash Cookie*
- pc: Persistent Cookie*
- rc: Rewrite Cookie*
- ec: Embed Cookie*
- sslsid: SSL Session ID*
- sipcid: SIP Call ID*
- sipuid: SIP User ID*
- sipcidps: SIP CallID Persistence Session*
- sipuidps: SIP UserID Persistence Session*
- rdprt: RDP Routing Token*
- radchu: Consistent Hash RADIUS Username
- radchs: Consistent Hash RADIUS Session ID
- radpsun: RADIUS Persistence Session by Username*
- persistence: Individual Session Persistence*
- diametersid: Diameter Session ID*
- tuxedo: Tuxedo*
- orchestrator: Orchestrator

默认值为“rr”。

no slb group method <group_name>

该命令用于删除指定后台服务组。该命令还将删除该后台服务组关联的策略、该后台服务组中的后台服务以及该后台服务组相关的配置。

show slb group method [group_name]

该命令用于显示指定的后台服务组及其使用的算法。如果不指定参数“group_name”，则显示所有的后台服务组及其使用的算法。

clear slb group method

该命令用于清除所有后台服务组。该命令还将清除每个后台服务组关联的策略、每个后台服务组中的后台服务以及每个后台服务组相关的配置。

**slb group member <group_name> <real_service>
[weight|cookie_value|url_tag_value] [priority]**

该命令用于将后台服务添加到指定的后台服务组中。

group_name 该参数指定已存在的后台服务组名称。

real_service 该参数指定已存在的后台服务名称。

weight|cookie_value|url_tag_value • **weight:** 该参数指定后台服务的权重值。取值必须为 1 到 4,294,967,295 之间的整数。默认值为 1。当后台服务组使用 rr、grr、lc 或 lb 算法时或者当后台服务组使用 pi、ph、hh、hq、hc、ic、rc、ec、sslsid、radchs 等算法且“首次选择算法”为 rr、grr、lc 或 lb 时，需要设置该参数。

• **cookie_value:** 该参数指定后台服务对应的 cookie 值。当后台服务组使用 pc 算法时需要设置该参数。详细信息请参见命令“**slb group method <group_name> pc [offset]**”。

• **url_tag_value:** 该参数指定后台服务对应的 URL tag 值。当后台服务组使用 pu 算法时需要设置该参数。详细信息请参见命令“**slb group method <group_name> pu**”。

priority 可选，该参数指定后台服务的优先级。取值必须为 0 到 4,294,967,295 之间的整数。默认值为 0。参数取值越大，优先级越高。

该参数需要与命令“**slb group activation**”配合使用。



注意:

- 添加到同一后台服务组中的后台服务必须是同一协议类型的后台服务。
- 如果一个算法的服务组成员配置了该命令的 “[weight|cookie_value|url_tag_value]” 参数，那么在该服务组的算法被修改后，该参数将被自动修改为默认值（“weight”修改为 1，“cookie_value”和“url_tag_value”修改为后台服务名称）。

no slb group member <group_name> <real_service>

该命令用于从指定后台服务组中删除一个后台服务。

show slb group member [group_name]

该命令用于显示指定后台服务组中的所有后台服务。如果不指定参数 “group_name”，则显示所有后台服务组中的后台服务。

clear slb group member<group_name>

该命令用于清除指定后台服务组中的所有后台服务。

slb virtual https <virtual_service> <vip> [vport] [arp_support]
[max_connection]

该命令用于配置一个 HTTPS 协议类型的虚拟服务。

virtual_service 该参数指定虚拟服务的名称，取值必须为长度不超过 128 个字节的字符串，支持数字、字母和特殊字符（特殊字符包括 ‘@’、‘!’、‘~’、‘_’、‘:’、‘-’、‘.’），区分大小写。当取值包含特殊字符时，必须置于双引号内。该参数取值不能设置为系统保留字 “default”、“all” 或 “global”（不区分大小写）。

vip 该参数指定虚拟服务的 IP 地址，取值必须为 IPv4 地址或 IPv6 地址。

vport 可选，该参数指定虚拟服务的端口，取值必须为 0 至 65,535 之间的整数。当该参数取值为 0 时，表示该虚拟服务在所有的端口监听客户端请求。

默认值为 443。

arp_support 可选，该参数指定该虚拟服务是否支持 ARP 协议，取值必须为：

- arp: 表示该虚拟服务支持 ARP 协议。

- **noarp**: 表示该虚拟服务不支持 ARP 协议。虚拟服务的 IP 地址无法 ping 通, 也不能被 ARP 协议探测到。客户端可以直接向后台服务的 IP 地址发送数据。这种情况下, 需将设备接口 IP 配置为客户端的网关。

默认值为 “arp”。

max_connection 可选, 该参数指定每个虚拟服务的最大并发连接数, 默认值为 0, 表示没有最大并发连接数限制。

no slb virtual https <virtual_service>

该命令用于删除指定协议类型的虚拟服务及其关联的所有策略。

show slb virtual https [virtual_service]

该命令用于显示指定虚拟服务的配置。如不指定参数 “virtual_service”, 则显示指定协议类型的所有虚拟服务的配置。

clear slb virtual https

该命令用于清除指定协议类型的所有虚拟服务。

slb policy doh <virtual_service> <group_name>

该命令用于配置 DoH (DNS over HTTPS) 策略, 将一个 HTTPS 虚拟服务与一个 DNS 类型的服务组关联。

virtual_service 该参数指定 HTTPS 虚拟服务的名称。

group_name 该参数指定 DNS 类型的服务组的名称。

服务组的算法必须为以下中的任意一个: 轮询 (rr)、全局轮询 (grr)、最少连接数 (lc)、最短响应时间 (sr)、最小带宽使用率 (lb)、保持域名 (ph)、保持 IP (pi)、通用保持算法 (persistence)、哈希头部 (hh)、SSL SID (sslsid)、哈希 IP 地址 (hi)、哈希 IP 地址和端口 (hip)、SNMP、一致性哈希头部 (chh)、一致性哈希 IP (chi)。



注意:

- DoH 策略不支持策略嵌套 (Vlink)。
- DoH 策略不支持后台 DNS 服务器发起的源认证。
- DoH 策略不支持 DNS64 和 DNS46 转换。
- 配置了 DoH 策略的 HTTPS 虚拟服务不支持 SSF 功能。

- 配置了 DoH 策略的 HTTPS 虚拟服务不支持 Chunk 编码的请求。

no slb policy doh <virtual_service>

该命令用于删除为指定的 HTTPS 虚拟服务配置的 DoH 策略。

show slb policy doh [virtual_service]

该命令用于显示为指定 HTTPS 虚拟服务配置的 DoH 策略。如果不指定“virtual_service”参数，将显示为所有 HTTPS 虚拟服务配置的 DoH 策略。

clear slb policy doh

该命令用于清除为所有 HTTPS 虚拟服务配置的 DoH 策略。

13.23 DNS ePolicy 集成

sdns epolicy attach script <host_name|listen_ip_address> <script_name>

该命令用于将指定的 ePolicy 事件处理脚本关联到指定的 SDNS 域名或者 SDNS 服务监听的 IP 地址。一个指定的 SDNS 域名或者 SDNS 服务监听的 IP 地址可以关联最多 10 个事件处理脚本，而一个事件处理脚本可以关联到多个 SDNS 域名或者 SDNS 服务监听的 IP 地址。如果 SDNS 域名关联了 ePolicy 事件处理脚本，同时 SDNS 服务监听的 IP 地址也关联了 ePolicy 事件处理脚本，则系统只执行 SDNS 服务监听的 IP 地址绑定的 ePolicy 事件处理脚本，不再执行 SDNS 域名绑定的 ePolicy 事件处理脚本。

host_name|listen_ip_address 该参数指定已存在的 SDNS 域名或 SDNS 服务监听的 IP 地址以及端口。当配置 SDNS 服务监听的 IP 地址时，IPv4 地址格式为“address:port”，IPv6 地址格式为“[address]:port”。如果只有地址，没有端口时，端口默认为 53。

如果该参数的取值为“global”，表示将指定的 ePolicy 事件处理脚本关联到所有 SDNS 的域名和所有 SDNS 服务监听的 IP 地址。

script_name 该参数指定已导入的事件处理脚本的名称。事件处理脚本必须已通过“**epolicy import script**”命令导入。

no sdns epolicy attach script <host_name|listen_ip_address> <script_name>

该命令用于删除指定的 ePolicy 事件处理脚本与指定的 SDNS 域名或者 SDNS 服务监听的 IP 地址的关联关系。如果参数“host_name|listen_ip_address”的取值为“global”时，将删除指定的 ePolicy 事件处理脚本与所有 SDNS 域名和所有 SDNS 服务监听的 IP 地址的关联关系。

show sdns epolicy attach [host_name|listen_ip_address]

该命令用于显示 ePolicy 事件处理脚本与指定的 SDNS 域名或者 SDNS 服务监听的 IP 地址的关联关系。如果不指定参数 “host_name|listen_ip_address”，则显示 ePolicy 事件处理脚本与所有的 SDNS 域名或者 SDNS 服务监听的 IP 地址的关联关系。

clear sdns epolicy attach [host_name|listen_ip_address]

该命令用于清除 ePolicy 事件处理脚本与指定的 SDNS 域名或者 SDNS 服务监听的 IP 地址的关联关系。如果不指定参数 “host_name|listen_ip_address”，则清除 ePolicy 事件处理脚本与所有的 SDNS 域名或者 SDNS 服务监听的 IP 地址的关联关系。

13.24 SDNS SSL 配置

sdns ssl global <host_name>

该命令用于为 SDNS 关联一个已存在的 SSL 主机，用于 SDNS 设备间的加密通信。系统支持关联一个 SSL 主机。该功能中，虚拟主机的密码套件不支持 ECDHE-SM4-SM3、ECC-SM4-GCM-SM3、ECDHE-SM4-GCM-SM3、RC4-MD5 和 DES-CBC-SHA。

host_name 该参数指定已存在 SSL 主机名。

no sdns ssl global

该命令用于删除 SDNS 和 SSL 主机的关联关系。

show sdns ssl global

该命令用于显示当前 SDNS 关联的 SSL 主机。

sdns ssl monitor <template_name> <host_name>

该命令用于关联 SDNS HTTPS 健康检查模板和一个已存在的 SSL 主机名称，用于 SSL 双向认证。系统支持为每个 SDNS HTTPS 健康检查模板关联一个 SSL 主机。该功能中，虚拟主机的密码套件不支持 ECDHE-SM4-SM3、ECC-SM4-GCM-SM3、ECDHE-SM4-GCM-SM3、RC4-MD5 和 DES-CBC-SHA。

template_name 该参数指定已存在的 SDNS HTTPS 健康检查模板名称。

host_name 该参数指定已存在的 SSL 主机名称。

no sdns ssl monitor <template_name>

该命令用于删除 SSL 主机和指定 SDNS HTTPS 健康检查模板的关联关系。

show sdns ssl monitor [template_name]

该命令用于显示指定 SDNS 健康检查模板关联的 SSL 主机名称。

template_name 可选。该参数指定已存在的 SDNS HTTPS 健康检查模板名称。默认为 ALL，显示所有 SDNS HTTPS 健康检查模板关联的 SSL 主机。

clear sdns ssl monitor

该命令用于清除所有的 SDNS 健康检查模板与 SSL 主机的关联关系。

13.25 SDNS 与 SLB 联动

sdns virtual discovery on

该命令用于启用全局负载均衡自动学习功能。启用该功能后，系统可以自动学习到对端虚拟服务的配置及其状态，并在本地自动生成一条命名为“noodeid_vsname” SDNS 服务的配置。功能默认设置为禁用。

注意： 启用该功能前，需要启用 SDNS 功能。

sdns virtual discovery off

该命令用于禁用全局负载均衡自动学习功能。禁用该功能后，系统会删除所有自动学习到的 SDNS 服务的配置。

show sdns virtual discovery

该命令用于显示全局负载均衡自动学习功能状态。

13.26 DNS Proxy

DNS 代理功能用于为出向的 DNS 查询请求选择 DNS 服务器。目前，系统支持用两种负载均衡算法 rr 和 wrr 来选择 DNS 服务器。此外，系统允许管理员配置域名定制策略和 DNS network 策略来为出向 DNS 查询请求选择 DNS 服务器。域名定制策略的优先级高于 DNS network 策略，DNS network 策略的优先级高于负载均衡算法。

llb dnsproxy {on|off}

该命令用于启用或禁用 DNS 代理功能。DNS 代理功能可以为出向 DNS 查询请求提供链路负载均衡。当启用 DNS 代理功能后，系统将为 DNS 查询请求选择指定的 DNS 服务器。系统默认禁用 DNS 代理功能。

llb dnsproxy server <server_name> <server_ip> [weight]

该命令用于为 DNS 代理功能定义一个 DNS 服务器，或者更新已经为 DNS 代理功能配置的 DNS 服务器的 IP 地址和权重值。系统允许为 DNS 代理功能配置最多 128 个 DNS 服务器。

server_name	该参数指定 DNS 服务器的名称。取值必须为最大长度不大于 63 个字节的字符串，区分大小写。当参数取值中包含特殊字符时，该参数值必须置于双引号内。
server_ip	该参数指定 DNS 服务器的 IP 地址。取值必须为 IPv4 或 IPv6 地址。 注意： 该参数取值不支持配置为 0.0.0.0/8 网段的 IP 地址。另外，建议管理员不要将该参数取值配置为包含接口 IP 地址的网络地址、广播地址以及 IPv6 任播地址。
weight	可选，用于设置使用 wrr 算法时 DNS 服务器的权重值。取值必须为 1 到 1000 之间的整数，默认值为 1。



注意：

- 如果为各个 DNS 服务器指定相同的“weight”或者没有为其指定参数“weight”，则使用 rr 算法选择 DNS 服务器，否则使用 wrr 算法。
- 如果客户端的本地 DNS 服务器不是命令“llb dnsproxy server”指定的 DNS 服务器，DNS 代理功能将不对该客户端生效。

no llb dnsproxy server <server_name>

该命令用于删除为 DNS 代理功能配置的指定的 DNS 服务器。

show llb dnsproxy server [server_name]

该命令用于显示为 DNS 代理功能配置的指定的 DNS 服务器。如果没有指定参数“server_name”，将显示所有为 DNS 代理功能配置的 DNS 服务器。

clear llb dnsproxy server

该命令用于清除所有为 DNS 代理功能配置的 DNS 服务器。

llb dnsproxy link <link_name> <server_name>

该命令用于将指定的 LLB 链路与为 DNS 代理功能配置的指定的 DNS 服务器关联。当一条 LLB 链路的使用带宽达到带宽阈值（通过命令“llb link route”配置）时，与该 LLB 链路关联的 DNS 服务器将不再被选中，直到该 LLB 链路出现空余带宽。系统将根据负载均衡算法从为 DNS 代理功能配置的其他可用 DNS 服务器中选择一个 DNS 服务器。系统允许最多 8 条 LLB 链路与一个 DNS 服务器关联。

link_name 该参数指定 LLB 链路的名称。

server_name 该参数指定 DNS 服务器的名称。

no llb dnsproxy link <link_name> <server_name>

该命令用于删除指定的 LLB 链路和为 DNS 代理功能配置的指定的 DNS 服务器的关联关系。

show llb dnsproxy link [link_name]

该命令用于显示指定的 LLB 链路和为 DNS 代理功能配置的指定的 DNS 服务器的关联关系。如果没有指定参数“link_name”，将显示所有 LLB 链路和为 DNS 代理功能配置的指定的 DNS 服务器的关联关系。

clear llb dnsproxy link

该命令用于清除所有 LLB 链路和为 DNS 代理功能配置的该参数指定的 DNS 服务器的关联关系。

llb dnsproxy network <network_ip> <netmask><server_name>

该命令用于配置一条 DNS network 策略，用于为源 IP 地址属于特定子网的 DNS 查询请求选择一个 DNS 服务器。配置该命令后，当 DNS 查询请求的源 IP 地址属于该策略指定的子网时，系统将选择该策略指定的 DNS 服务器。如果一个 DNS 查询请求同时匹配多条 DNS network 策略，系统将优先选择子网掩码最长的 DNS network 策略。

如果参数“network_ip”和“netmask”的值设置为已存在的值，该命令还可以用于修改该 DNS network 策略的 DNS 服务器。

系统只允许为指定的子网配置一条 DNS network 策略，且最多允许配置 512 条 DNS network 策略。

network_ip	该参数指定 DNS 查询请求所属子网的 IP 地址。取值必须为 IPv4 地址。
netmask	该参数指定 DNS 查询请求所属子网的 IP 地址对应的子网掩码。取值必须为点分十进制格式或是一个 0 到 32 之间的整数。
server_name	该参数指定已存在的 DNS 服务器的名称。该 DNS 服务器必须已经使用命令 “ llb dnsproxy server ” 配置。



注意：对于匹配 DNS network 策略的 DNS 查询请求，即使该 DNS network 策略选择的 DNS 服务器状态为 “Down”，系统仍将选择该 DNS 服务器。

no llb dnsproxy network <network_ip> <netmask>

该命令用于删除指定的 DNS network 策略。

show llb dnsproxy network [network_ip] [netmask]

该命令用于显示指定的 DNS network 策略。如果不指定参数 “network_ip” 和 “netmask”，将显示所有的 DNS network 策略。

clear llb dnsproxy network

该命令用于清除所有的 DNS network 策略。

llb dnsproxy domain <host_name> <custom_policy>

该命令用于为指定域名配置一条域名定制策略，或者更新已经为指定域名配置的定制策略。系统只允许为指定的域名配置一条域名定制策略。系统支持三种类型的域名定制策略：

- 静态域名策略：系统为指定域名的 DNS 查询请求固定地选择指定的 DNS 服务器。
- Bypass 域名策略：系统不对指定域名的 DNS 查询请求应用 DNS 代理功能。
- Persistent 域名策略：系统根据源 IP 地址为指定域名的 DNS 查询请求持续地选择指定的 DNS 服务器。当 DNS 查询请求首次匹配上域名的 persistent 策略时，系统根据 DNS network 策略（如果配置并匹配）或负载均衡算法为 DNS 查询请求选择一个 DNS 服务器，并记录源 IP 地址和选择的 DNS 服务器的对应关系。当后续来自同一个 IP 地址的 DNS 查询请求匹配该策略时，系统将持续地为请求选择同一个 DNS 服务器。

host_name 该参数指定域名的名称。取值必须为最大长度不大于为 128 个字节的字符串，格式为“www.xyz.com”，该字符串中由“.”分隔的各部分长度不能超过 63 个字符。该参数支持“^”、“*”和“\$”三种通配符，具体含义如下：

- ^：匹配域名的开始。
- *：匹配 0 个或多个字符。例如，“www*.com”匹配任何以“www.”开始和“.com”结束的域名。
- \$：匹配域名的结束。

custom_policy 该参数指定域名的定制策略。取值必须为：

- DNS 服务器名称：表示该定制策略为静态域名策略。
- “bypass”：表示该定制策略为 bypass 域名策略。
- “persistent”：表示该定制策略为 persistent 域名策略。

**注意：**

- 对匹配上静态域名策略的 DNS 查询请求，即使该域名定制策略选择的 DNS 服务器的状态为“Down”，系统仍将选择该 DNS 服务器。
- 如果根据 persistent 策略选择的 DNS 服务器变为不可用时，系统将根据该策略重新选择一个 DNS 服务器。

no llb dnsproxy domain <host_name>

该命令用于删除指定域名的定制策略。

show llb dnsproxy domain [host_name]

该命令用于显示指定域名的定制策略。如果没有指定参数“host_name”，将显示所有域名的定制策略。

clear llb dnsproxy domain

该命令用于清除所有域名的定制策略。

show llb dnsproxy all

该命令用于显示 DNS 代理功能的全部配置。

clear llb dnsproxy all

该命令用于将 DNS 代理功能的全部配置重置为默认值。

13.27 External DNS 云原生方式容器平台对接方案

操作步骤:

1、在 Kuberentes 集群中部署相关资源对象

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: external-dns
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: external-dns
rules:
- apiGroups: [""]
  resources: ["services","endpoints","pods","namespaces","Secret"]
  verbs: ["get","watch","list"]
- apiGroups: ["extensions","networking.k8s.io"]
  resources: ["ingresses"]
  verbs: ["get","watch","list"]
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["list"]
---
apiVersion: v1
kind: Secret
metadata:
  name: array-credentials
  namespace: default
type: Opaque
data:
  #base64 编码
  url: aHR0cHM6Ly8xPC4yMTAuMTQuMTc0Ojk5OTc=
  username: cmVzdHFwaQ==
  password: QXJyYXPjbGljazE=
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
```

```
name: external-dns-owner
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: external-dns
subjects:
- kind: ServiceAccount
  name: external-dns
  namespace: default
---

apiVersion: apps/v1
kind: Deployment
metadata:
  name: infosec-external-dns
spec:
  strategy:
    type: Recreate
  selector:
    matchLabels:
      app: infosec-external-dns
  template:
    metadata:
      labels:
        app: infosec-external-dns
    spec:
      containers:
      - args:
        - --source=service
        - --source=ingress
        - --domain-filter=external-dns-example.com # 将使 ExternalDNS 仅看到与提供的域
匹配的域, 忽略不匹配的域
        - --provider=infosec
        - --policy=sync # 设置 “upsert-only” 将阻止 ExternalDNS 删除任何记录
        - --apv-addresses=$(ARRAY_URL)
        - --apv-username=$(ARRAY_USERNAME)
        - --apv-password=$(ARRAY_PASSWORD)
        image: "x.x.x.x:5000/external-dns:v1.1.0"
        imagePullPolicy: IfNotPresent
      env:
        # Get sensitive values from the credentials secret
        - name: ARRAY_USERNAME
```

```

      valueFrom:
        secretKeyRef:
          name: array-credentials
          key: username
    - name: ARRAY_PASSWORD
      valueFrom:
        secretKeyRef:
          name: array-credentials
          key: password
    - name: ARRAY_URL
      valueFrom:
        secretKeyRef:
          name: array-credentials
          key: url
  name: external-dns
  volumeMounts:
    - mountPath: /etc/kubernetes
      name: config-file
  dnsPolicy: ClusterFirst
  serviceAccount: external-dns
  serviceAccountName: external-dns
  volumes:
    - name: config-file
      hostPath:

        path: /etc/kubernetes/

```

2、创建 nginx 服务进行验证

```

apiVersion: v1
kind: Service
metadata:
  name: nginx
  annotations:
    external-dns.alpha.kubernetes.io/hostname: nginx.external-dns-example.com # 公网域名地址
    external-dns.alpha.kubernetes.io/internal-hostname: nginx-internal.external-dns-example.com
# 内网域名地址
    external-dns.alpha.kubernetes.io/ttl: "600"
spec:
  type: LoadBalancer
  ports:
    - port: 80
      name: http

```

```
targetPort: 80
selector:
  app: nginx
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx
spec:
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - image: nginx
          name: nginx
          ports:
            - containerPort: 80
              name: http
服务创建后 kubectl get svc 查看
CLUSTER-IP 对应域名 nginx.external-dns-example.com
EXTERNAL-IP 对应域名 nginx-internal.external-dns-example.com
```

3、按照上述步骤配置后，DNS 设备上会自动生成正确的 DNS 配置，提供 DNS 服务。

13.28 SDNS IANA

sdns iana import <url>

该命令用于导入一个 IANA（Internet Assigned Numbers Authority）文件。

url 该参数指定 IANA 文件的 HTTP 或 FTP URL 地址。

show sdns iana <ip_address>

该命令用于查询指定的 IP 地址所属的国家或地区。

ip_address 该参数指定 IP 地址。取值必须为 IPv4 地址。

13.29SDNS 日志

sdns log query custom <format>

该命令用于设置自定义 SDNS 域名解析日志的格式。

format

- 该参数指定自定义 SDNS 域名解析日志的格式。取值必须为长度不大于 256 个字节的字符串且必须置于双引号内。

管理员可以使用下表列出的符号来组成自定义的日志内容。如果参数取值包含下表列出的符号以外的其他字符，这些字符将按原样被复制到日志信息中。

13.29.1.1.1.1 支持的自定义日志内容

符号	含义
%c	记录客户端 IP 地址
%s	记录服务器 IP 地址
%p	记录客户端源端口
%i	记录每个 DNS 查询请求的唯一 ID
%n	要解析的域名
%t	指定查询的类型
%q	记录 DNS 请求的时间
%r	记录 DNS 响应的时间
%e	记录完成查询消耗的时间（单位：毫秒）
%S	DNS 报文中 RCODE 字段表示的状态码
%R	解析的结果，可以是 IP 地址、CNAME 记录等
%P	记录要解析的域名命中了哪个策略
%M	记录服务池选择服务 IP 使用的算法

若管理员需要在 WebUI 界面上按字段对 SDNS 域名解析日志进行索引，则需要首先配置“**log localhost on**”命令并且配置该命令时需要给各个字段添加前缀，前缀如下表所示。

13.29.1.1.1.2 支持的前缀

符号	含义
%c	client ip:
%s	server ip:
%p	client port:
%i	qid:

符号	含义
%n	qname:
%t	qtype:
%q	query time:
%r	response time:
%e	processing time:
%S	status code:
%R	result:
%P	policy:
%M	method:



注意:

1. SDNS 域名解析日志级别固定为 INFO 级别。
2. 使用该命令的日志默认会打印出 “SDNS:” 用于标识 SDNS 域名。
3. 若因域名解析失败，导致没有获取到某些字段的值，则显示为 “-”。
4. 该命令不仅作用于 SDNS 解析过程，也支持 Bind。但 Bind 可能会导致获取不到某些字段的值，此时显示为 “-”。
5. 该命令支持 HA 实时同步、全量同步、增量同步和启动时运行同步以及 SDNS 实时同步和全量同步。
6. 该命令不支持在分区模式下运行。
7. 在 WebUI 上按时间过滤 SDNS 日志时，需要设置设备时间与本地时间相同。
8. 在 WebUI 上按关键字过滤 SDNS 日志时，当日志中同时存在默认格式的日志和自定义格式的日志，应该按照最新的自定义格式进行过滤；若用户未配置自定义格式，则按照默认格式进行过滤。

no sdns log query custom

该命令用于删除自定义 SDNS 域名解析日志的格式。

show sdns log query custom

该命令用于显示自定义 SDNS 域名解析日志的格式。

13.30SDNS 统计功能

sdns statistics localdns {on|off}

该命令用于启用或禁用本地 DNS 服务器的统计功能。默认情况下，该功能是启用的。

show statistics sdns localdns all

该命令用于显示每个本地 DNS 服务器的统计信息。

例如:

Demo(config)#show statistics sdns localdns all					
Local DNS	Total	Success	Unauthoritative	Fail	
Drop					
IPV4:					
10.8.6.45	150	148	2	0	0
IPV6:					

show statistics sdns localdns summary

该命令用于显示全部本地 DNS 服务器的总体统计信息。

例如：

Demo(config)#show statistics sdns localdns summary					
Localdns Statistics Summary:					
	Total	Success	Unauthed	Fail	Drop
IPV4: 150	148	2	0	0	0
IPV6: 0	0	0	0	0	0

clear statistics sdns localdns

该命令用于清除本地 DNS 服务器的统计信息。

sdns statistics query {on|off}

该命令用于启用或禁用 DNS 查询统计功能。默认情况下，该功能是启用的。

show statistics sdns query [segment_name] [type]

该命令用于显示指定分区指定协议类型的 DNS 查询统计信息，包括请求总数（Request）、SDNS 处理成功的请求数（Success）、转交 Bind9 处理的请求数（Unauthed）、转发给其他 DNS 服务器处理的请求数（Forward）、处理失败的请求数（Fail）以及无法处理或者不处理的请求数（Drop）。

segment_name 可选。该参数指定需要显示 DNS 查询统计信息的分区名称。如果不指定该参数，即取值为空，则显示全局的 DNS 查询统计信息。

默认值为空。

type 可选，该参数指定需要显示的 DNS 查询统计信息的协议类型。取值必须为：

- **udp**：表示显示 UDP 协议的 DNS 查询统计信息。
- **tcp**：表示显示 TCP 协议的 DNS 查询统计信息。

默认值为 “udp”。

该参数取值不区分大小写。

分区下支持：

show statistics sdns query [type]

该命令用于显示当前分区指定协议类型的 DNS 查询统计信息。如果不指定参数 “type”，则显示当前分区 UDP 协议的 DNS 查询统计信息。

例如：

```
Demo(config)#show statistics sdns query
```

SDNS Query Statistics Summary:

Request:	150
Success:	148
Unauthed:	2
Fail:	0
Drop:	0

Second Statistics:

Request:	0
Success:	0
Unauthed:	0
Fail:	0
Drop:	0
Peak Request:	6
Peak Success:	6
Peak Unauthed:	2
Peak Fail:	0
Peak Drop:	0

5 Second Statistics:

Request:	0
Success:	0
Unauthed:	0
Fail:	0
Drop:	0
Peak Request:	8
Peak Success:	8
Peak Unauthed:	2
Peak Fail:	0
Peak Drop:	0

Minute Statistics:

Request:	0
Success:	0

```

Unauthed:      0
Fail:          0
Drop:          0
Peak Request:  37
Peak Success:  37
Peak Unauthed: 2
Peak Fail:     0
Peak Drop:     0
Hour Statistics:
Request:       150
Success:       148
Unauthed:      2
Fail:          0
Drop:          0
Peak Request:  150
Peak Success:  148
Peak Unauthed: 2
Peak Fail:     0
Peak Drop:     0
Day Statistics:
Request:       0
Success:       0
Unauthed:      0
Fail:          0
Drop:          0
Peak Request:  0
Peak Success:  0
Peak Unauthed: 0
Peak Fail:     0
Peak Drop:     0

```

clear statistics sdns query [segment_name] [type]

该命令用于清除指定分区指定协议类型的 DNS 查询统计信息。

segment_name 可选。该参数指定需要清除 DNS 查询统计信息的分区名称。如果不指定该参数，即取值为空，则清除全局的统计信息。

默认值为空。

type 可选，该参数指定需要清除的 DNS 查询统计信息的协议类型。取值必须为：

- **udp**: 表示清除 UDP 协议的 DNS 查询统计信息。

- tcp: 表示清除 TCP 协议的 DNS 查询统计信息。

默认值为 “udp”。

该参数取值不区分大小写。

分区下支持:

clear statistics sdns query [type]

该命令用于清除当前分区指定协议类型的 DNS 查询统计信息。如果不指定参数 “type”，则清除当前分区 UDP 协议的 DNS 查询统计信息。

show statistics sdns listener [ip_address] [sdns_listener_port]

该命令用于显示被监听的指定 IP 地址以及端口的统计信息。

ip_address 可选，该参数指定需要显示统计信息的 SDNS 服务监听的 IP 地址。如果不指定该参数，即取值为空时，表示显示 SDNS 服务监听的全部 IP 地址的统计信息。

默认值为空。

sdns_listener_port 可选，该参数指定需要显示统计信息的 SDNS 服务监听的端口。取值必须为 1 到 65,000 之间的整数。

默认值为 53。

clear statistics sdns listener [ip_address] [sdns_listener_port]

该命令用于清除被监听的指定 IP 地址以及端口的统计信息。

ip_address 可选，该参数指定需要清除统计信息的 SDNS 服务监听的 IP 地址。如果不指定该参数，即取值为空时，表示清除 SDNS 服务监听的全部 IP 地址的统计信息。

默认值为空。

sdns_listener_port 可选，该参数指定需要清除统计信息的 SDNS 服务监听的端口。取值必须为 1 到 65,000 之间的整数。

默认值为 53。

show sdns statistics status

该命令用于显示本地 DNS 服务器统计功能和 DNS 查询统计功能的状态。

show statistics sdns service ip [service_name]

该命令用于显示指定的 SDNS 服务的统计信息。如果不指定参数 “service_name” 的值，则将显示全部 SDNS 服务的统计信息。

例如：

```
Demo(config)#show statistics sdns service ip
```

```
Service Name:    sv1
Ip Address:      10.8.6.201
Port:            0
Health:          UP
Disabled:        NO
Relation:        AND
Hits:            4
Monitor Count:   0
    Instance ID: 0
    Monitor:      h1
    Status:       INIT
    Type:         HTTP
    Address:      10.8.6.201
    Source:       0.0.0.0
    Gateway:      0.0.0.0
```

```
Service Name:    sv2
Ip Address:      10.8.6.202
Port:            0
Health:          UP
Disabled:        NO
Relation:        AND
Hits:            4
Monitor Count:   0
    Instance ID: 1
    Monitor:      h1
    Status:       UP(PROBE_SUCCESS)
    Type:         HTTP
    Address:      10.8.6.202
    Source:       0.0.0.0
    Gateway:      0.0.0.0
```

show statistics sdns pool [pool_name]

该命令用于显示指定的 SDNS 服务池的统计信息。如果不指定参数 “pool_name” 的值，则将显示全部 SDNS 服务池的统计信息。

例如：

```
Demo(config)#show statistics sdns pool
```

```
Pool Name:        p1
Health Relation:  and
```

```
Max Resource Record Count: 1
Hit: 0
Primary Method: rr
Primary Method Success: 0
Secondary Method: none
Secondary Method Success: 0
Pool Monitor Count: 6
    Monitor Name: m1_v4
    Type: ICMP
    Monitor Name: m2_v4
    Type: ICMP
    Monitor Name: m3_v4
    Type: ICMP
    Monitor Name: m1_v6
    Type: ICMP
    Monitor Name: m2_v6
    Type: ICMP
    Monitor Name: m3_v6
    Type: ICMP
Pool Member Count: 6
    Service Name: s1_v4
    Service IP: 1.1.1.1
    Health: UP
    Weight: 1
    Priority: 6
    Hit: 0
    Instance ID: 0
    Status: UP
    Instance ID: 3
    Status: UP
    Instance ID: 6
    Status: UP

    Service Name: s2_v4
    Service IP: 1.1.1.2
    Health: UP
    Weight: 1
    Priority: 10
    Hit: 0
    Instance ID: 1
    Status: UP
    Instance ID: 4
```

Status:	UP
Instance ID:	7
Status:	UP
Service Name:	s3_v4
Service IP:	1.1.1.3
Health:	DOWN
Weight:	1
Priority:	1
Hit:	0
Instance ID:	2
Status:	DOWN
Instance ID:	5
Status:	DOWN
Instance ID:	8
Status:	DOWN
Service Name:	s1_v6
Service IP:	11::1
Health:	DOWN
Weight:	1
Priority:	1
Hit:	0
Instance ID:	9
Status:	DOWN
Instance ID:	12
Status:	DOWN
Instance ID:	15
Status:	DOWN
Service Name:	s2_v6
Service IP:	11::2
Health:	DOWN
Weight:	1
Priority:	1
Hit:	0
Instance ID:	10
Status:	DOWN
Instance ID:	13
Status:	DOWN
Instance ID:	16
Status:	DOWN

```

Service Name:      s3_v6
Service IP:        11::3
Health:            DOWN
Weight:            1
Priority:           1
Hit:               0
Instance ID:       11
Status:            DOWN
Instance ID:       14
Status:            DOWN
Instance ID:       17
Status:            DOWN

```

若为地址池配置混合关系，则显示如下：

```

Pool Name:          p1
Health Mix Relation: (m1_v4 AND m2_v4) OR (m3_v4),(m1_v6 OR
                    m2_v6) AND (m3_v6)
Max Resource Record Count: 1
Hit:                0
Primary Method:      rr
Primary Method Success: 0
Secondary Method:     none
Secondary Method Success: 0

```

show statistics sdns host [host_name]

该命令用于显示指定的 SDNS 域名的统计信息。如果不指定参数 “host_name” 的值，则将显示全部 SDNS 域名的统计信息。

例如：

```

Demo(config)#show statistics sdns host
Host Name:          www.abc.com
Host TTL:           60
Hit:                6
Default Pool:       p2
Default Policy Hit:  0
Region Policy Count: 1
Region Policy Hit:   6

Host Name:          www.xyz.com
Host TTL:           60

```



```
Hit: 2
Default Pool: bug
Default Policy Hit: 2
Region Policy Count: 0
```

show statistics sdns proximity [region_name]

该命令用于显示指定的 SDNS 区域的命中统计信息。如果不指定参数“region_name”的值，则将显示全部 SDNS 区域的命中统计信息。

例如：

```
Demo(config)#show statistics sdns proximity
Region Name          HIT
region1              6
region2              0

Total Region Number is: 2
```

show statistics sdns policy region [policy_name]

该命令用于显示指定的 SDNS 区域策略的命中统计信息。如果不指定参数“policy_name”的值，则将显示全部 SDNS 区域策略的命中统计信息。

例如：

```
Demo(config)#show statistics sdns policy region
Policy Name: policy1
Host Name: www.abc.com
Pool Name: p1
Region Name: region1
Priority: 0
Match Count: 6
```

show statistics sdns policy byhost [host_name]

该命令用于显示与指定的 SDNS 域名相关的 SDNS 策略的命中统计信息。如果不指定参数“host_name”的值，则将显示全部 SDNS 域名的策略命中统计信息。

例如：

```
Demo(config)#show statistics sdns policy byhost
Policy Name: policy1
Host Name: www.abc.com
Pool Name: p1
Region Name: region1
Priority: 0
Match Count: 6
```

```
Policy Name:      Default Policy
Host Name:        www.abc.com
Default Pool:     default_pool
Match Count:      0
Host "www.abc.com" configured default policy
Policy Name:      Resort Policy
Host Name:        www.abc.com
Resort Pool:      resort_pool
Match Count:      0
Host "www.abc.com" configured resort policy
Host "www.abc.com" has 1 region policy
Host "www.xyz.com" has 0 region policy
```

show statistics sdns policy bypool [pool_name]

该命令用于显示与指定的 SDNS 服务池相关的 SDNS 策略的命中统计信息。如果不指定参数 “pool_name” 的值，则将显示全部 SDNS 服务池的策略命中统计信息。

例如：

```
Demo(config)#show statistics sdns policy bypool
```

```
Policy Name:      policy1
Host Name:        www.abc.com
Pool Name:        p1
Region Name:      region1
Priority:          0
Match Count:      6
Pool "p1" related with 1 region policy
```

```
Pool "return" related with 0 region policy
```

```
Policy Name:      Resort Policy
Host Name:        apv.tctc.com
Pool Name:        resort_pool
Priority:          0
Match Count:      0
Pool "resort_pool" related with 0 region policy
```

```
Policy Name:      Default Policy
Host Name:        www.abc.com
Pool Name:        default_pool
Priority:          0
Match Count:      0
```

Pool "default_pool" related with 0 region policy

Pool "resort_return" related with 0 region policy

show statistics sdns policy byregion [region_name]

该命令用于显示与指定的 SDNS 区域相关的 SDNS 区域策略的命中统计信息。如果不指定参数 “region_name” 的值，则将显示全部 SDNS 区域的区域策略命中统计信息。

例如：

Demo(config)#show statistics sdns policy byregion

Policy Name: policy1
Host Name: www.abc.com
Pool Name: p1
Region Name: region1
Priority: 0
Match Count: 6
Region "region1" related with 1 region policy

Region "region2" related with 0 region policy

show statistics sdns policy default [host_name]

该命令用于显示与指定的 SDNS 域名相关的 SDNS 默认策略的命中统计信息。如果不指定参数 “host_name” 的值，则将显示全部 SDNS 域名的 SDNS 默认策略的命中统计信息。

例如：

Demo(config)#show statistics sdns policy default

Host Name	Default Pool	Match
www.abc.com	p2	0
www.xyz.com	p1	2

show statistics sdns policy resort [host_name]

该命令用于显示与指定的 SDNS 域名关联的 SDNS 应急策略被命中的统计信息。如果不指定参数 “host_name”，系统将显示所有 SDNS 域名的 SDNS 应急策略的被命中的统计信息。

例如：

Demo(config)#show statistics sdns policy resort

Host Name	Resort Pool	Match
www.abc.com	p2	0
www.xyz.com	p1	2

show statistics sdns ranking host

该命令用于显示命中次数为前 10 的 SDNS 域名。

show statistics sdns ranking policy

该命令用于显示命中次数为前 10 的 SDNS 策略。

show statistics sdns ranking pool

该命令用于显示命中次数为前 10 的 SDNS 服务池。

show statistics sdns ranking service

该命令用于显示命中次数为前 20 的 SDNS 服务。

show statistics sdns summary [host_name]

该命令用于显示指定域名相关的所有策略的统计信息。如果不指定参数“host_name”，系统将显示所有域名相关的所有策略的统计信息。

例如：

```
Demo(config)#show statistics sdns summary "www.1.com"
```

```
Host Name:          www.1.com
```

```
Host TTL:           60
```

```
Hit:                0
```

```
Region Policy Count: 1
```

```
Policy Name:        p1
```

```
Region Name:        r1
```

```
Policy Priority:     0
```

```
Policy Hit:          0
```

```
Pool Name:           p1
```

```
Health Relation:     and
```

```
Max Resource Record Count: 3
```

```
Primary Method:      rr
```

```
Primary Method Success: 0
```

```
Secondary Method:    none
```

```
Secondary Method Success: 0
```

```
Pool Monitor Count:  0
```

```
Pool Member Count:   2
```

```
Service Name:         s2
```

```
Service IP:           2.2.2.2
```

```
Health:               UP
```

```
Weight:               1
```

```
Priority:              1
```

Service Name:	s1
Service IP:	5.3.2.1
Health:	UP
Weight:	1
Priority:	1
Default Policy Hit:	0
Policy Name:	Default Policy
Pool Name:	p1
Health Relation:	and
Max Resource Record Count:	3
Primary Method:	rr
Primary Method Success:	0
Secondary Method:	none
Secondary Method Success:	0
Pool Monitor Count:	0
Pool Member Count:	2
Service Name:	s2
Service IP:	2.2.2.2
Health:	UP
Weight:	1
Priority:	1
Service Name:	s1
Service IP:	5.3.2.1
Health:	UP
Weight:	1
Priority:	1

13.31SDNS 配置备份

sdns config write file <file_name>

该命令用于将当前运行的 SDNS 配置在本地磁盘上进行备份。系统支持备份最多 10 个 SDNS 配置文件。

file_name 该参数指定要备份的 SDNS 配置文件的名称。文件名不包含后缀 “.cfg”。取值必须为长度不大于 255 个字节的字符串，支持大小写字母、数字和除 “\”、“/” 和 “” 之外的特殊字符。

注意：取值不支持全为 “.”。



注意：如果要备份的 SDNS 配置文件超过 10 个，新的 SDNS 配置文件会自动覆盖最旧的 SDNS 配置文件。

sdns config write scp <remote_server_ip|name> <user_name>
<config_file_name>

该命令用于将当前 SDNS 配置备份到远程 SCP 服务器。需要注意的是该命令需要使用密码验证功能，输入完所有参数后，系统将提示输入密码。

remote_server_ip name	该参数指定远程 SCP 服务器的 IP 地址（IPv4 或 IPv6）或名称。
user_name	该参数指定用于登录远程服务器的用户名称。
config_file_name	该参数指定需要保存的 SDNS 配置文件名称。取值必须为包含字母、数字和特殊字符的字符串，不区分大小写。当取值包含特殊字符时，必须置于双引号内。 取值不支持以下特殊字符：“>”、“'”、“””、“[]”、“{}”、“ ”、“\$”和“\”。

13.32SDNS 配置加载

sdns config file <file_name>

该命令用于从本地磁盘上加载备份的 SDNS 配置文件。在加载备份的 SDNS 配置文件前，系统会预先加载下列的 SDNS 命令，然后再加载 SDNS 配置文件中的命令。预先加载的 SDNS 命令如下：

- clear sdns zone name all
- clear sdns record all
- clear sdns pool cname
- clear sdns pool name
- clear sdns host name
- clear sdns service ip
- clear sdns service monitor apply
- clear sdns policy default
- clear sdns policy resort
- clear sdns policy region
- clear sdns proximity

- clear sdns region
- clear sdns monitor
- clear sdns snmp exp weight

file_name 该参数指定待加载的 SDNS 配置文件的名称。文件名称取值中不能包含扩展名。



注意：执行该命令时，如果启用了 SDNS 运行时配置同步或者 HA 运行时配置同步或者增量同步功能，系统会同时将预先加载的 SDNS 命令和备份的 SDNS 配置文件中的命令进行同步（同步白名单中的命令）。如果备份的 SDNS 配置文件中的 SDNS 功能为禁用状态或者 SDNS 运行时配置同步功能为禁用状态，SDNS 运行时配置同步将失败。

sdns config scp <remote_server_ip|name> <user_name>
<config_file_name>

该命令用于用户加载保存在 SCP 服务器上的 SDNS 配置文件。需要注意的是该命令需要使用密码验证功能，输入完所有参数后，系统将提示输入密码。

remote_server_ip|name 该参数指定远程 SCP 服务器的 IP 地址（IPv4 或 IPv6）或名称。

user_name 该参数指定远程服务器的用户名称。

config_file_name 该参数指定待加载的 SDNS 配置文件名称。取值必须为包含字母、数字和特殊字符的字符串，不区分大小写。当取值包含特殊字符时，必须置于双引号内。

取值不支持以下特殊字符：“>”、“'”、“””、“[]”、“{}”、“||”、“\$”和“\”。

no sdns config file <file_name>

该命令用于删除本地指定 SDNS 配置文件。

file_name 该参数指定删除的文件名称，文件名中需要包含扩展名。例如，执行命令“**no sdns config file abc.cfg**”将会删除名为 abc 的配置文件。

show sdns config file [file_name] [regex]

该命令用于显示本地指定 SDNS 配置文件中匹配过滤字符串的配置信息。

file_name 可选，该参数指定需要显示的 SDNS 配置文件的名称，文件名中不包含扩展名。

- 如果指定该参数，系统将显示 SDNS 配置文件的详细信息。
- 如果不指定该参数，系统将显示已加载的所有 SDNS 配置文件。

regex

可选，该参数指定用于过滤配置文件中配置信息的字符串，该参数仅在指定参数“file_name”时可用。该参数支持正则表达式。例如，命令行“**show sdns config file new_sdns service**”将列出配置文件“new_sdns”中所有包含“service”字符串的配置信息。

如果不指定该参数，系统将显示指定配置文件中的所有配置信息。

clear sdns config file

该命令用于清除本地所有 SDNS 配置文件。

第14章 应用安全

本章介绍如何开关防火墙以及如何设置网络安全访问规则。这些配置指明哪些互联网地址可以访问你的系统，以及只能通过哪些网络接口。

14.1 防火墙

14.1.1 访问组

accessgroup <accesslist_id> <interface>

这条命令允许用户把多个访问规则与特定的网络接口相关联起来。

accesslist_id 访问规则的标识（1~999）。这个值应该与用“**accesslist**”命令创建访问规则标识值相匹配。

interface 该访问规则将要控制的网络接口，可以为系统接口、聚合接口或 VLAN 接口。

例如：

```
Demo(config)#accessgroup 250 port1
```

no accessgroup <accesslist_id> <interface>

这条命令允许用户从指定接口上删除访问规则。

show accessgroup

显示所有的访问组配置。

clear accessgroup

删除所有“**accessgroup**”命令创建的规则与网络接口的关联。如果防火墙被启用并且没有设置允许访问规则，则所有的 TCP、UDP 或者 ICMP 包都不能通过防火墙，用户也不能通过 WebUI 访问设备，直到防火墙被禁用。

14.1.2 访问规则

以下命令需要和“**accessgroup**”命令配合使用。创建访问规则后，管理员必须运行“**accessgroup**”命令把新创建的访问规则标识绑定到接口上，并在该接口上启用防火墙功能，这些规则才生效。

```
accesslist permit {tcp|udp} <source_ip> {source_mask|source_prefix}  
<source_port> <destination_ip> {destination_mask|destination_prefix}  
<destination_port> <accesslist_id>
```

该命令用于创建一条 TCP 或 UDP 允许访问规则，并将该规则与指定的访问规则标识绑定。

source_ip	该参数指定需要允许的报文的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。
source_mask source_prefix	该参数指定需要允许的报文的源 IP 地址对应的子网掩码或前缀长度。 “source_mask”用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。 “source_prefix”用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。
source_port	该参数指定需要允许的报文的源端口号。取值必须为 0 至 65535 之间的整数。 取值为 0 时，表示所有端口。
destination_ip	该参数指定需要允许的报文的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。
destination_mask destination_prefix	该参数指定需要允许的报文的目的 IP 地址对应的子网掩码或前缀长度。 “destination_mask”用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。 “destination_prefix”用于配置 IPv6 地址对应的前

缀长度，取值必须为 0 到 128 之间的整数。

destination_port 该参数指定需要允许的报文的目的端口号。取值必须为 0 至 65535 之间的整数。

取值为 0 时，表示所有端口。

accesslist_id 该参数指定访问规则标识。取值必须为 1 至 999 之间的整数。

```
no accesslist permit {tcp|udp} <source_ip> {source_mask|source_prefix}  
<source_port> <destination_ip> {destination_mask|destination_prefix}  
<destination_port> <accesslist_id>
```

该命令用于删除一条 TCP 或 UDP 允许访问规则。

```
accesslist deny {tcp|udp} <source_ip> {source_mask|source_prefix}  
<source_port> <destination_ip> {destination_mask|destination_prefix}  
<destination_port> <accesslist_id>
```

该命令用于创建一条 TCP 或 UDP 拒绝访问规则，并将该规则与指定的访问规则标识绑定。

source_ip 该参数指定需要拒绝的报文的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。

source_mask|source_prefix 该参数指定需要拒绝的报文的源 IP 地址对应的子网掩码或前缀长度。

- “source_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。
- “source_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

source_port 该参数指定需要拒绝的报文的源端口号。取值必须为 0 至 65535 之间的整数。

取值为 0 时，表示所有端口。

destination_ip 该参数指定需要拒绝的报文的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

destination_mask|destination_prefix 该参数指定需要拒绝的报文的目的 IP 地址对应的子网掩码或前缀长度。

- “destination_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。

- “destination_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

destination_port 该参数指定需要拒绝的报文的目的端口号。取值必须为 0 至 65535 之间的整数。

取值为 0 时，表示所有端口。

accesslist_id 该参数指定访问规则标识。取值必须为 1 至 999 之间的整数。

no accesslist deny {tcp|udp} <source_ip> {source_mask|source_prefix} <source_port> <destination_ip> {destination_mask|destination_prefix} <destination_port> <accesslist_id>

该命令用于删除一条 TCP 或 UDP 拒绝访问规则。

accesslist permit {esp|ah|icmp echoreply|icmp echorequest} <source_ip> {source_mask|source_prefix} <destination_ip> {destination_mask|destination_prefix} <accesslist_id>

该命令用于创建一条 ESP、AH、ICMP Echo Reply 或 ICMP Echo Request 允许访问规则，并将该规则与指定的访问规则标识绑定。

source_ip 该参数指定需要允许的报文的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。

source_mask|source_prefix 该参数指定需要允许的报文的源 IP 地址对应的子网掩码或前缀长度。

- “source_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。
- “source_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

destination_ip 该参数指定需要允许的报文的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

destination_mask|destination_prefix 该参数指定需要允许的报文的目的 IP 地址对应的子网掩码或前缀长度。

- “destination_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。
- “destination_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

accesslist_id 该参数指定访问规则标识。取值必须为 1 至 999 之间的整数。



注意：

- ICMP Echo Reply 允许访问规则也允许内嵌了 Echo Request 的 Destination Unreachable 和 Time Exceeded 差错报文通过。不携带 Echo Request 的 Destination Unreachable 和 Time Exceeded 差错报文以及携带了 Echo Request 的其他 ICMP 差错报文不受该规则控制。
- ICMP Echo Request 允许访问规则也允许内嵌了 Echo Reply 的 Destination Unreachable 和 Time Exceeded 差错报文通过。不携带 Echo Reply 的 Destination Unreachable 和 Time Exceeded 差错报文以及携带了 Echo Reply 的其他 ICMP 差错报文不受该规则控制。

no accesslist permit {esp|ah|icmp echoreply|icmp echorequest}

<source_ip> {source_mask|source_prefix} <destination_ip>
{destination_mask|destination_prefix} <accesslist_id>

该命令用于删除一条 ESP、AH、ICMP Echo Reply 或 ICMP Echo Request 允许访问规则。

accesslist deny {esp|ah|icmp echoreply|icmp echorequest} <source_ip>

{source_mask|source_prefix} <destination_ip>
{destination_mask|destination_prefix} <accesslist_id>

该命令用于创建一条 ESP、AH、ICMP Echo Reply 或 ICMP Echo Request 拒绝访问规则，并将该规则与指定的访问规则标识绑定。

source_ip 该参数指定需要拒绝的报文的源 IP 地址。取值必须为 IPv4 或 IPv6 地址。

source_mask|source_prefix 该参数指定需要拒绝的报文的源 IP 地址对应的子网掩码或前缀长度。

- “source_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。
- “source_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

destination_ip 该参数指定需要拒绝的报文的目的 IP 地址。取值必须为 IPv4 或 IPv6 地址。

destination_mask|destination_prefix 该参数指定需要拒绝的报文的目的 IP 地址对应的子网掩码或前缀长度。

- “destination_mask” 用于配置 IPv4 地址对应的子网掩码，取值必须为点分地址格式或 0 到 32 之间的整数。

数。

- “destination_prefix” 用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。

accesslist_id 该参数指定访问规则标识。取值必须为 1 至 999 之间的整数。



注意：

- ICMP Echo Reply 拒绝访问规则也拒绝内嵌了 Echo Request 的 Destination Unreachable 和 Time Exceeded 差错报文通过。不携带 Echo Request 的 Destination Unreachable 和 Time Exceeded 差错报文以及携带了 Echo Request 的其他 ICMP 差错报文不受该规则控制。
- ICMP Echo Request 拒绝访问规则也拒绝内嵌了 Echo Reply 的 Destination Unreachable 和 Time Exceeded 差错报文通过。不携带 Echo Reply 的 Destination Unreachable 和 Time Exceeded 差错报文以及携带了 Echo Reply 的其他 ICMP 差错报文不受该规则控制。

no accesslist deny {esp|ah|icmp echoreply|icmp echorequest}

**<source_ip> {source_mask|source_prefix} <destination_ip>
{destination_mask|destination_prefix} <accesslist_id>**

该命令用于删除一条 ESP、AH、ICMP Echo Reply 或 ICMP Echo Request 拒绝访问规则。

show accesslist

该命令用于显示设备接口上已经配置的所有允许和拒绝访问规则。

clear accesslist

该命令用于删除所有的允许和拒绝访问规则。



注意：执行“**clear accesslist**”命令后，所有的 TCP、UDP 和 ICMP 报文都不能通过防火墙。

14.1.3 防火墙

webwall <interface> on [mode]

这条命令用来在指定接口上启用防火墙功能。

interface 该参数指定接口的名称，接口可以为系统接口、聚合接口、VLAN 接口或 VXLAN 接口。

mode 可选，该参数用于设置防火墙的模式。

- 0: 表示正常模式；所有的数据报都遵守 ACL 规则。出于安全因素考虑，默认模式为正常模式。
- 1: 表示 ACK 模式；在这个模式下，防火墙是兼容的，所有的 ACK TCP 数据报都被允许通过防火墙。

默认值为 0。

webwall <interface> off

这条命令用来在指定接口上禁用防火墙功能。通过禁用防火墙，设备允许数据报自由通过系统。使用者只应该为了诊断目的禁用防火墙，因为这样做会禁用所有访问规则。用户可以选择启用或者禁用指定接口的防火墙功能。使用集群技术的用户在配置防火墙功能以前，需要参考手册的“集群”章节。防火墙功能默认是禁用的。

例如：

```
Demo(config)#webwall port2 off
```

show statistics webwall [interface]

这条命令用来显示系统中所有接口上的防火墙功能的运行信息（已经启用了防火墙功能），包括允许访问、拒绝访问和动态允许访问等信息。如果指定了某个接口，则只显示该接口相关的防火墙运行信息。



注意：执行该命令前，请先启用“ip statistics on”命令。

show webwall

这条命令显示当前的防火墙配置信息。

clear statistics webwall [interface]

这条命令用于删除指定接口上的防火墙统计资料。如果没有指定接口，这条命令则删除所有启用防火墙的接口上的防火墙统计资料。

14.2 Web 应用防火墙（WAF）

waf profile name <profile_name>

该命令用于定义 Web 应用防火墙（Web Application Firewall，WAF）的 Security Profile。设备支持的 Security Profile 的最大数量根据系统内存的不同而有所区别。具体请参见下表。

profile_name	该参数指定 Security Profile 的名称。取值必须为长度不超过 40 个字节的字符串，区分大小写，支持数字、大

小写字母以及特殊字符“@”、“-”、“_”和“!”。如果取值包含特殊字符或只包含数字，则必须置于双引号内。

14.2.1.1.1 Security Profile 的最大数量

系统内存	Security Profile 的最大数量
4GB	16
8GB	32
16GB	64
32GB	128

no waf profile name <profile_name>

该命令用于删除指定的 Security Profile。

waf profile assign <profile_name> <virtual_service>

该命令用于将一个 Security Profile 和一个虚拟服务关联。一个 Security Profile 最多能和 4000 个虚拟服务关联，但是一个虚拟服务只能和一个 Security Profile 关联。

profile_name 该参数指定 Security Profile 的名称。

virtual_service 该参数指定 HTTP 和 HTTPS 类型的虚拟服务的名称。



注意：通过将 Security Profile 与虚拟服务关联，管理员可以在该虚拟服务上启用 WAF 功能。

no waf profile assign <profile_name> <virtual_service>

该命令用于删除 Security Profile 和指定的虚拟服务的关联关系。

waf profile mode {passive|active} <profile_name>

该命令用于设置指定 Security Profile 的工作模式。WAF 功能支持两种工作模式：被动（passive）模式和主动（active）模式。在被动模式下，系统检测攻击并记录日志，但是不阻断流量并且不向客户端发送错误页面。在主动模式下，系统可以检测攻击、记录日志、阻断流量并向客户端发送错误页面。默认情况下，WAF 功能工作在主动模式下。

profile_name 该参数指定 Security Profile 的名称。

waf profile predefine <profile_name> <ruleset_name> [action_name]
[priority]

该命令用于为指定的 Security Profile 配置预定义规则集。

profile_name	该参数指定 Security Profile 的名称。
ruleset_name	该参数指定预定义规则集的名称。支持的预定义规则集包括 SQL 注入攻击（Structured Query Language injection, SQL injection）和跨站脚本攻击（Cross Site Scripting, XSS）。取值必须为“sql”或“xss”，区分大小写。
action_name	可选。该参数指定发现攻击时采取的动作。取值必须为“pass”或“deny”。 - deny: 拒绝。当参数值为“deny”时，系统检测攻击，向客户端发送错误页面指明请求被阻断，并记录日志。注意：只有当指定的 Security Profile 工作在主动（active）模式下时，“deny”动作才能生效。 - pass: 通过。当参数值为“pass”时，系统检测攻击并记录日志。 默认值为“deny”。
priority	可选。该参数指定预定义规则集的优先级。取值必须为 1 至 2000 之间的整数。取值越大，优先级越高。注意：当预定义规则集的优先级相同时，执行顺序不确定。 默认值为 1000。

no waf profile predefine <profile_name> <ruleset_name>

该命令用于从指定的 Security Profile 中删除预定义规则集。

waf profile custom <profile_name> <ruleset_name> [action_name] [priority]

该命令用于为指定的 Security Profile 配置自定义规则集。系统允许配置最多 1024 个自定义规则集。

profile_name	该参数指定 Security Profile 的名称。
ruleset_name	该参数指定自定义规则集的名称。取值必须为长度不超过 64 个字节的字符串。
action_name	可选。该参数指定检测到攻击时采取的动作。取值必须为“pass”或“deny”。 - deny: 拒绝。当参数值为“deny”时，系统检测攻击，向客户端发送错误页面指明请求被阻断，并记录日志。注意：只有当指定的 Security Profile 工作在主动（active）模式下时，“deny”动作才能生效。 - pass: 通过。当参数值为“pass”时，系统检测攻击

并记录日志。

默认值为“deny”。

priority 可选。该参数指定自定义规则集的优先级。取值范围必须为 1 至 2000 之间的整数。取值越大，优先级越高。
注意：当自定义规则集的优先级相同时，执行顺序不确定。
默认值为 1000。



注意：当一个 Security Profile 同时配置了预定义规则集和自定义规则集时，根据规则集名称的 ASCII 码值从小到大顺序执行。

no waf profile custom <profile_name> <ruleset_name>

该命令用于从指定的 Security Profile 中删除自定义规则集。

waf import <ruleset_name|data_name> <url> [type]

该命令用于导入自定义规则集文件或自定义规则集相关的数据文件（data）。

ruleset_name|data_name 该参数指定自定义规则集文件或自定义规则集相关的数据文件的名称。取值必须为长度不超过 64 个字节的字符串。

url 该参数指定 HTTP 服务器或 FTP 服务器的 URL 地址。管理员可以通过该 URL 地址导入自定义规则集文件或自定义规则集相关的数据文件。

注意：FTP 类型 URL(ftp://user:password@host:port/path) 中的“path”需使用相对路径。

type 可选。该参数指定导入文件的类型。取值必须为“ruleset”或“data”。

默认值为“ruleset”。



注意：

1. 对于存在相关数据文件的自定义规则集，在导入自定义规则集前，必须先导入与自定义规则集相关的数据文件。
2. 系统支持大多数 Modsecurity 规则。关于 Modsecurity 规则的支持情况的细节请联系公司技术支持获取相关文档。

no waf import <ruleset_name|data_name>

该命令用于删除已经导入的指定的自定义规则集或自定义规则集相关的数据文件。

clear waf import

该命令用于清除已经导入的所有自定义规则集和与自定义规则集相关的数据文件。

show waf ruleset [keyword]

该命令用于显示系统中名称与指定字符串匹配的预定义规则集和自定义规则集。

keyword 可选。该参数指定用于匹配规则集名称的字符串。如果取值以数字开头，则必须置于双引号内，区分大小写。如不指定该参数，则显示系统中的所有预定义规则集和自定义规则集。

show waf data [keyword]

该命令用于显示系统中与指定名称字符串匹配的与自定义规则集相关的数据文件。

keyword 可选。该参数指定用于匹配与自定义规则集相关的数据文件的字符串。如果取值以数字开头，则必须置于双引号内，区分大小写。如不指定该参数，则显示所有与自定义规则集相关的数据文件。

show statistics waf [virtual_service]

该命令用于显示指定虚拟服务的 WAF 功能的相关统计信息。如果不指定参数“virtual_service”，则显示所有虚拟服务的 Web 功能的相关统计信息。

waf log audit {on|off}

该命令用于启用或禁用 WAF 的审计日志功能，该功能将记录 HTTP 流量的信息。如果禁用审计日志功能，将不会记录任何审计日志信息。该功能的默认设置为启用。

waf log audit server <url> <user_name> <password>

该命令用于为 WAF 定义第三方远程审计日志服务器。如果未定义第三方远程审计日志服务器，审计日志将存储在本地硬盘上；如果定义了第三方远程审计日志服务器，系统将发送审计日志到第三方远程审计日志服务器。只能定义一个第三方远程审计日志服务器。关于如何安装第三方远程审计日志服务器，请联系公司技术支持获取相关文档。

url 该参数指定第三方远程审计日志服务器的 URL 地址。
该参数不支持以下特殊字符：
“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“`”。

user_name	该参数指定用于登录第三方远程审计日志服务器的用户名。取值必须为长度不超过 64 个字节的字符串，区分大小写，支持数字、大小写字母以及特殊字符“@”、“-”、“_”和“!”。如果取值包含特殊字符或只包含数字，则必须置于双引号内。
password	该参数指定用于登录第三方远程审计日志服务器的密码。取值必须为长度不超过 32 个字节的字符串，支持数字、大小写字母以及特殊字符“@”、“-”、“_”和“!”。如果取值包含特殊字符或只包含数字，则必须置于双引号内。

**注意：**

1. 存放在本地硬盘上的审计日志的总大小不超过 2GB。当审计日志的总大小超过 2GB 时，新的审计日志将覆盖最早的审计日志。
2. 在使用命令“**waf log audit server**”定义第三方远程审计日志服务器前，需要确保该服务器可以正常工作。否则，审计日志将会丢失。
3. 审计日志不能同时存储在本地硬盘和第三方远程审计日志服务器上。

no waf log audit server

该命令用于删除 WAF 的第三方远程审计日志服务器。

waf update <url>

该命令用于更新预定义规则集。请联系公司技术支持获取预定义规则集的更新地址。

url	该参数指定 HTTP 服务器或 FTP 服务器的 URL 地址。管理员可以通过该 URL 地址更新预定义规则集。 注意：FTP 类型 URL(ftp://user:password@host:port/path) 中的“path”需使用相对路径。



注意：更新过程中，预定义规则集将被删除并更新，自定义规则集及与自定义规则集的相关数据文件将被保留。

clear waf config

该命令用于清除除了预定义规则集、自定义规则集和与自定义规则集相关的数据文件以外的 WAF 功能的所有配置。

14.3 高级访问控制

14.3.1 ACL 规则

acl rule <rule_name> <client_ip> {netmask|prefix} <acl_mode> <acl_type>
<max_limit>

该命令用于配置一条访问控制规则。如果客户端的 IP 地址在由参数 “client_ip” 和 “netmask|prefix” 确定的子网上，则该客户端受访问控制规则的限制。

系统允许最多配置 200 条访问控制规则。

rule_name	指定访问控制规则的名称。
client_ip	指定子网中一个客户端的 IP 地址。该参数的取值可以为 IPv4 地址或 IPv6 地址。
netmask prefix	指定子网的屏蔽或前缀长度。参数 “client_ip” 和 “netmask prefix” 确定一个子网。 • “netmask” 用于配置 IPv4 地址对应的子网掩码，其值应是点分地址格式或者 0 到 32 之间的整数。 • “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。
acl_mode	指定访问控制规则的控制模式。该参数的取值只能为 “total” 或 “per-ip”，区分大小写。 • “total” 表示指定子网中所有客户端作为一个整体受该控制规则的限制。 • “per-ip” 表示指定子网中每个客户端单独受该控制规则的限制。
acl_type	指定访问控制的控制类型。该参数的取值只能为 “cps” 或 “concurrent”，区分大小写。 • 当 “acl_mode” 的取值为 “total” 时：“cps” 表示该规则对子网中所有客户端的每秒新建连接数（CPS，connections per second）的总和进行限制。“concurrent” 表示该规则对子网中所有客户端的并发连接数（CC，concurrent connections）的总和进行限制。 • 当 “acl_mode” 的取值为 “per-ip” 时：“cps” 表示该规则对子网中每个客户端的每秒新建连接数进行限制。“concurrent” 表示该规则对子网中每个客户

端的并发连接数进行限制。

max_limit 指定每秒新建连接数或并发连接数的上限。该参数的取值范围为 1~4294967295。

例如：

```
Demo(config)#acl rule rule1 210.82.10.0 255.255.255.0 total cps 1000000
```



注意：配置的访问控制规则只对后续创建的连接生效，不对已有连接生效。

show acl rule [rule_name]

该命令用于显示指定的访问控制规则。如果不指定参数“rule_name”，系统将显示配置的所有访问控制规则。

no acl rule <rule_name>

该命令用于删除指定的访问控制规则。



注意：在删除访问控制规则之前，请确保该规则没有应用到任何单个虚拟服务或者全局虚拟服务。

clear acl rule

该命令用于删除所有的访问控制规则。



注意：在删除所有访问控制规则之前，请确保所有的访问控制规则都没有应用到任何单个虚拟服务或者全局虚拟服务。

acl whitelist <whitelist_name> <client_ip> {netmask|prefix}

该命令用于配置一个访问控制白名单。如果客户端的 IP 地址在由“client_ip”和“netmask|prefix”确定的子网上，则该客户端不受任何访问控制规则的限制。

系统允许最多配置 400 个访问控制白名单。

whitelist_name 指定访问控制白名单的名称。

client_ip 指定子网中一个客户端的 IP 地址。该参数的取值可以为 IPv4 地址或 IPv6 地址。

netmask|prefix 指定子网的屏蔽或前缀长度。

- “netmask”用于配置 IPv4 地址对应的子网掩码，其值应是点分地址格式或者 0 到 32 之间的整数。
- “prefix”用于配置 IPv6 地址对应的前缀长度，其

值应是一个 0 到 128 之间的整数。

show acl whitelist [whitelist_name]

该命令用于显示指定的访问控制白名单。如果不指定参数“whitelist_name”，系统将显示配置的所有访问控制白名单。

no acl whitelist <whitelist_name>

该命令用于删除指定的访问控制白名单。



注意：在删除访问控制白名单之前，请确保该白名单没有应用到任何单个虚拟服务或者全局虚拟服务。

clear acl whitelist

该命令用于删除所有的访问控制白名单。



注意：在删除所有访问控制白名单之前，请确保所有的白名单都没有应用到任何单个虚拟服务或者全局虚拟服务。

acl apply rule virtual <rule_name> <vs_name>

该命令用于把指定的访问控制规则应用于指定虚拟服务或全局虚拟服务。当客户端访问指定的虚拟服务时，如果匹配到了该访问控制规则，则受到该规则的限制。

rule_name 指定访问控制规则的名称。

vs_name 指定虚拟服务的名称。如果该参数的取值为“global”，表示该访问控制规则应用于全局虚拟服务。



注意：高级访问控制功能仅支持基于 TCP 协议的虚拟服务，例如 TCP 和 HTTP 类型虚拟服务。因此，只有当参数“vs_name”设置为基于 TCP 类型的虚拟服务的名称时，该命令配置才能生效。

show acl apply rule <rule_name>

该命令用于显示指定的访问控制规则应用到虚拟服务的配置，包含应用到单个虚拟服务以及全局虚拟服务的配置。

rule_name 指定访问控制规则的名称。

no acl apply rule virtual <rule_name> <vs_name>

该命令用于删除指定的访问控制规则应用到指定虚拟服务的配置。如果参数“vs_name”的取值为“global”时，系统将删除指定的访问控制规则应用到全局虚拟服务的配置。

clear acl apply rule virtual <vs_name>

该命令用于删除所有应用于指定虚拟服务的访问控制规则。如果参数“vs_name”的取值为“global”，系统将删除所有应用于全局虚拟服务的访问控制规则。

acl apply whitelist virtual <whitelist_name> <vs_name>

该命令用于把指定的访问控制白名单应用于指定虚拟服务或全局虚拟服务。当客户端访问指定的虚拟服务时，如果匹配到了该访问控制白名单，则不受到任何访问控制规则的限制。

whitelist_name	指定访问控制白名单的名称。
vs_name	指定虚拟服务的名称。如果该参数的取值为“global”，表示该访问控制白名单应用于全局虚拟服务。



注意：高级访问控制功能仅支持基于 TCP 协议的虚拟服务，例如 TCP 和 HTTP 类型虚拟服务。因此，只有当参数“vs_name”设置为基于 TCP 类型的虚拟服务的名称时，该命令配置才能生效。

show acl apply whitelist <whitelist_name>

该命令用于显示指定的访问控制白名单应用到虚拟服务的配置，包含应用到单个虚拟服务以及全局虚拟服务的配置。

whitelist_name	指定访问控制白名单的名称。

no acl apply whitelist virtual <whitelist_name> <vs_name>

该命令用于删除指定的访问控制白名单应用到指定虚拟服务的配置。如果参数“vs_name”的取值为“global”，系统将删除指定的访问控制白名单应用到全局虚拟服务的配置。

clear acl apply whitelist virtual <vs_name>

该命令用于删除所有应用于指定虚拟服务的访问控制白名单。如果参数“vs_name”的取值为“global”时，系统将删除所有应用于全局虚拟服务的访问控制白名单。

show acl apply virtual [vs_name]

该命令用于显示应用到指定虚拟服务的访问控制规则和访问控制白名单。

vs_name	可选，该参数指定虚拟服务的名称。 如果该参数的取值为“global”，则显示应用到全局虚拟服务的访问控制规则和访问控制白名单。 如果未指定该参数，系统将显示应用到单个虚拟服务以及全局虚拟服务的访问控制规则和访问控制白名单。

单。

clear acl all

该命令用于删除所有高级访问控制相关的配置。

show statistics acl rule [rule_name] [vs_name]

该命令用于显示指定的访问控制规则应用到指定虚拟服务的统计信息。

rule_name	可选，该参数指定访问控制规则的名称。 如果不指定参数“rule_name”，系统将显示所有访问控制规则应用到单个虚拟服务和全局虚拟服务的统计信息。
vs_name	可选，该参数指定虚拟服务的名称。只有指定了参数“rule_name”，该参数才可用。 如果该参数的取值为“global”，系统将显示指定的访问控制规则应用到全局虚拟服务的统计信息。 如果未指定该参数，系统将显示指定的访问控制规则应用到所有单个虚拟服务以及全局虚拟服务的统计信息。

show statistics acl whitelist [whitelist_name] [vs_name]

该命令用于显示指定的访问控制白名单应用到指定虚拟服务的统计信息。

whitelist_name	可选，该参数指定访问控制白名单的名称。 如果不指定参数“whitelist_name”，系统将显示所有访问控制白名单应用到单个虚拟服务和全局虚拟服务的统计信息。
vs_name	可选，该参数指定虚拟服务的名称。只有指定了参数“whitelist_name”，该参数才可用。 如果该参数的取值为“global”，系统将显示指定的访问控制白名单应用到全局虚拟服务的统计信息。 如果未指定该参数，系统将显示指定的访问控制白名单应用到所有单个虚拟服务以及全局虚拟服务的统计信息。

show statistics acl virtual [vs_name]

该命令用于显示应用到指定的虚拟服务的访问控制规则以及访问控制白名单的统计信息。

vs_name	可选，该参数指定虚拟服务的名称。 如果该参数的取值为“global”，系统将显示应用到全局虚拟服务的访问控制规则以及访问控制白名单的统计信息。 如果未指定该参数，系统将显示应用到所有单个虚拟服务和全局虚拟服务的访问控制规则以及访问控制白名单的统计信息。

clear statistics acl

该命令用于清除所有访问控制规则和访问控制白名单的相关统计信息。

14.3.2 HTTP ACL 规则

acl http rule <rule_name> <client_ip> {netmask|prefix} <acl_type>
<max_limit> <condition>

该命令用于配置一条 HTTP ACL 规则。系统支持最多配置 1000 条 HTTP ACL 规则。

rule_name	该参数指定 HTTP ACL 规则的名称。取值必须为长度不大于 40 个字节的字符串，支持字母、数字和特殊字符。取值包含特殊字符时，必须置于双引号内。
client_ip	该参数指定客户端的网络 IP 地址。取值必须为 IPv4 或 IPv6 地址。
netmask/prefix	该参数指定客户端网络 IP 地址对应的子网掩码或前缀长度。 “netmask”用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。
acl_type	该参数指定 HTTP ACL 规则的限速类型。取值必须为： - rps: 表示基于 RPS（request per second，每秒请求数）进行限速。 - throughput: 表示基于下载速度进行限速。
max_limit	该参数指定一个阈值。 当参数“acl_type”的取值为“rps”时，该参数指定 RPS 的阈值，取值必须为 1 至 20,000,000 之间的整

数。

- 当参数“acl_type”的取值为“throughput”时，该参数指定下载速度的阈值，单位为 KB/s。取值必须为 10 至 102,400 之间的整数。

condition

该参数指定 HTTP ACL 规则的匹配条件，取值必须为长度不大于 300 个字节的字符串。

1. 当参数“acl_type”的取值为“rps”时，该参数必须包含以下三个关键字：

- url: 表示针对该 URL 进行限速，格式为“url=<regex>url_regex”，“url_regex”的取值必须为长度不大于 256 个字节的正则表达式字符串。
- method: 表示 HTTP 访问方法，取值必须为“ALL”、“GET”、“POST”、“HEAD”、“PUT”或“DELETE”，格式为“method=value”，例如“method=ALL”。
- action: 表示当 RPS 超限后对 HTTP 请求的处理方法，取值必须为“errorpage”或“reset”，格式为“action=value”，例如“action=errorpage”。当取值为“action=errorpage”时，系统默认会返回内置的 480 错误页面。如果需要对 HTTP 请求进行重定向，可以通过命令“**http redirect error**”配置错误页面重定向。如果需要返回自定义的 480 错误页面，可以通过命令“**http import error**”和“**http error**”导入和启用自定义的 480 错误页面。如果同时配置了错误页面重定向和自定义的 480 错误页面，系统会优先返回重定向响应。当取值为“action=reset”时，如果 RPS 超限，系统会发送 RST 报文重置连接。

三个关键字之间用空格分隔后置于双引号内，例如

“url=<regex>abc* method=ALL action=reset”。

2. 当参数“acl_type”的取值为“throughput”时，该参数只能包含关键字“url”，格式为

“url=<regex>url_regex”，“url_regex”的取值必须为长度不大于 256 个字节的正则表达式字符串。

注意：关键字“url”的取值必须是与 Perl 兼容的正则表达式，该正则表达式必须以“<regex>”开头。如果需要匹配 Perl 的元字符，需要在元字符前加反斜杠“\”转义。系统支持的 Perl 元字符包括“^”、“.”、“+”、“*”、

“?”、“\$”、“[]”、“|”和“()”。例如，“*”表示匹配 0 或多个在它之前的字符。如果匹配“*”，要使用“*”作转义。

no acl http rule <rule_name>

该命令用于删除指定的 HTTP ACL 规则。删除一条 HTTP ACL 规则之前，需先解除该规则 and 所有虚拟服务之间的绑定关系。

show acl http rule [rule_name]

该命令用于显示指定的 HTTP ACL 规则。如果不指定参数“rule_name”，则显示所有的 HTTP ACL 规则。

clear acl http rule auto

该命令用于清除当前系统里所有动态 HTTP ACL 规则。执行该命令后，系统会重新生成动态 HTTP ACL 规则。

clear acl http rule manual

该命令用于清除管理员手动配置的所有 HTTP ACL 规则。

acl http apply rule virtual <rule_name> <virtual_service>

该命令用于将指定 HTTP ACL 规则与指定虚拟服务绑定。HTTP ACL 规则只有在绑定了虚拟服务之后才生效。系统支持最多配置 10,000 条绑定关系。

rule_name 该参数指定 HTTP ACL 规则的名称。

virtual_service 该参数指定虚拟服务的名称。

no acl http apply rule virtual <rule_name> <virtual_service>

该命令用于解除指定 HTTP ACL 规则与指定虚拟服务之间的绑定关系。

show acl http apply rule <rule_name>

该命令用于显示指定 HTTP ACL 规则绑定的所有虚拟服务。

show acl http apply virtual [virtual_service]

该命令用于显示指定虚拟服务绑定的 HTTP ACL 规则。如不指定参数“virtual_service”，则显示所有虚拟服务绑定的 HTTP ACL 规则。

show acl http all

该命令用于显示所有的 HTTP ACL 规则和绑定的虚拟服务，以及这些 HTTP ACL 规则应用到各个虚拟服务的统计信息。

clear acl http apply rule virtual <virtual_service>

该命令用于清除指定虚拟服务与所有 HTTP ACL 规则之间的绑定关系。

show statistics acl http virtual [virtual_service]

该命令用于显示 HTTP ACL 规则应用到指定虚拟服务的统计信息。如果不指定参数“virtual_service”，则显示 HTTP ACL 规则应用到所有虚拟服务的统计信息。

14.3.3 DNS ACL 规则

**acl dns rule <rule_name> <client_ip> {netmask|prefix} <acl_mode>
<dns_type> <max_limit>**

该命令用于配置一条 DNS ACL 规则。系统支持最多配置 1000 条 DNS ACL 规则。

rule_name	该参数指定 DNS ACL 规则的名称。取值必须为长度不大于 40 个字节的字符串，支持字母、数字和特殊字符。取值包含特殊字符时，必须置于双引号内。
client_ip	该参数指定客户端的网络 IP 地址。取值必须为 IPv4 或 IPv6 地址。
netmask/prefix	该参数指定客户端网络 IP 地址对应的子网掩码或前缀长度。 “netmask”用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。 “prefix”用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。
acl_mode	该参数指定 DNS ACL 规则的控制模式。取值必须为“total”或“per-ip”，区分大小写： - total: 表示指定子网中所有客户端作为一个整体受该 DNS ACL 规则的限制。 - per-ip: 表示指定子网中每个客户端单独受该控制规则的限制。
dns_type	该参数指定请求的 DNS 资源记录类型，取值必须为“A”、“NS”、“MD”、“MF”、“CNAME”、“SOA”、“MB”、“MG”、“MR”、“NULL”、“WKS”、“PTR”、“HINFO”、“MINFO”、“MX”、“TXT”、“AAAA”、“ANY”、“OTHERS”或者“ALL”，区分大小写。取值“ALL”表示所有 DNS 资源记录类型。
max_limit	该参数指定每秒 DNS 查询请求的最大数量，取值必须

为 1 至 4,294,967,295 之间的整数。

no acl dns rule <rule_name>

该命令用于删除指定的 DNS ACL 规则。

show acl dns rule [rule_name]

该命令用于显示指定的 DNS ACL 规则。如不指定参数“rule_name”，则显示所有 DNS ACL 规则。

clear acl dns rule auto

该命令用于清除系统自动生成的所有 DNS ACL 规则。执行该命令后，系统将重新计算和生成 DNS ACL 规则。

clear acl dns rule manual

该命令用于清除管理员手动配置的所有 DNS ACL 规则。

acl dns apply rule virtual <rule_name> <virtual_service>

该命令用于将指定 DNS ACL 规则与指定虚拟服务绑定。DNS ACL 规则只有在绑定了虚拟服务之后才生效。系统支持最多配置 40,000 条绑定关系。

rule_name 该参数指定 DNS ACL 规则的名称。

virtual_service 该参数指定虚拟服务的名称，取值必须为：

- DNS 虚拟服务名称：表示将 DNS ACL 规则与该虚拟服务绑定。
- global：表示将 DNS ACL 规则与所有 DNS 虚拟服务绑定。

no acl dns apply rule virtual <rule_name> <virtual_service>

该命令用于解除指定 DNS ACL 规则与指定虚拟服务之间的绑定关系。

show acl dns apply rule <rule_name>

该命令用于显示指定 DNS ACL 规则绑定的所有虚拟服务。

show acl dns apply virtual [virtual_service]

该命令用于显示指定虚拟服务绑定的 DNS ACL 规则。如不指定参数“virtual_service”，则显示所有虚拟服务绑定的 DNS ACL 规则。

show acl dns all

该命令用于显示所有的 DNS ACL 规则和绑定的虚拟服务，以及各个虚拟服务绑定的 DNS ACL 规则的匹配统计数据以及全局 SDNS 绑定的所有的 DNS ACL 规则，各个 SDNS 域名绑定的 DNS ACL 规则的匹配统计数据。

clear acl dns apply rule virtual <virtual_service>

该命令用于解除指定虚拟服务与所有 DNS ACL 规则的绑定关系。

virtual_service

该参数指定虚拟服务的名称，取值必须为：

- DNS 虚拟服务名称：表示解除该虚拟服务与所有 DNS ACL 规则的绑定关系。
- global：表示解除所有 DNS 虚拟服务与 DNS ACL 规则的绑定关系。

show statistics acl dns virtual [virtual_service]

该命令用于显示 DNS ACL 规则应用到指定虚拟服务的统计信息。如果不指定参数“virtual_service”，则显示 DNS ACL 规则应用到所有虚拟服务的统计信息。

acl dns apply rule sdns <rule_name> [host_name] [action]

该命令用于为全局 SDNS 和单个 SDNS 域名绑定一条 DNS ACL 规则。系统默认为全局 SDNS 绑定 DNS ACL 规则。

- 如果为全局绑定了 DNS ACL 规则，系统将限制全局 SDNS 的 DNS 查询请求数。
- 如果为单个域名绑定了 DNS ACL 规则，系统将限制单个域名的 DNS 查询请求数。
- 如果同时为全局和单个域名绑定了 DNS ACL 规则，系统会优先处理全局绑定的 DNS ACL 规则。

系统支持为一个域名绑定多条 DNS ACL 规则。如果一个域名绑定多条 DNS ACL 规则，系统会按照绑定规则的先后顺序进行处理。

rule_name

该参数指定 DNS ACL 规则的名称。

host_name

可选，该参数指定一个已有的 SDNS 域名。

- 如果指定该参数，系统为指定的 SDNS 域名绑定一条 DNS ACL 规则。
- 如果不指定该参数，系统为全局 SDNS 绑定一条 DNS ACL 规则。

默认值为空。

action

可选，该参数指定 DNS 请求匹配 DNS ACL 规则时系统

的处理动作，取值必须为：

- 0：表示系统仅告警。
- 1：表示系统告警并且防护。

默认值为 1。



注意：启用 DDoS 功能后，系统不会为该命令根据流量实时生成 DNS ACL 规则。

no acl dns apply rule sdns <rule_name> [host_name]

该命令用于解除指定 DNS ACL 规则与全局 SDNS 或单个 SDNS 域名的绑定关系。

rule_name 该参数指定 DNS ACL 规则的名称。

host_name 可选，该参数指定一个已有的 SDNS 域名。

- 如果指定该参数，系统将为指定的 SDNS 域名解除绑定关系。
- 如果不指定该参数，系统将为全局 SDNS 解除绑定关系。

show acl dns apply sdns [host_name]

该命令用于显示与指定的 SDNS 域名绑定的所有 DNS ACL 规则。当不指定参数“host_name”时，系统将显示全局 SDNS 绑定的所有 DNS ACL 规则。

clear acl dns apply rule sdns [host_name]

该命令用于解除指定的 SDNS 域名绑定的所有 DNS ACL 规则。当不指定参数“host_name”时，系统将解除全局 SDNS 绑定的所有 DNS ACL 规则。

show statistics acl dns sdns [host_name]

该命令用于显示 DNS ACL 规则应用到指定的 SDNS 域名的统计信息。当不指定参数“host_name”时，系统将显示 DNS ACL 规则应用到全局 SDNS 的统计信息。

14.4 DDoS 攻击防御

ddos {on|off}

该命令用于启用或禁用系统的 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击防御功能。该功能默认设置为禁用。

topn {on|off} <protocol_type>

该命令用于对指定协议类型启用或禁用实时流量 TopN 统计功能。启用该功能后，系统将统计 IP、TCP、UDP 和 ICMP 流量中的 Top 10 客户端和服务端。该功能的默认设置为禁用。

protocol_type 该参数指定协议类型，取值必须为“ip”、“tcp”、“udp”或“icmp”。

show topn status <type>

该命令用于显示指定协议类型的 Top10 流量客户端和服务端。

show topn settings

该命令用于显示实时流量 TopN 统计功能的开启状态。

clear topn settings

该命令用于将实时流量 TopN 统计功能恢复为默认状态。

show ddos settings

该命令用于显示 DDoS 相关的所有攻击防御功能的开启状态和相关配置。

clear ddos settings

该命令用于将 DDoS 相关的所有攻击防御功能和相关配置恢复为默认设置。

show ddos blacklist

该命令用于显示 DDoS 黑名单。该命令只显示最近的 2000 条黑名单记录。如果系统重启，所有的黑名单记录都会清空。

clear ddos blacklist

该命令用于清除所有的 DDoS 黑名单记录。

show ddos record [filter_string] [start_date] [end_date]

该命令用于显示指定时间段内匹配指定过滤字符串的 DDoS 攻击相关日志。

filter_string 可选。该参数指定用于匹配 DDoS 攻击记录的过滤字符串。如不指定该参数，则显示指定时间段内的所有 DDoS 攻击相关记录。

start_date 可选。该参数指定起始日期。取值必须为“yyyymmdd”格式，其中“yyyy”的取值应该为 2000 至 2037 之间的整数。如不指定该参数，则显示所有 DDoS 攻击日志。

end_date 该参数指定结束日期。取值必须为“yyyymmdd”格式，且大于参数“start_date”的取值。如不指定该参数，则显示所有 DDoS 攻击日志。

ddos record export <remote_file_path>

该命令用于将 DDoS 攻击相关记录备份至指定的 URL 地址。

remote_file_path 该参数指定用于保存记录的 URL 地址，取值必须包含存放文件的目录，例如“ftp://10.8.3.28/record/”。只支持 FTP 类型的 URL 地址。

注意：FTP 类型 URL(ftp://user:password@host:port/path) 中的“path”需使用相对路径。

clear ddos record

该命令用于清除系统中的所有 DDoS 攻击相关记录。

14.4.1 TCP DDoS**ddos tcp {on|off}**

该命令用于启用或禁用 TCP DDoS 攻击防御功能。当系统的 DDoS 攻击防御功能为禁用状态时，TCP DDoS 攻击防御功能不生效。该功能的默认设置为启用。

show statistics ddos tcp

该命令用于显示 TCP DDoS 攻击相关统计数据。

clear statistics ddos tcp

该命令用于清除 TCP DDoS 攻击相关统计数据。

14.4.2 UDP DDoS**ddos udp {on|off}**

该命令用于启用或禁用 UDP DDoS 攻击防御功能。当系统的 DDoS 攻击防御功能为禁用状态时，UDP DDoS 攻击防御功能不生效。该功能的默认设置为启用。

show statistics ddos udp

该命令用于显示 UDP DDoS 攻击相关统计数据。

clear statistics ddos udp

该命令用于清除 UDP DDoS 攻击相关统计数据。

14.4.3 DNS DDoS**ddos dns {on|off}**

该命令用于启用或禁用 DNS DDoS 攻击防御功能。当系统的 DDoS 攻击防御功能为禁用状态时，DNS DDoS 攻击防御功能不生效。该功能的默认设置为启用。

show statistics ddos dns

该命令用于显示 DNS DDoS 攻击（包括基于 TCP、UDP 协议的 DNS DDoS 攻击）相关统计数据。

clear statistics ddos dns all

该命令用于清除所有 DNS（包括基于 TCP 和 UDP 协议的 DNS）虚拟服务上所有资源类型的 DDoS 统计数据。

clear statistics ddos dns virtual <virtual_service> [dns_type]

该命令用于清除指定虚拟服务上指定资源类型的 DDoS 统计数据。

virtual_service	该参数指定 DNS 虚拟服务的名称。
dns_type	可选。该参数指定 DNS 资源类型，取值必须为“A”、“NS”、“MD”、“MF”、“CNAME”、“SOA”、“MB”、“MG”、“MR”、“NULL”、“WKS”、“PTR”、“HINFO”、“MINFO”、“MX”、“TXT”、“AAAA”、“ANY”、“OTHERS”或者“ALL”。 默认值为“ALL”。

14.4.4 SSL DDoS

ddos ssl handshake timeout [timeout]

该命令用于设置 SSL 握手的超时时间。TCP 连接建立后，如果系统未在指定时间内收到 SSL 握手消息或应用数据，系统会重置连接，并记录一次 SSL 握手超时攻击。如不配置该命令，系统会在初始启动时采用 10,000 ms 作为默认的超时时间。随着实际的流量变化，系统会生成一个动态的超时时间，然后按照动态生成的超时时间进行探测。如果使用该命令自定义了一个超时时间，则动态生成的超时时间不生效。

timeout	可选。该参数指定 SSL 握手的超时时间。取值必须为 0 至 7,200,000 之间的整数，单位为毫秒。取值为 0 时，系统不检查 SSL 握手是否超时。 默认值为 10,000。

no ddos ssl handshake timeout

该命令用于将 SSL 握手超时时间恢复为系统的默认配置。执行该命令后，系统会按照动态生成的超时时间进行探测。

ddos ssl renegotiation interval [interval]

该命令用于设置 SSL 重协商的时间间隔阈值。如果两个重协商请求之间的时间间隔小于指定阈值，则重置连接，并记录一次 SSL 重协商攻击。如不配置该参数“interval”，默认值为 10000 毫秒。

interval 可选。该参数指定 SSL 重协商的时间间隔阈值。取值必须为 1 至 7,200,000 之间的整数，单位为毫秒。
默认值为 10,000。

no ddos ssl renegotiation interval

该命令用于将 SSL 重协商时间间隔阈值恢复为系统的默认配置。

show ddos threshold ssl

该命令用于显示系统自动生成的 SSL 握手超时时间。

clear ddos threshold ssl

该命令用于清除系统自动生成的 SSL 握手超时时间。执行该命令后，系统会根据实时流量重新生成动态的 SSL 握手超时时间。

show statistics ddos ssl [virtual_service]

该命令用于显示生成动态 SSL 攻击阈值所需的相关统计信息。

clear statistics ddos ssl [virtual_service]

该命令用于清除生成动态 SSL 攻击阈值所需的相关统计信息。

14.4.5 HTTP DDoS

ddos http verify {on|off}

该命令用于启用或禁用 HTTP 验证功能。启用该功能后，系统会对可疑客户端进行验证，判断对方是否是攻击者。该功能的默认设置为禁用。

ddos http acl blacklist {on|off}

该命令用于控制是否将发起 HTTP DDoS 攻击的客户端的客户端 IP 地址自动添加到 ACL 黑名单。该功能的默认设置为禁用。

ddos http slow interval [interval]

该命令用于设置 HTTP 数据报的时间间隔阈值，如果一个 HTTP 头部或 POST 消息分成多个数据报传输，而且两个数据报到达的时间间隔超过指定阈值，则记录一次超时，累计超时三次，则重置连接，并记录一次 Slowloris 攻击或 Slowpost 攻击。如不配置该命令，系统会在初始启动时采用 2000 ms 作为默认阈值。随着

实际的流量变化,系统会生成一个动态阈值,然后按照动态生成的阈值进行探测。如果使用该命令自定义了一个阈值,则动态生成的阈值不生效。

interval 可选。该参数指定 HTTP 数据报到达的时间间隔阈值。取值必须为 0 至 7,200,000 之间的整数,单位为毫秒。取值为 0 时,系统不检查 HTTP 数据报到达的时间间隔。默认值为 2000。

no ddos http slow interval

该命令用于将 HTTP 数据报的时间间隔阈值恢复为系统的默认配置。执行该命令后,系统会按照动态生成的阈值进行探测。

ddos http resptime <method> <interval>

该命令用于通过指定的 HTTP 方法对 HTTP 服务器的响应速度进行探测,并设置 HTTP 服务器的响应时间阈值。如果所有 HTTP 服务器的平均响应时间超过指定的阈值并持续超过 30s,则认为服务器可能遭受了攻击。如不配置该命令,系统会在初始启动时按照以下默认配置进行探测。

- **ddos http resptime get 100**
- **ddos http resptime post 100**
- **ddos http resptime head 100**
- **ddos http resptime put 100**
- **ddos http resptime delete 100**

随着实际的流量变化,系统会生成动态阈值,然后按照动态生成的阈值进行探测。如果使用该命令自定义了一个阈值,则动态生成的阈值不生效。。

method 该参数指定用于探测的 HTTP 请求方法,取值必须为“get”、“post”、“head”、“put”或“delete”。

interval 该参数指定 HTTP 服务器的响应时间阈值,取值必须为 1 至 10,000 之间的整数,单位为毫秒。默认值为 100。

no ddos http resptime <method>

该命令用于将 HTTP 服务器对指定类型 HTTP 请求的响应时间阈值恢复为系统的默认配置。执行该命令后,系统会按照动态生成的阈值进行探测。

ddos http kvincookie <count>

该命令用于设置 HTTP 请求里携带的 cookie 个数阈值。如果请求里 cookie 的个数超过指定的阈值,则认为服务器可能遭受了攻击。如不配置该命令,系统会在

初始启动时采用 10 个作为默认阈值。随着实际流量的变化，系统会生成一个动态阈值，并按照动态生成的阈值进行探测。如果使用该命令自定义了请求里携带的 cookie 个数阈值，则动态生成的阈值不生效。

count 该参数指定 HTTP 请求里携带的 cookie 个数的阈值。取值必须为 1 至 100 之间的整数。

默认值为 10。

no ddos http kvincookie

该命令用于将 HTTP 请求里携带的 cookie 个数阈值恢复为系统的默认配置。执行该命令后，系统会按照动态生成的阈值进行探测。

ddos http querycnt <count>

该命令用于设置 URL 里携带的 query 个数阈值。如果 query 的个数超过指定的阈值，则认为服务器可能遭受了攻击。如不配置该命令，系统会在初始启动时采用 10 个作为默认阈值。随着实际流量的变化，系统会生成一个动态阈值，并按照动态生成的阈值进行探测。如果使用该命令自定义了 URL 里携带的 query 个数阈值，则动态生成的阈值不生效。

count 该参数指定 HTTP 请求 URL 里携带的 cookie 个数的阈值。取值必须为 1 至 100 之间的整数。

默认值为 10。

no ddos http querycnt

该命令用于将 URL 里携带的 query 个数阈值恢复为系统的默认配置。执行该命令后，系统会按照动态生成的阈值进行探测。

show ddos threshold http [virtual_service]

该命令用于显示系统为指定虚拟服务动态生成的 HTTP 攻击阈值，包括 HTTP 服务器的响应时间阈值、HTTP 请求里携带的 cookie 个数阈值以及 HTTP 请求 URL 里携带的 query 个数阈值。如不指定参数“virtual_service”，则显示系统为所有虚拟服务动态生成的 HTTP 攻击阈值。

clear ddos threshold http [virtual_service]

该命令用于清除系统为指定虚拟服务动态生成的 HTTP 攻击阈值，包括 HTTP 服务器的响应时间阈值、HTTP 请求里携带的 cookie 个数阈值以及 HTTP 请求 URL 里携带的 query 个数阈值。如不指定参数“virtual_service”，则清除系统为所有虚拟服务动态生成的 HTTP 攻击阈值。执行该命令后，系统会重新生成动态 HTTP 攻击阈值。

show statistics ddos http [virtual_service]

该命令用于显示指定虚拟服务上 HTTP DDoS 攻击相关统计信息。如不指定参数“virtual_service”，则显示所有虚拟服务上 HTTP DDoS 攻击相关统计信息。

clear statistics ddos http [virtual_service]

该命令用于清除指定虚拟服务上 HTTP DDoS 攻击相关统计信息。如不指定参数“virtual_service”，则清除所有虚拟服务上 HTTP DDoS 攻击相关统计信息。

14.4.6 ACL 黑名单

acl blacklist {on|off}

该命令用于启用或禁用 ACL 黑名单功能。启用该功能后，系统会对所有报文的源 IP 进行检查，如果源 IP 匹配 ACL 黑名单，则丢弃报文。该功能的默认设置为禁用。

acl blacklist rule <ip> <netmask|prefix> [timeout]

该命令用于将指定的 IP 地址或子网添加到 ACL 黑名单中，并设置超时时间。到达指定的超时时间后，该 IP 地址或子网将会被移出当前的 ACL 黑名单。

ip	该参数指定需要添加到 ACL 黑名单的 IP 地址或子网地址。
netmask prefix	该参数指定需要添加到 ACL 黑名单的 IP 地址对应的子网掩码或前缀长度。 • 参数“netmask”用于配置 IPv4 地址对应的子网掩码，取值应为点分地址格式或一个 0 至 32 之间的整数。 • 参数“prefix”用于配置 IPv6 地址对应的前缀长度，取值必须为 0 到 128 之间的整数。
timeout	可选，该参数指定添加到 ACL 黑名单的 IP 地址或子网的超时时间，取值必须为 0 至 1440 之间的整数，单位为分钟。取值为 0 表示永不超时。 默认值为 0。

no acl blacklist rule <ip> <netmask|prefix>

该命令用于手动将指定的 IP 地址或子网移出 ACL 黑名单。

show acl blacklist rule manual

该命令用于显示通过“acl blacklist rule”命令添加到 ACL 黑名单的所有 IP 地址和子网。

clear acl blacklist rule manual

该命令用于清除通过“**acl blacklist rule**”命令添加到 ACL 黑名单的所有 IP 地址和子网。

show acl blacklist rule auto

该命令用于显示系统安全模块动态生成的所有 ACL 黑名单。

acl blacklist ipfile generate <security_module> <filename>

该命令用于将系统为指定安全模块动态生成的 ACL 黑名单保存到指定的本地文件里。

security_module	该参数指定安全模块的名称，取值必须为“ddos”或“waf”，区分大小写。
filename	该参数指定用于存放 ACL 黑名单的本地文件名称，取值必须为长度不超过 24 个字节的字符串。

clear acl blacklist rule auto

该命令用于清除系统动态生成的所有 ACL 黑名单。

acl blacklist import <remote_file_path> [filename]

该命令用于从指定的 URL 地址导入一个自定义的 IP 列表文件。每个导入的 IP 列表文件的大小不能超过 1000 KB。

remote_file_path	该参数指定需要导入的 IP 列表文件的 URL 地址，取值必须包含需要导入的 IP 列表文件名称，支持 HTTP 和 FTP 类型的 URL 地址，例如“ftp://10.8.3.28/iplist”。
filename	可选，该参数用于为导入的 IP 列表文件重命名，取值必须为长度不超过 24 个字节的字符串。如不指定该参数，IP 列表文件名称不变。

clear acl blacklist ipfile [filename]

该命令用于清除指定的 IP 列表文件。如不指定参数“filename”，则清除所有的 IP 列表文件。

acl blacklist export <local_file> <remote_file_path>

该命令用于将一个 IP 列表文件导出到指定的 URL 地址。

local_file	该参数指定需要导出的 IP 列表文件的名称。
remote_file_path	该参数指定用于保存导出的 IP 列表文件的 URL 地址，取值必须包含文件目录，例如“ftp://10.8.3.28/”。仅支持 FTP 类型的 URL 地址。

注意：FTP 类型 URL(ftp://user:password@host:port/path)

中的“path”需使用相对路径。

acl blacklist ipfile apply <filename> [timeout]

该命令用于将指定的 IP 列表文件添加到 ACL 黑名单中，并设置超时时间。到达指定的超时时间后，该 IP 列表文件将被移出 ACL 黑名单。系统支持添加最多 10 个 IP 列表到 ACL 黑名单。

filename	该参数指定 IP 列表文件的名称。
timeout	可选，该参数指定 IP 列表文件的超时时间，取值必须为 0 至 1440 之间的整数，单位为分钟。取值为 0 表示永不超时。 默认值为 0。

no acl blacklist ipfile apply <filename>

该命令用于手动将指定 IP 列表文件从 ACL 黑名单中移除。

show acl blacklist ipfile apply

该命令用于显示当前被加入到 ACL 黑名单中的所有 IP 列表文件。

clear acl blacklist apply

该命令用于手动将所有 IP 列表文件从 ACL 黑名单中移除。

show acl blacklist ipfile filename [filename]

该命令用于显示指定 IP 列表文件中包含的 IP 地址。如不指定参数“filename”，则显示所有通过“acl blacklist import”命令导入的 IP 列表文件的名称。

show acl blacklist match <ip>

该命令用于查看 ACL 黑名单中是否包含指定的 IP 地址。

ip	该参数指定需要查看的 IP 地址。

show acl blacklist settings

该命令用于显示 ACL 黑名单功能的启用状态及所有相关配置。

show acl blacklist status

该命令用于显示所有 ACL 黑名单的超时状态，包括通过“acl blacklist rule”命令配置和系统自动生成的 ACL 黑名单以及通过“acl blacklist ipfile apply”命令应用到 ACL 黑名单的 IP 列表文件的超时状态。

clear acl blacklist all

该命令用于将 ACL 黑名单功能恢复为默认配置并清除所有相关配置。

acl blacklist source tcptoption <tcp_option_kind> [offset]

该命令用于配置一条黑名单匹配规则，检查指定的 TCP 选项中的客户端 IP 地址是否匹配黑名单。

配置该命令后，当 ACL 黑名单功能启用时（“**acl blacklist on**”），在收到客户端的 TCP 握手或数据报文时，除了源 IP 地址以外，系统还会将指定的 TCP 选项中的客户端 IP 地址与 ACL 黑名单进行匹配。当源 IP 和 TCP 选项中的客户端 IP 中有任意一个匹配黑名单时，就会触发黑名单丢弃报文。

tcp_option_kind 该参数指定 TCP 选项的 kind 值，取值必须为 20 至 252 之间的整数。

offset 可选，该参数指定 TCP 选项 kind 的 Value 字段的偏移量，单位为字节，取值必须为 0 至 4 之间的整数。
默认值为 0。

no acl blacklist source tcptoption

该命令用于删除 “**acl blacklist source tcptoption**” 命令的配置。

show acl blacklist source tcptoption

该命令用于显示 “**acl blacklist source tcptoption**” 命令的配置。

show statistics acl blacklist

该命令用于显示当前 ACL 黑名单的所有统计信息。

clear statistics acl blacklist

该命令用于清除当前 ACL 黑名单的所有统计信息。

第15章 IPv6 高级配置

15.1 DNS64 和 NAT64

ipv6 dns64 on <dns_vs_name> [priority_mode]

该命令用于为指定的 DNS 类型的虚拟服务启用 DNS64 功能并设置资源优先模式。默认情况下，系统禁用 DNS64 功能。

DNS64 功能将 IPv6 客户端发送的 DNS AAAA 请求转换为 DNS A 请求，然后把 DNS A 响应转换成 DNS AAAA 响应，确保了 IPv6 客户端能够访问 IPv4 服务器。

在整个系统中，DNS64 功能只能启用在一个 DNS 类型的虚拟服务上。

dns_vs_name 该参数指定 DNS 类型的虚拟服务的名称。

priority_mode 可选，该参数指定资源优先模式，取值必须为：

- **A**: 优先将 DNS A 请求发往 DNS A 服务器，优先选择 DNS A 响应。
- **AAAA**: 优先将 DNS AAAA 请求发往 DNS AAAA 服务器，优先选择 DNS AAAA 响应。
- **Response**: 将 DNS A 请求发往 DNS A 服务器，DNS AAAA 请求发往 DNS AAAA 服务器，优先选择先收到的响应中的资源记录。

以上取值不区分大小写。默认值为“AAAA”。

ipv6 dns64 off <dns_vs_name>

该命令用于为指定的 DNS 类型的虚拟服务禁用 DNS64 功能。

ipv6 dns64 prefix <dns64_prefix>

该命令用于设置 DNS64 功能所使用的 IPv6 地址前缀。DNS64 功能通过在 A 记录添加该前缀得到转换的 AAAA 记录。

dns64_prefix 指定 DNS64 功能使用的 IPv6 地址前缀。该参数的固定长度为 96 比特。默认值为 64:ff9b::。

show ipv6 dns64 settings

该命令用于显示与 DNS64 功能相关的设置。

clear ipv6 dns64 settings

该命令用于删除与 DNS64 功能相关的设置，并恢复 DNS64 功能相关的默认设置。

ipv6 nat64 on

该命令用于启用 NAT64（Network Address Translation IPv6 to IPv4）功能。默认情况下，系统禁用 NAT64 功能。

NAT64 功能将客户端发送的 IPv6 报文转换为 IPv4 报文，然后将 IPv4 报文转换成 IPv6 报文。这样确保了 IPv6 客户端能与 IPv4 服务器正常通信。

ipv6 nat64 off

该命令用于禁用 NAT64 功能。

ipv6 nat64 ippool <ipv4_pool_name>

该命令用于设置 NAT64 功能使用的全局 IPv4 地址池。当设备收到 IPv6 客户端的 IPv6 报文时，NAT64 功能将报文中的 IPv6 源地址转换成 IPv4 地址池中的地址。

ipv4_pool_name 指定 IPv4 地址池的名称。

no ipv6 nat64 ippool <ipv4_pool_name>

该命令用于删除 NAT64 功能使用的全局 IPv4 地址池。

ipv6 nat64 prefix <nat64_prefix>

该命令用于设置 NAT64 功能使用的 IPv6 地址前缀。当设备收到 IPv6 客户端的报文时，NAT64 功能将去掉目的地址的 IPv6 地址前缀，得到后台服务器的 IPv4 地址。

nat64_prefix 指定 NAT64 功能使用的 IPv6 地址前缀。该参数的固定长度为 96 比特。

如果需要 NAT64 功能和 DNS64 功能在一台设备上配合使用，请确保该参数的取值与命令“**ipv6 dns64 prefix <dns64_prefix>**”中参数“dns64_prefix”的取值相同。



注意：如果设备收到的 IPv6 报文的目的地址既匹配上了参数“dns64_prefix”，又匹配上了其它的 VIP 地址，那么这些 IPv6 报文将不会命中 NAT64。因此，NAT64 将不会用来转发这些 IPv6 报文。

ipv6 nat64 timeout <idle_timeout>

该命令用于设置 NAT64 TCP 连接的空闲超时时间。

idle_timeout 指定 NAT64 TCP 连接的空闲超时时间，单位为秒。该参数的取值范围为 60~7200，默认值为 300。

show ipv6 nat64 connection

该命令用于显示 NAT64 连接的地址转换信息。

show ipv6 nat64 settings

该命令用于显示与 NAT64 功能相关的设置。

clear ipv6 nat64 settings

该命令用于删除与 NAT64 功能相关的设置，并恢复 NAT64 功能相关的默认设置。

15.2 DNS46 和 NAT46

ipv6 dnsnat46 on <dns_vs_name> [priority_mode]

该命令用于为指定的 DNS 类型的虚拟服务同时启用 DNS46 功能和 NAT46 功能，并设置资源优先模式。默认情况下，系统禁用 DNS46 功能和 NAT46 功能。

DNS46 功能将 IPv4 客户端发出的 DNS A 请求转换为 DNS AAAA 请求，然后将返回的 DNS AAAA 响应转换为 DNS A 记录响应，并建立一条 IPv6 地址到 IPv4 地址的映像记录。设备返回转换后的 IPv4 地址给 IPv4 客户端。当 IPv4 客户端使用该 IPv4 地址访问 IPv6 服务器时，NAT46 功能根据已经建立的映像记录将客户端发送的 IPv4 报文转换为 IPv6 报文。当设备收到服务器的 IPv6 报文时，NAT46 功能将 IPv6 报文转换为 IPv4 报文。这样确保了 IPv4 客户端能与 IPv6 服务器正常通信。

在整个系统中，DNS46 和 NAT46 功能只能启用在一个 DNS 类型的虚拟服务上。

dns_vs_name 该参数指定 DNS 类型的虚拟服务的名称。

priority_mode 可选，该参数指定资源优先模式，取值必须为：

- **A:** 优先将 DNS A 请求发往 DNS A 服务器，优先选择 DNS A 响应。
- **AAAA:** 优先将 DNS AAAA 请求发往 DNS AAAA 服务器，优先选择 DNS AAAA 响应。
- **Response:** 将 DNS A 请求发往 DNS A 服务器，DNS AAAA 请求发往 DNS AAAA 服务器，优先选择先收到的响应中的资源记录。

以上取值不区分大小写。默认值为“AAAA”。

ipv6 dnsnat46 off <dns_vs_name>

该命令用于为指定的 DNS 类型的虚拟服务同时禁用 DNS46 功能和 NAT46 功能。

ipv6 dnsnat46 ipmap <ipv4_address> <netmask> [timeout]

该命令用于设置 DNS46 和 NAT46 功能共享的 IPv4 映像子网。该子网中的 IP 地址用于建立 IPv6 地址和 IPv4 地址的映像。

当 IPv4 客户端发送 DNS A 解析请求到设备时，设备将先后发送 DNS A 解析请求和 DNS AAAA 解析请求到 DNS 服务器。如果 DNS 服务器只返回了 AAAA 记录，设备从该子网中选取一个可用的 IPv4 地址作为映像的 A 记录中的域名解析地址，然后把映像的 A 记录返回给 IPv4 客户端。同时，设备在映像表中添加一条映像记录来记录 IPv6 地址与 IPv4 地址的对应关系。设备在收到 IPv4 客户端发送的 IPv4 报文时，NAT46 功能将根据之前动态创建的 IP 映像记录，将报文中的目的地址转换回对应的 IPv6 地址。

ipv4_address	指定 IPv4 子网中的一个 IP 地址。
netmask	指定 IPv4 子网的屏蔽。该参数的取值应为点分地址格式，取值范围为 255.255.0.0~255.255.255.255。 参数“ipv4_address”和“netmask”共同确定一个 IPv4 子网。
timeout	可选，该参数指定 IPv6 地址到 IPv4 地址映像记录的超时时间，单位为秒。该参数的取值范围为 1~86400，默认值为 600。

no ipv6 dnsnat46 ipmap <ipv4_address> <netmask>

该命令用于删除 DNS46 和 NAT46 功能共享的 IPv4 映像子网。

show ipv6 dnsnat46 ipmap

该命令用于显示 DNS46 和 NAT46 功能共享的映像表中地址映像记录。

ipv6 dnsnat46 ippool <ipv6_pool_name>

该命令用于设置 NAT46 功能使用的全局 IPv6 地址池。当设备收到 IPv4 客户端发送的 IPv4 报文时，NAT46 功能将请求中的源地址转换为 IPv6 地址池中的地址。

ipv6_pool_name	指定 IPv6 地址池名称。

no ipv6 dnsnat46 ippool <ipv6_pool_name>

该命令用于删除 NAT46 功能使用的全局 IPv6 地址池。

ipv6 dnsnat46 timeout <idle_timeout>

该命令用于设置 NAT46 TCP 连接的空闲超时时间。

idle_timeout	指定 NAT46 TCP 连接的空闲超时时间，单位为秒。该参数的取值范围为 60~7200，默认值为 300。

show ipv6 dnsnat46 connection

该命令用于显示 NAT46 连接的地址转换信息。

show ipv6 dnsnat46 settings

该命令用于显示与 DNS46 和 NAT46 功能相关的设置。

clear ipv6 nat64 settings

该命令用于删除与 DNS46 和 NAT46 功能相关的设置，并恢复两个功能相关的默认设置。

show statistics ipv6 nat64

该命令用于显示与 DNS64、NAT64、DNS46 和 NAT46 功能相关的统计信息。

15.3 通用配置

ipv6 tune dnsnat priority time [priority_time]

该命令用于设置在 A 优先模式和 AAAA 优先模式下的优先计时器。该计时器表示在优先发送一个请求后，如果在计时器指定的时间内没收到响应，就发送缓存的请求。优先计时器对响应优先模式无效。

当不配置该命令时，默认的优先计时器为 100 毫秒。

priority_time	该参数指定优先计时器，单位为毫秒。取值必须为 1 至 5000 之间的整数，建议的取值范围为 100 至 500。
	默认值为 100。

ipv6 tune dnsnat response timeout [timeout]

该命令用于设置系统等待域名服务器返回响应时的超时时间。

在 A 和 AAAA 优先模式下，该超时时间是指发送完缓存的请求后等待响应时的超时时间。在响应优先模式下，该超时时间指同时向 DNS A 和 DNS AAAA 域名服务器发送完请求后等待响应时的超时时间。如果在超时后才收到响应，系统将丢弃该响应。

当不配置该命令时，响应计时器的默认值为 5000 毫秒。

timeout	该参数指定响应计时器，单位为毫秒。取值必须为 100 至 10,000 之间的整数。
	默认值为 5000。

show ipv6 tune dnsnat

该命令用于显示“**ipv6 tune dnsnat priority time**”和“**ipv6 tune dnsnat response timeout**”命令的配置。

clear ipv6 tune dnsnat

该命令用于将“**ipv6 tune dnsnat priority time**”和“**ipv6 tune dnsnat response timeout**”命令的配置恢复为默认值。

第16章 ePolicy

本章介绍 ePolicy 功能的相关配置命令。

epolicy import script <url> <script_name>

该命令用于导入事件处理脚本。

url 该参数指定 URL 地址。管理员从这个 URL 地址导入事件处理脚本。目前可支持 HTTP 和 FTP 两种 URL 地址。

注意: FTP 类型 URL (ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

script_name 该参数指定事件处理脚本的本地文件名。该脚本的文件扩展名必须为.tcl，取值必须为长度不大于 80 个字节的字符串。



注意：断电后，硬盘中的 TCL 脚本仍然保留。

no epolicy import script <script_name>

该命令用于删除硬盘中指定的事件处理脚本。

script_name 该参数指定事件处理脚本的名称。

show epolicy import

该命令用于显示硬盘中已所有已导入的事件处理脚本。

clear epolicy import

该命令用于清除硬盘中所有已导入的事件处理脚本。

epolicy attach script <virtual_service> <script_name>

该命令用于关联虚拟服务和事件处理脚本。一个虚拟服务可以关联最多 10 个事件处理脚本，而一个事件处理脚本可以与多个虚拟服务进行关联。

virtual_service 该参数指定虚拟服务的名称。取值必须为 HTTP、HTTPS、TCP、TCPS 或 UDP 类型的虚拟服务。

script_name 该参数指定事件处理脚本的名称。



注意：虚拟服务关联事件处理脚本后快速转发功能默认为禁用。

no epolicy attach script <virtual_service> <script_name>

该命令用于删除指定的虚拟服务和指定的事件处理脚本的关联关系。

virtual_service 该参数指定虚拟服务的名称。

script_name 该参数指定事件处理脚本的名称。

show epolicy attach [virtual_service]

该命令用于显示某个指定的或全部和虚拟服务关联的事件处理脚本。

virtual_service 可选参数，指定虚拟服务的名称。默认值为空，即显示全部虚拟服务和事件处理脚本的关联关系。

clear epolicy attach [virtual_service]

该命令用于清除某个指定的或全部虚拟服务和事件处理脚本的关联关系。

virtual_service 可选参数，指定虚拟服务的名称。默认值为空，即清除全部虚拟服务和事件处理脚本的关联关系。



注意：断电后，内存中未保留的配置将丢失。

show epolicy persistence session <session_table_name>

该命令用于显示为 ePolicy 模块创建的指定保持会话表。

session_table_name 该参数指定保持会话表的名称。取值必须为 ePolicy 脚本中指定的保持会话表名称。

epolicy class <class_name> <class_key_name> <class_key_value> [class_type]

该命令用于为 ePolicy 模块创建一个类，并为该类添加一个键值对，用于兼容 F5 Networks 公司的 Class iRules（使用 Class 相关命令的 iRules）。通过创建的类，管理员能够直接将 Class iRules 脚本导入设备。

系统支持最多配置 100 个类，每个类中最多可添加 100 个键值对。

class_name 该参数指定类的名称。取值必须为长度不大于 256 个字节的字符串。

class_key_name 该参数指定类中键的名称。取值必须为长度不大于 256 个字节的字符串或者 IP 地址或者数字。

class_key_value 该参数指定类中键对应的值。取值必须为长度不大于 256 个字节的字符串。

class_type 可选。该参数指定类的类型。取值必须为：

- “string”：表示字符串类型；
- “IP”：表示 IP 地址类型；
- “value”：表示值类型。

默认值为 “string”。

no epolicy class <class_name> <class_key_name>

该命令用于为 ePolicy 模块的类删除一个键值对。

show epolicy class [class_name] [class_key_name]

该命令用于显示 ePolicy 模块的指定类的指定键值对。

class_name 可选，该参数指定已创建的类的名称。取值必须为长度不大于 256 个字节的字符串。不指定该参数系统将显示所有类的键值对信息。

class_key_name 可选，该参数指定已创建的类中键的名称。取值必须为长度不大于 256 个字节的字符串或者 IP 地址或者数字。不指定该参数系统将显示所有键值对信息。

clear epolicy class [class_name]

该命令用于清除 ePolicy 模块的指定类的所有键值对。如果不指定参数 “class_name”，系统将清除所有类的所有键值对。

第17章 日志

本章介绍日志（Logging）功能的相关配置命令。

17.1 基本设置

log on

该命令用于启用系统日志功能。此功能默认是禁用的。

log off

该命令用于禁用系统日志功能。

log level <level>

该命令用于设置系统日志级别。设定系统日志级别后，低于这个级别的日志消息将被忽略，即不记录在系统中。如果不配置该命令，系统日志级别默认为 info。

level 该参数指定系统日志的级别。取值按级别从高到低依次为 emerg、alert、crit、err、warning、notice、info 或 debug。

例如，要让日志系统记录 debug 及以上级别的所有信息，则配置如下命令：

```
Demo(config)#log level debug
```



注意：

- NAT 日志的级别为 info。如果要系统记录 NAT 日志，系统日志级别需要设置为 info 或 debug。
- 本地日志级别（通过“**log localhost on**”命令设置）的优先级高于系统日志级别。

log facility <facility>

设置日志设备。支持的设备从 LOCAL0 到 LOCAL7，缺省设置为 LOCAL0。

```
Demo(config)#log facility LOCAL1
```

log language {chinese|english}

该命令用于设置系统日志的语言。配置“**log language chinese**”将设置日志语言为中文，配置“**log language english**”将设置日志语言为英文。默认情况下，系统日志的显示语言为英文。



注意：部分功能不支持中文日志，包括“**log nat custom**”、“**log http custom**”、“**log appvisual**”、“**log http {squid|common|combined|welf}**”、以及 epolicy、Diameter、WAF 等等。

log source port <source_port>

设置设备发送日志信息的源端口。源端口的取值范围为 0~65535，其中 0 意味着源端口将被随机指定。缺省端口为 syslog 端口 514。

```
Demo(config)#log source port 555
```

log timestamp {on|off}

该命令用于控制是否在日志中添加时间戳。

log option logid {on|off}

该命令用于控制是否将日志 ID 添加到日志消息中。默认情况下，该功能是禁用的。

log option levelinfo {on|off}

该命令用于控制是否将级别信息添加到即将发送到日志主机的日志中。默认情况下，该功能是禁用的。

log option sourceip {on|off}

该命令用于控制是否将源 IP 地址添加到操作日志消息中。默认情况下，该功能是禁用的。

show log buff {forward|backward} [match_str]

显示缓存中最新的 2000 条日志信息，可以以正序或者逆序显示。需要注意的是 CLI 日志级别为 Debug。

match_str 可选参数。仅显示与某个关键词串相匹配的日志信息。

例如：

```
Demo(config)#show log buff backward
```

clear log buff

清除日志缓存。

log test

该命令用于生成一条“emerg”级别的测试日志消息。

show log cli [line_number] [filter_string]

该命令用于显示命令相关的日志信息。

line_number 可选。该参数指定显示命令日志的行数。其取值范围为 0 到 5000 之间的整数。

默认值为 200。表示系统将显示最新产生的 200 行命令

日志信息。

filter_string 可选。该参数指定用于搜索命令日志的过滤字符串，取值必须为长度不大于 200 个字节的字符串，置于双引号中。

show log restapi cli [line_number] [filter_string]

该命令用于显示 RESTful API 命令相关的日志信息。

line_number 可选。该参数指定显示命令日志的行数。取值必须为 0 到 5000 之间的整数。

默认值为 200，表示系统将显示最新产生的 200 行命令日志信息。

filter_string 可选。该参数指定用于搜索命令日志的过滤字符串，取值必须为长度不大于 200 个字节的字符串，置于双引号中。默认值为空，表示系统将显示所有 RESTful API 命令相关的日志信息。

17.2 RFC 5424 Syslog

log rfc5424 on

该命令用于启用 RFC 5424 syslog 功能。启用该功能后，系统将会生成符合 RFC 5424 标准格式的系统日志。RFC 5424 标准日志格式为**<PRI>VER TIMESTAMP HOSTNAME APPNAME PROCID MSGID STRUCTURED-DATA MSG-CONTENT**。（暂不支持 PROCID 和 STRUCTURED-DATA 字段，这两个字段默认显示为“-”。）例如：**<134>1 2015-06-12T15:50:13Z AN - - 100013004 - CLI: User "admin" executed cmd "log rfc5424 on"**就是采用 RFC 5424 标准格式生成的系统日志。

默认情况下，系统禁用 RFC 5424 syslog 功能。



注意：只有执行“log on”命令启用系统日志功能后，“log rfc5424 on”命令配置才能生效。

log rfc5424 off

该命令用于禁用 RFC 5424 syslog 功能。

log rfc5424 appname <app_name>

该命令用于指定 RFC 5424 标准格式日志头部中 APPNAME 字段的值。如果不指定 APPNAME 字段的值，那么 APPNAME 字段在系统日志中将显示为“-”。

app_name 指定生成系统日志的设备或应用的名称。该参数的取值为不多于 48 位的字符串。

no log rfc5424 appname

该命令用于删除对 RFC 5424 标准格式日志头部中 APPNAME 字段的设置。

log rfc5424 msgid <system_log_id> <custom_log_id>

该命令用于设定指定 RFC 5424 标准格式日志头部中 MSGID 字段的值。如果没有为指定的系统日志设置 MSGID 字段的值，那么将使用该系统日志的内部 ID。

system_log_id 指定一条系统日志的内部 ID。

custom_log_id 指定该 RFC 5424 标准格式日志头部中 MSGID 字段的值。该参数的取值为不多于 32 位的字符串。

no log rfc5424 msgid <system_log_id>

该命令用于删除指定 RFC 5424 标准格式日志头部中 MSGID 字段的设置。MSGID 字段将使用系统日志的内部 ID。该设置只对后续生成的该 RFC 5424 标准格式日志生效。

system_log_id 指定一条系统日志的内部 ID。

clear log rfc5424 msgid

该命令用于清除所有 RFC 5424 标准格式日志头部中 MSGID 字段的设置。MSGID 字段将使用系统日志的内部 ID。该设置只对后续生成的该 RFC 5424 标准格式日志生效。

17.3 日志定制

log http {squid|common|combined|welf} [vip|novip] [host|nohost]

该命令用于启用 HTTP 访问日志功能，并设置记录 HTTP 访问信息的日志格式。

该功能的默认设置为启用，HTTP 访问信息的日志格式默认为 squid。

squid|common
|combined|welf 该参数指定 HTTP 访问信息设置日志格式。日志格式可以为：squid、welf、common 或者 combined。系统默认为 squid。管理员可以使用“**log http custom**”命令自定义自己的日志格式。

vip|novip 该参数指定是否记录接收请求的虚拟服务 IP 地址，取值必须为：

- **vip**：记录接收请求的虚拟服务 IP 地址。

- novip: 不记录接收请求的虚拟服务 IP 地址。

默认值为“novip”。

host|nohost

该参数指定是否记录请求的目的主机的名称，取值必须为：

- host: 记录请求的目的主机的名称。
- nohost: 不记录请求的目的主机的名称。

默认值为“nohost”。



注意：如果需要记录 ID 为 100002221 的 HTTP 访问日志，日志格式必须设置为 welf。

下面例子中，日志消息的格式被设置为 squid，且不记录虚拟服务 IP 和目的主机信息：

```
Demo(config)#log http squid novip nohost
```

log http custom <format>

该命令用于配置 HTTP 自定义访问日志的格式。

format

该参数指定记录 HTTP 访问信息的日志格式。取值必须置于双引号内。

管理员可以使用下表列出的符号来组成自定义的日志格式。如果输入的“format”字符串中包含以下符号以外的其他字符，这些字符将按原样被复制到日志信息中。管理员也可以根据情况，在“format”字符串中输入其他字符。

表17 - 1 HTTP 日志格式支持的符号

符号	含义
%a	缓存结果
%b	从代理返回到客户端的字节数
%c	客户端 IP 地址
%d	日期戳[MM/DD/YYYY]
%e	HTTP MIME 类型信息
%f	“PROXY_LOG” 标记，用来同其它类型的日志信息作区分的标记
%g	时间戳[HH:MM:SS]
%h	从请求的 Host 头域获取到的主机名
%i	用户代理

符号	含义
%l	请求头
%m	HTTP 方法
%n	完整日期/时间戳[MM/DD/YYYY:HH:MM:SS +/-0000]
%k	会话 cookie
%o	虚拟服务端口
%p	虚拟服务 IP 地址
%q	一个单个双引号
%r	HTTP 返回状态码
%s	后台服务器 IP 地址
%t	Unix 时间戳
%u	请求的 URI 注意：系统支持显示最多 800 个字符的 URI；长度超过 800 字符的 URI 显示为“-”。
%v	协议版本
%w	从请求的 Referer 头域获取到的引用页
%x	响应头
%y	请求 body
%z	响应 body
%A	返回响应给客户端时的时间戳
%E	显示错误日志的信息，包括“error_code”和“error_string”信息。“error_code”是对错误的简短描述，“error_string”记录错误发生的位置。
%F	设备用来连接后台服务器的 IP 地址
%U	请求的完整 URL 注意：系统支持显示最多 800 个字符的路径（Path）；长度超过 800 字符的路径显示为“-”。
%R	接收请求和返回响应之间的间隔
%T	时间格式与 W3C（GMT）兼容
%O	设备用来连接后台服务器的端口
%N	完整日期/时间戳[DD/MMM/YYYY:HH:MM:SS +/-0000]
%D	SSL 会话 ID
%P	后台服务器端口
%H	客户端源端口号
%B	转发请求到后台服务的时间
%S	从转发请求给后台服务到收到响应所用的时间
%C	客户端连接 RTT 平均值
%I	处理请求所用时间的平均值
%G	处理响应所用时间的平均值
%J	后台服务组名称
%K	HTTP 连接的类型，长连接或短连接

符号	含义
%L	设备的主机名称
%M	IP 地址池的名称
%Q	系统处理一个请求所用的时间
%V	收到客户端请求时的时间戳
%W	系统处理一个响应所用的时间
%X	拓展头部 X-Forwarded-For
%Y	收到服务端响应时的时间戳
%Z	虚拟服务的名称

管理员在使用 HTTP 访问日志功能前需要指定日志格式，通过执行下面的命令，将日志格式设置为“%c%d%g%k”，使得日志系统记录客户端 IP 地址、日期戳、时间戳以及会话 cookie 等。

```
Demo(config)#log http custom "%c %d %g %k"
```



注意：

1. 该命令对 HTTP/2 协议不生效。
2. 如果配置了 HTTP 改写功能，日志记录的 HTTP 头部和 HTTP 主体均为改写前的内容。
3. 管理员通过命令“show log buff”查看日志信息时，日志格式“%l”、“%x”“%y”、“%z”对应的内容系统均显示为“*”。

no log http

该命令用于禁用 HTTP 访问日志功能。

log http response timeout <timeout> [resp_content]

该命令用于配置 HTTP 自定义访问日志的超时时间以及超时时的响应内容。

timeout 该参数指定 HTTP 自定义访问日志的超时时间，单位为秒。取值必须为 1 至 300 之间的整数。

resp_content 可选，该参数指定 HTTP 自定义访问日志超时时的响应内容。取值必须为长度不超过 511 个字节的字符串。

默认值为“Response Timeout”。



注意：

1. 在分区模式下不支持该命令。
2. 不配置“log http response timeout”命令，则在 HTTP 自定义访问日志中 HTTP 响应永不超时。

log custom maxlen [length]

该命令用于配置 TCP 和 HTTP 自定义访问日志的最大长度，超过最大长度的日志内容会被截断。

length 可选，该参数指定 TCP 和 HTTP 自定义访问日志的最大长度，单位为 KB。取值必须为 1 至 3072 之间的整数。

默认值为 64。



注意：

- 在分区模式下不支持该命令。
- 向 UDP 类型的远程日志主机发送日志消息时，一条日志的长度最大允许为 64KB，超过最大长度的日志内容会被截断。

no log custom maxlen

该命令用于重置 HTTP 自定义访问日志的最大长度。

log tcp custom <format>

该命令用于自定义 TCP 访问日志的日志格式。

format 该参数指定 TCP 访问 日志的日志格式。取值必须置于双引号内。

管理员可以使用下表列出的符号来组成自定义的日志内容。如果参数取值包含下表列出的符号以外的其他字符，这些字符将按原样被复制到日志信息中。

表17 - 2 支持自定义的日志内容

符号	含义
%a	收到请求的时间
%b	发送请求的时间（等于收到请求的时间）
%c	处理请求的时间（固定 1ms）
%d	收到响应的时间
%e	发送响应的时间
%f	处理响应的时间（固定 1ms）
%g	请求数据
%h	响应数据
%i	客户端 IP 地址
%j	客户端源端口
%k	虚拟服务 IP 地址
%l	虚拟服务端口
%m	设备用来连接后台服务器的 IP 地址
%n	设备用来连接后台服务器的端口

符号	含义
%o	后台服务器 IP 地址
%p	后台服务器端口

no log tcp custom

该命令用于删除所有已定义的 TCP 访问日志的日志格式。

log tcp response timeout <log_timeout> [log_content]

该命令用于设置 TCP 访问日志的超时时间和 TCP 访问超时后的响应数据(%h)，即在指定的超时时间内未收到后台服务器返回的响应时，系统根据自定义内容记录响应数据。

log_timeout 该参数指定 TCP 访问日志的超时时间，单位为秒，取值必须为 1 至 300 之间的整数。

log_content 可选，该参数指定 TCP 访问超时后的响应日志内容。取值必须为长度不超过 511 个字符的字符串。

默认值为“Response Timeout”。

no log tcp response timeout

该命令用于清除已配置的 TCP 访问日志的超时时间和 TCP 访问超时后的响应日志。

log nat custom <format_string>

该命令用于使系统生成 SLB 地址转换日志。在 SLB 反向代理模式中，当收到客户端的请求时，设备分别将请求的源地址和目的地址转换为 VIP 和后台服务的 IP 地址。当客户端和设备之间以及设备与后台服务之间成功建立连接时，系统将生成一条 SLB 地址转换日志。需要注意的是，只有通过命令“**ipv6 dns64 on**”为指定的 DNS 类型的虚拟服务启用 DNS64 功能，并通过命令“**ipv6 nat64 on**”启用 NAT64 功能后，该功能才能生效。默认情况下，系统不生成 SLB 地址转换日志。

format_string 指定系统生成的 SLB 地址转换日志的内容格式。该参数的取值为不多于 64 位的字符串，设置的字符串必须置于双引号内。

除了下述字符外，所有字符在日志中都按照原样式显示：

- %t: 显示四层协议类型。
- %s: 显示转换前的源 IP 地址。

- %p: 显示转换前的源端口。
- %d: 显示转换前的目的 IP 地址。
- %o: 显示转换前的目的端口。
- %S: 显示转换后的源 IP 地址。
- %P: 显示转换后的源端口。
- %D: 显示转换后的目的 IP 地址。
- %O: 显示转换后的目的端口。
- %a: 显示“SETUP”，表明客户端 IP 地址与 VIP 之间以及 VIP 与后台服务之间的连接已经建立。
- %: 显示“%”。

例如：

```
Demo(config)#log nat custom "%t %s %p %d %o %S %P %D %O %a"
```

no log nat custom

该命令用于禁止系统生成的 SLB 地址转换日志。

17.4 本地和远程日志主机

log localhost on [log_level]

该命令用于在系统中启用本地日志主机并设置本地日志的级别。启用本地日志主机并设定本地日志级别后，低于该级别的日志消息将被忽略，即不记录在系统中。本地日志主机默认设置为禁用。

当启用本地日志主机后，本地日志主机开始在 IP 地址 127.0.0.1 和 UDP 端口 515 上接收系统发送的系统日志。本地日志主机可以为每个日志级别存储最多 500,000 条系统日志。在本地日志主机上存储的系统日志可以通过 WebUI 查看和导出。

本地日志级别的优先级高于系统日志级别（通过“**log level**”命令设置）。设置本地日志级别时，需要使其等于或大于系统日志级别。

该命令还支持修改已设置的本地日志级别。

log_level 可选，该参数指定日志级别。取值按级别从高到低依次为 emerg、alert、crit、err、warning、notice、info 或 debug。

默认值为 info。

log localhost off

该命令用于在系统中禁用本地日志主机。

log storage {on|off}

该命令用于在系统中启用或者禁用本地日志保存功能。启用该功能后，系统将在本地硬盘上保存最近 6 个月内的系统日志。如果管理员需要获取最近 6 个月保存的本地日志，管理员还需要通过命令“**debug log storage**”启用生成本地日志压缩文件的功能。该功能默认设置为禁用。

log host <host_ip> [port] [protocol] [host_id] [delimiter]

该命令用于配置接收日志消息的远程日志主机。

host_ip 该参数指定日志主机的 IP 地址。取值必须是 IPv4 或 IPv6 地址。

注意：对于 IPv4 地址，系统支持点分十进制格式；对于 IPv6 地址，系统支持首选格式（例如：2000:0000:0000:0000:0001:2345:6789:ABCD）和压缩表示（例如：2001:DB8::8:800:200C:417A），不支持内嵌 IPv4 地址的 IPv6 地址表示（例如：::FFFF:192.168.0.1）。

port 可选，该参数指定日志主机的服务端口。取值必须为 0 至 65535 之间的整数。

默认值为 514。

protocol 可选，该参数指定发送日志消息使用的协议。取值必须为“udp”或“tcp”。

默认值为“udp”。

host_id 可选，该参数指定日志主机的 ID。取值必须为 1 至 15 之间的整数。

默认值为 1。

delimiter 可选，该参数指定日志信息分界符，仅在参数“protocol”设置为“tcp”时才可用。取值必须为：

- 0：表示使用 NUL 作为分界符。
- 1：表示使用 LF 作为分界符。
- 2：表示使用 CR 作为分界符。
- 3：表示使用 CR 和 LF 作为分界符。

默认值为 0。



注意:

- 远程日志主机的配置不能为“**log host 127.0.0.1 515 udp**”，系统将该配置预留为本地日志主机使用。
- 确认远程日志主机可以正确接收日志信息。可以通过服务器系统上的 Syslogd 来配置日志主机。

no log host <host_ip> <port> [protocol]

该命令用于删除远程日志主机。

host_ip	该参数指定日志主机的 IP 地址。
port	该参数指定日志主机的服务端口。
protocol	可选，该参数指定发送日志消息使用的协议。 默认值为“udp”。

clear log host

该命令用于清除所有的日志主机。

log attach <virtual_service|vlink_name> <host_id>

该命令用于将指定的虚拟服务或虚连接与指定的日志主机绑定。绑定后，日志主机只会收到该虚拟服务或虚连接相关的系统日志。

在不配置日志过滤器的情况下，不绑定任何虚拟服务或虚连接的日志主机，将收到所有系统日志。如果配置了日志过滤器，将只收到过滤后的日志。

每个日志主机支持绑定最多 128 个虚拟服务。

virtual_service|vlink_name 该参数指定已存在的虚拟服务或虚连接的名称。

host_id 该参数指定已存在的日志主机的 ID。

no log attach <virtual_service|vlink_name> <host_id>

该命令用于解除指定的虚拟服务或虚连接与指定的日志主机的绑定关系。

clear log attach <host_id>

该命令用于解除所有虚拟服务和虚连接与指定的日志主机的绑定关系。

host_id 该参数指定已存在的日志主机的 ID。取值为 0 时表示解除所有虚拟服务和虚连接与所有日志主机的绑定关系。

log filter <host_id> <filter_id> <filter_string> [module_name] [method]

该命令用于为指定日志主机创建日志过滤器。系统支持为同一日志主机配置最多 20 个日志过滤器，不同过滤器之间的逻辑关系为“OR”。

host_id	该参数指定日志主机的 ID。该 ID 必须已经由“ log host <host_ip> [port] [udp tcp] [host_id]”命令配置。
filter_id	该参数指定日志过滤器的 ID。取值必须为 1 到 20 之间的整数。
filter_string	该参数指定日志过滤字符串。取值必须为长度不大于 40 个字节的字符串，不区分大小写。该参数为“*”时，将匹配所有日志。
module_name	可选，该参数指定用于日志过滤的模块名称，与“filter_string”参数指定的日志过滤字符串一起用于日志过滤。取值必须为以下模块名称： • Fastlog • WebWall • uProxy • Cache • Proxy • HTTP Access Log • Filter • LLB • Conn API • Feature Control • Clustering • Health Check • SNMP • Debug • XMLRPC • Sysmon • CLI • WebUI

- SLB
- Compression
- Port Forwarding
- SSL
- LDAP
- IP Redundancy
- SDNS
- ClickTCP
- Hardware
- Diskfree
- Authentication
- Snmpinfod
- SIP
- RTSP
- Triangle
- Dynamic Route
- Radius
- Ulandmon
- IPv6
- IPregion
- PPTP
- ePolicy
- HA
- all

参数取值可以包含多个模块，中间用分号隔开。例如“SSL:SLB:LLB”。默认值为“all”，表示所有的模块。

method

可选，该参数指定日志的发送方法。

- 0: 表示将匹配配置的过滤字符串但不属于指定的模块的日志发送到日志主机。

- 1: 表示将匹配配置的过滤字符串并且属于指定的模块的日志发送到日志主机。

默认值为 1。



注意：中文日志过滤器只能通过 WebUI 配置。

no log filter <host_id> [filter_id]

该命令用于删除为指定日志主机配置的某条或者所有日志过滤器。

host_id 该参数指定日志主机的 ID。该 ID 必须已经由“**log host <host_ip> [port] [udp|tcp] [host_id]**”命令配置。

filter_id 可选，该参数指定要删除的日志过滤器的 ID，取值必须为 0 到 20 之间的整数。当取值为 0 时，表示删除指定日志主机的所有日志过滤器。

默认值为 0。

17.5 单个系统日志禁用

log message disable <log_id>

该命令用于禁用指定的系统日志。禁用的系统日志将会添加到禁用系统日志列表中。设备最多允许禁用 32 个系统日志。

该命令的默认配置如下：

log message disable 100017001

log message disable 100017002

log message disable 100017003

log message disable 100017004

log message disable 100017005

log message disable 100017006

log message disable 100024013

log message disable 100024014

log_id 该参数指定系统日志的 ID。

管理员可以在 WebUI 的工具栏上点击图标，然后从下拉列表中选择**日志列表文档**来查看所有系统日志的 ID。

show log message disable [log_id]

该命令用于显示禁用系统日志列表中指定的系统日志。如果不指定参数“log_id”，系统将会显示禁用系统日志列表中的所有系统日志。

no log message disable <log_id>

该命令用于从禁用系统日志列表中删除指定的系统日志，即启用该系统日志。

clear log message disable

该命令用于从禁用系统日志列表中删除所有的系统日志，即启用所有系统日志。

17.6 日志报警

log alert <id> <expression> <email> <interval> [data|count]

该命令用于配置设备发送日志报警消息的规则。

当日志的内容匹配参数“expression”的设置时，设备将根据指定的日志 ID、发送时间间隔和消息类型，向指定的邮件地址发送日志报警消息。

id	指定日志报警消息的 ID，取值范围为 1 到 32。
expression	指定用于匹配日志内容的字符串。该字符串支持简单的正则表达式。如果使用正则表达式，则需要将其置于双引号内。该参数支援的通配符及含义如下： ^：匹配字符串的起始位置。 \$：匹配字符串的结束位置。 *
email	指定接收日志报警消息的电子邮件地址。该邮件地址应置于双引号内。
interval	指定设备发送日志报警消息的时间间隔，取值范围为 0 到 10000，单位为分钟。其中 0 表示立即发送。 如果有连续匹配的日志消息，可以通过设置报警邮件的发送间隔来降低发送频率。
data count	指定日志报警消息的类型。data 表示发送匹配的整条日志内容，count 表示发送匹配的日志内容的数量统计信息。预设情况下，采用 data 类型。

例如：

```
Demo(config)#log alert 1 "sdns" "xyz@mailserver.com" 1 "data"
```

以上命令配置表示，如果日志内容中包含“sdns”字符串，设备将每隔 1 分钟把 ID 为 1 的日志报警消息发送到邮件地址 xyz@mailserver.com。邮件信息示例如下：

```
From: AN<alert@log.domain>
To: Alert Log System Operator(s)<xyz@mailserver.com>
Subject: Log Alert ID: 1 - sdns
MIME-Version: 1.0
<134>Apr 25 21:05:01 CLI: cmd "log alert 2 "sdns" "xyz@mailserver.com"
0 "data""
<134>Apr 25 21:05:11 CLI: cmd "sdns on"
<134>Apr 25 21:05:12 CLI: cmd "sdns off"
```

管理员可以通过命令“**show log config**”查看配置好的规则。

为了正确解析邮件地址，需要在设备上用“**ip nameserver**”命令配置 DNS 服务器地址。

no log alert <id>

该命令用于删除一条指定的日志报警规则。

show log alert

该命令用于显示所有的日志报警规则配置。

clear log alert

该命令用于清除所有报警规则配置。

show log config

该命令用于显示当前日志配置。

clear log config

该命令用于恢复日志设置为缺省配置。

log sms user <index> <phone_num> <log_level>

该命令用于配置设备发送日志短信告警功能。

index	必选。该参数用于配置短信告警索引号，最大支持 10 条。取值为 1~10。
phone_num	必选。该参数用于指定短信告警电话号码，仅支持中国大陆手机号。
log_level	必选。该参数用于指定短信告警日志级别，大于该日志级别的日志将会发送短信告警至指定电话号码。取值按级别从高到低依次为 emerg、alert、crit、err、warning、

notice、info 和 debug。

no log sms user <index_id>

该命令用于删除一条指定的日志短信告警配置。

show log sms user

该命令用于显示所有的日志短信告警配置。

clear log sms user

该命令用于清除所有的日志短信告警配置。

log sms server tencent <appid> <secret_id> <secret_key> <template_id>

该命令用于配置腾讯云短信网关。

appid	必选。该参数用于配置短信平台应用 ID，用于 API 请求认证。取值必须为长度不大于 64 字节的字符串。
secret_id	必选。该参数用于配置短信平台访问身份 ID。取值必须为长度不大于 64 字节的字符串。
secret_key	必选。该参数用于配置短信平台密钥。取值必须为长度不大于 64 字节的字符串。
template_id	必选。该参数用于配置短信平台模板 ID。取值必须为长度不大于 32 字节的字符串。

no log sms server <index_id>

该命令用于删除一条指定的短信平台服务配置。

show log sms server

该命令用于显示所有的短信平台服务配置。

clear log sms server

该命令用于清除所有的短信平台服务配置。

log url <index> <url> [log_level]

该命令用于配置设备日志告警 URL 回调功能。

index	必选。该参数用于配置索引号，最大支持 15 条。取值为 1 到 15。

url	必选。该参数用于配置回调 URL。
log_level	可选。该参数用于指定短信告警日志级别，大于该日志级别的日志将会推送告警日志至指定 http 服务器。取值按级别从高到低依次为 emerg、alert、crit、err、warning、notice、info 和 debug。默认为 alert。

no log url <index_id>

该命令用于删除一条指定的日志告警 URL 回调功能配置。

show log url

该命令用于显示所有的日志告警 URL 回调功能配置。

clear log url

该命令用于清除所有的日志告警 URL 回调功能配置。

17.7 日志关联 SNMP trap

log snmp trap <log_id> <trap_oid>

该命令用于为指定的系统日志设置 SNMP trap OID。

系统日志和 SNMP trap OID 关联后，只要系统生成该日志，就会触发一条 SNMP trap 消息。

log_id 该参数指定日志消息 ID。

trap_oid 该参数指定 SNMP trap OID，取值必须为 2 至 65,535 之间的整数。

no log snmp trap <log_id>

该命令用于删除对指定系统日志的 SNMP trap OID 设置。

show log snmp trap [log_id]

该命令用于显示对指定系统日志的 SNMP trap OID 设置。如不指定“log_id”参数，则显示对所有系统日志的 SNMP trap OID 设置。

clear log snmp trap [log_id]

该命令用于删除对指定系统日志的 SNMP trap OID 设置。如不指定“log_id”参数，则清空对所有系统日志的 SNMP trap OID 设置。

17.8 应用可视化

log appvisual {on|off} [/log_module]

该命令用于为指定的应用模块启用或禁用可视化日志功能。

启用可视化日志功能后，系统将收集 ELK 服务器需要使用的该模块的日志信息。

该功能默认设置为对所有应用模块禁用。

- log_module** 可选，该参数指定应用模块的名称，取值必须为：
- **ssl**: 表示为 SSL 应用模块启用或禁用可视化日志功能。
 - **sdns**: 表示为 SDNS 应用模块启用或禁用可视化日志功能。
 - **slb-http**: 表示为 SLB HTTP 应用模块启用或禁用可视化日志功能。
 - **slb-tcp**: 表示为 SLB TCP 应用模块启用或禁用可视化日志功能。需要注意的是，为 SLB TCP 应用模块启用可视化日志功能后，如果配置 TCP 类型的健康检查，系统会每秒打印日志，可能造成日志数据激增。
 - **slb-ftp**: 表示为 SLB-FTP 应用模块启用或禁用可视化日志功能。
 - **slb-rtsp**: 表示为 SLB-RTSP 应用模块启用或禁用可视化日志功能。
 - **slb-sip**: 表示为 SLB-SIP 应用模块启用或禁用可视化日志功能。
 - **llb**: 表示为 LLB 应用模块启用或禁用可视化日志功能。
 - **all**: 表示为所有应用模块启用或禁用可视化日志功能。

默认值为 “all”。

show log appvisual [/log_module]

该命令用于显示指定应用模块是否开启了应用可视化日志功能。如不指定参数 “log_module”，将显示可视化日志功能对所有应用模块的启用状态。

17.9 系统日志去重和限速

log rate limit [*max_limit*]

该命令用于配置系统日志限速速率。

当每秒产生的相同日志 ID 的日志数量达到设置的日志数量上限时，系统将不会再生成该系统日志 ID 的日志。该功能仅针对 Notice 及以上级别的系统日志生效。该功能默认是禁用的。

max_limit 可选，该参数指定每秒产生的相同日志 ID 的日志的数量上限。取值必须为 0 至 100 之间的整数。其中 0 表示禁用日志限速功能。默认值为 5。

no log rate limit

该命令用于删除系统日志限速速率的配置。

log uniq list <*log_id*>

该命令用于配置系统日志去重列表。执行该命令后，指定日志 ID 的系统日志将会被添加到系统日志去重列表中。该功能仅针对 Notice 及以上级别的系统日志生效。系统日志去重列表的默认配置如下：

```
log uniq list 100007011
```

```
log uniq list 100007012
```

log_id 该参数指定系统日志的 ID。

管理员可以在 WebUI 的工具栏上点击图标，然后从下拉列表中选择**日志列表文档**来查看所有系统日志的 ID。

no log uniq list <*log_id*>

该命令用于从系统日志去重列表中删除指定的系统日志，即禁用该系统日志的去重功能。

clear log uniq list

该命令用于从系统日志去重列表中清除所有的系统日志，即禁用所有系统日志的去重功能。

log uniq interval [*interval*]

该命令用于配置内容相同的日志的去重时间间隔。

当日志 ID 和日志内容相同时，在指定的时间间隔内，系统将不再生成该日志。该功能默认是禁用的。

interval 可选，该参数指定系统日志的去重时间间隔。取值必须为 0 至 300 之间的整数，单位为秒。其中 0 表示禁用日志去重功能。默认值为 5 秒。

no log uniq interval

该命令用于删除日志去重间隔的配置，即禁用日志去重功能。

第18章 管理工具

本章介绍管理工具的相关配置命令。

18.1 配置管理命令

admin aaa {on|off} [priority]

该命令用于启用或禁用外部认证功能。该功能允许通过 RADIUS 或 TACACS+ 服务器对管理员帐号进行登录认证。该功能的默认设置为禁用。

priority 可选，该参数指定当启用外部认证功能时，本地数据库和外部认证服务器的使用优先级。取值必须为：

- 0：表示优先使用本地数据库。只有当用户名在本地数据库中不存在时，才使用外部认证服务器。
- 1：表示优先使用外部服务器。如果因为用户名不存在、密码输入错误和外部认证服务器不可达等原因导致认证失败，将使用本地数据库。如果使用的是 RADIUS 类型的外部服务器，系统支持在 RADIUS 认证报文中设置 Vendor_ID。

默认值为 0。

admin aaa authorize {on|off}

该命令用于启用或禁用外部授权功能。该功能允许通过 RADIUS 或 TACACS+ 服务器对管理员帐号进行不同级别的授权。该功能的默认设置为禁用。禁用状态下，只要认证成功，该帐号就可以访问 Config 级别。

在 TACACS+ 授权方式下，只有“priv-lvl”字段值为 15 的管理员帐号能够访问 Config 级别，其他的管理员帐号只能访问 Enable 级别。

在 RADIUS 授权方式下，

- 授权报文中“Service-Type”属性值为“Administrative”的管理员帐号能够访问 Config 级别。

- 对于授权报文中“Service-Type”属性值不为“Administrative”的管理员账号，如果 Vendor-Specific 属性包含 Vendor-Type 为 29 的子属性时：
 - 子属性的 Vendor-Data 值在 0 到 9 之间时，管理员账号只能访问 Enable 级别。
 - 子属性的 Vendor-Data 值在 10 到 15 之间，管理员账号能够访问 Config 级别。
- 对于授权报文中“Service-Type”属性值不为“Administrative”，Vendor-Specific 属性不包含 Vendor-Type 为 29 的子属性时，
 - 当禁用了外部授权功能时，管理员账号能够访问 Config 级别。
 - 当启用了外部授权功能时，管理员账号只能访问 Enable 级别。

admin aaa method [method]

该命令用于配置外部认证和授权方式。管理员可以部署 RADIUS 或者 TACACS+ 服务器进行外部认证和授权。默认方式为 RADIUS。

method 该参数指定外部认证和授权方式，取值必须为：

- **radius**: 表示使用 RADIUS 服务器进行外部认证和授权。
- **tac_x**: 表示使用 TACACS+服务器进行外部认证和授权。

默认值为“radius”。

admin aaa server <server_id> {host_name|ip_address} <port> [secret]

该命令用于配置外部认证和授权服务器。系统支持部署两个 ID 分别为“es01”和“es02”的认证和授权服务器。如果在服务器 es01 上认证或授权失败，系统将尝试在服务器 es02 上认证或授权。

server_id 该参数指定认证和授权服务器的 ID 的值，取值必须为“es01”或“es02”。

host_name|ip_address 该参数指定认证和授权服务器的主机名称或 IP 地址。若指定为 IP 地址，必须置于双引号内。支持 IPv4 或 IPv6 地址。

port 该参数指定认证和授权服务器的端口号，取值必须为 0 至 65,535 之间的整数。

secret 可选。该参数指定认证和授权服务器的密钥。取值包含特殊字符或由纯数字组成时，必须置于双引号内。不配置该参数时，密钥为空。

注意：在“**show admin aaa all**”命令输出和日志中，密钥将显示为“*****”形式。在运行配置、启动配置和配置备份文件中，密钥将显示为加密形式，并通过“**ENCRYPTED**”标志进行标识。

例如，配置两个 ID 分别为 es01 和 es02 的认证和授权服务器：

```
Demo(config)#admin aaa server es01 "10.1.31.1" 1812 radiusceret
Demo(config)#admin aaa server es02 radius_host 1812 radiusceret
```

no admin aaa server <server_id>

该命令用于删除指定外部认证和授权服务器的相关配置。

clear admin aaa all

该命令用于清除所有外部认证和授权服务器的相关配置。

show admin aaa all

该命令用于显示外部授权和认证功能的开启状态以及所有的外部认证和授权服务器相关配置。

passwd enable [passwd_string]

该命令用于设置或修改进入 Enable 模式的密码。

passwd_string 可选参数。指定进入 Enable 模式的密码。该参数取值为长度不大于 8 个字节的字符串，区分大小写，必须置于双引号内。支持数字、字母和特殊符号。如果不设置该参数，在命令行提示输入密码时按回车键即可进入 Enable 模式。

user <user_name> <password> [level]

该命令用于创建新的管理员用户，并设置账号密码和权限等级。

对于已存在的管理员账号，如果需要修改权限等级，需删除账号后重新创建。

系统支持创建最多 100 个管理员用户。

user_name 该参数指定管理员用户的用户名。取值必须为不大于 32 字节的字符串，支持字母和数字，不支持特殊字符，但是允许“\$”出现在参数值的结尾。

password 该参数指定密码。

在强制密码模式关闭时，取值必须为 1 至 116 个字节的字符串，区分大小写。当参数取值包含数字或特殊字符（除了大小写字母、数字以外的其他所有可见字符）时，

必须置于双引号内。

在强制密码模式开启时，取值必须满足强制密码模式的密码复杂度要求（参考“**passwd forcemode**”命令）。

level

可选。该参数指定管理员用户的权限级别。取值必须为：

- **enable**: 拥有该权限级别的管理员用户只能运行“enable”级别下的 CLI 命令。
- **config**: 拥有该权限级别的管理员用户可以运行全部 CLI 配置命令，对设备的各项功能进行配置和管理。
- **api**: 拥有该权限级别的管理员用户可以访问基于 API 的 Web 服务，但是不能运行任何 CLI 命令。

默认值为“config”。



注意：

- 设备最多支持 100 个管理员用户。通常情况下，API 用于集中控制设备，因此虽然系统支持创建多个拥有“api”权限级别的用户，但建议只创建一个拥有“api”权限级别的用户。
- 不能为权限级别为“api”的管理员用户配置基于角色的权限管理功能。

no user <user_name>

该命令用于删除指定的管理员用户。

如果启用了三权分立功能，当系统中只存在一个关联管理员角色（role_administrator）的管理员用户，则不允许删除该管理员用户。

show users

该命令用于显示已创建的管理员用户的配置。

clear users

该命令将清除所有的管理员用户。执行该命令后，系统会重新创建初始登录用户（admin）。

如果启用了三权分立功能，该命令将重新创建三权分立用户 Administrator。

passwd user <user_name> <password>

该命令用于修改已有管理员账户的密码。

user_name 该参数指定已存在的管理员账户的用户名。

password 该参数指定新密码。

在强制密码模式关闭时，取值必须为 1 至 116 个字节的

字符串，区分大小写。当参数取值包含数字或特殊字符（除了大小写字母、数字以外的其他所有可见字符）时，必须置于双引号内。

在强制密码模式开启时，取值必须同时满足强制密码模式的密码复杂度要求（参考“**passwd forcemode**”命令）。

passwd forcemode {on|off}

该命令用于启用或禁用强制密码修改模式。该功能默认设置为启用。启用强制密码修改模式后，系统对新创建的管理员账户（包括分区管理员账户）增加以下要求和限制：

1. 新建管理员账户时，密码长度必须在 8 至 116 个字符之间，而且必须由大写字母、小写字母、数字和特殊字符（除了大小写字母、数字以外的其他所有可见字符）中的至少三种字符组成。另外，密码中不能包含用户名，用户名不区分大小写。
2. 修改已有管理员账户的密码时，密码也必须满足第一条中的要求。
3. 新建的管理员账户在第一次登录时必须修改密码。启用强制密码修改模式前创建的管理员账户（包括修改过密码的默认账户）在下次登录时不会强制修改密码。
4. 如果从未修改过默认管理员账户密码，或者恢复过管理员账户的出厂配置，例如“**clear config factory**”，那么默认账户在下次登录时也必须修改密码。
5. 连续认证失败 5 次的管理员账户会被锁定五分钟。
6. 同一管理员账户修改密码时不能与最近使用过的 5 个密码相同。
7. 密码有效期为 90 天。到期未修改密码的管理员账户在下次登录时会被强制修改密码。

禁用强制密码修改模式后管理员账户不受以上要求的限制。

passwd forcemode rule [min_length] [min_letter_type] [min_digi_num] [min_caplett_num] [min_lowlett_num] [min_speclett_num] [max_contilett_num]

该命令用于设置管理员账户的密码复杂度规则。该命令在“**passwd forcemode**”命令启用后才能生效。

min_length 可选，该参数指定密码的最小长度，取值必须为 8 至 116 之间的整数。

默认值为 8。

min_letter_type 可选，该参数指定密码中包含的最少字符种类的数量，取值必须为 2 至 4 之间的整数。

	默认值为 3。
min_digi_num	可选，该参数指定密码中包含的数字最少数量，取值必须为 0 至 25 之间的整数。
	默认值为 0。
min_caplett_num	可选，该参数指定密码中包含的大写字母的最少数量，取值必须为 0 至 25 之间的整数。
	默认值为 0。
min_lowlett_num	可选，该参数指定密码中包含的小写字母的最少数量，取值必须为 0 至 25 之间的整数。
	默认值为 0。
min_speclett_num	可选，该参数指定密码中包含的特殊字符的最少数量，取值必须为 0 至 25 之间的整数。
	默认值为 0。
max_contilett_num	可选，该参数指定密码中包含的连续字符的最大数量，取值必须为 0 至 25 之间的整数。
	默认值为 0。

passwd forcemode lock [retry_times] [lockout_duration]

该命令用于设置达到连续认证失败的次数后管理员账户被锁定的时长。该命令在“**passwd forcemode**”命令启用后才能生效。

retry_times	可选，该参数指定连续认证失败的次数，取值必须为 3 至 10 之间的整数。
	默认值为 5。
lockout_duration	可选，该参数指定管理员账户被锁定的时长，单位为秒，取值必须为 60 至 600 之间的整数。
	默认值为 300。

passwd expire on [expire_days]

该命令用于启用密码过期功能。启用该功能后，密码将在超过有效期后失效。密码失效后，管理员如果没有更换密码，下次登录成功后，管理员会被强制要求修改密码。该功能默认设置为启用。

- “**passwd forcemode**”和“**passwd expire**”功能同时启用时，“**passwd expire**”功能生效。

- “**passwd forcemode**” 功能启用且 “**passwd expire**” 功能禁用时，“密码有效期为 90 天” 的要求将会失效，即密码永不过期。
- “**passwd forcemode**” 功能禁用时，无论 “**passwd expire**” 功能启用或禁用，“**passwd expire**” 功能失效。

expire_days 可选，该参数指定管理员账户的密码有效期，单位为天，取值必须为 3 至 365 之间的整数。

默认值为 90。



注意：该功能开启后只对后续创建的管理员账户和后续修改密码的管理员账户生效。

passwd expire off

该命令用于禁用密码过期功能。

show passwd forcemode

该命令用于显示强制密码修改模式的启用状态和密码复杂度规则、连续认证失败的次数以及管理员账户被锁定的时长的配置。



注意：在强制密码修改模式禁用时，该命令也能显示已经设置的密码复杂度规则、连续认证失败的次数以及管理员账户被锁定的时长。

show passwd expire

该命令用于显示密码过期验证功能是否开启以及设置的密码有效期。

system serialnumber

该命令用于手动生成 vAPV 序列号。该命令仅用于 vAPV。

system license <key> [validate|novalidate]

这个命令将允许用户给设备导入产品许可密钥。如果没有许可密钥，系统无法装载配置信息并且无法正常运行。

validate 该命令参数的默认选项。当用户输入许可密钥并执行该命令将密钥导入设备时，系统会首先对该密钥进行验证。验证成功后，系统会将密钥导入并存储起来。

novalidate 使用该参数选项，系统不会立刻对密钥予以验证，而是直接将密钥导入并存储起来。

system reboot [interactive|noninteractive]

这个命令将允许使用者重新启用设备。重启之后，设备将会使用最后一次保存（通过“**write memory**”命令）的系统配置。

interactive|noninteractive 该可选参数用于启用或禁用重新启动设备时的用户交互接口。当该参数被设置为“**interactive**”时，用户需要在系统命令行提示后输入“**YES**”才确认设备重启操作。当参数被设置为“**noninteractive**”时，设备将立即重新启动，系统不会提示任何信息。该参数的默认值是“**interactive**”。

system restart <service_name>

该命令用于重启指定服务。

process_name 该参数指定需要重启的服务名称。取值必须为“**system_service**”、“**hc_service**”、“**config_service**”、“**ha_service**”或“**llb_hc_service**”。



注意： 半小时内累计执行 4 次“**system restart system_service**”命令后，设备将重启。

system shutdown [halt|poweroff]

这个命令将终止设备的所有功能并且禁用执行命令行。运行该命令后，系统会提示管理员输入“**YES**”进行确认。之后系统的所有功能会在 60 秒后自动终止。

halt|poweroff 用于定义系统的终止模式。该参数为可选参数，默认为“**poweroff**”。

当使用“**halt**”时，系统将会在 60 秒后关闭。当系统关闭后，管理员可以通过重新连接电源线来启动系统。

当使用“**poweroff**”时，系统会在 60 秒后自动关闭。管理员可以按设备的电源按钮来启动系统。

system dump {on|off}

该命令用于启用或禁用系统转存功能。默认启用该功能。如果启用了该功能，当系统发生崩溃时，系统运行信息将会被保存到 **vmcore** 文件中，以供管理员将来查找和解决问题时使用。

show system dump

这条命令用于查看系统转存功能的启用状态。

system console reset

这条命令用来重置系统串口。执行完这条命令后，系统将会提示“Reset console”。

config terminal [force]

这个命令将允许用户进入到命令配置级别。配置可选参数“force”将强行终止其他已存在的配置会话。



注意：

- 当现存的配置会话处于活跃状态时，用户通过执行此命令进入到命令配置级别后，可能无法执行配置命令。
- 通过“**config multiconfig enable**”开启多登录 Config 级别功能后，命令“**config terminal force**”无法生效。

config multiconfig enable

该命令用于启用多登录 Config 级别功能。启用该功能后，系统允许同一时间多个管理员账户处于 Config 级别或同一管理员账户开启多个 Config 级别的 SSH 连接。该功能默认设置为禁用。

config multiconfig disable

该命令用于禁用多登录 Config 级别功能。禁用该功能后，同一时间只能有一个管理员账户处于 Config 级别。如果多个管理员账户同时处于 Config 级别或同一管理员账户开启多个 Config 级别的 SSH 连接，在其中一个 SSH 连接执行该命令后，其他的 SSH 连接将会被强制登出。

show config multiconfig

该命令用于显示多登录 Config 级别功能的状态。

config timeout <timeout>

该命令用于设置 Config 模式会话的超时时间。

当 Config 模式会话的不活动时间超出该超时时间时，无论是否有新的 Config 模式会话，当前 Config 会话都将回退到 Enable 模式。

timeout 超时时间以秒为单位，范围为 30~36000（10 小时）。
默认设置为 180 秒（3 分钟）。

show config timeout

这个命令将允许用户查看当前的超时时间设置。

clear config timeout

这个命令将允许用户清除当前的超时时间设置，并将恢复到默认设置 3 分钟。

system fallback [partition_number]

该命令用于下次启用设备时切换到另一个分区的系统。

partition_number 可选。该参数指定下一次启用设备时使用的分区的编号，取值必须为 0 至 3 之间的整数，且不允许指定为当前分区的编号。如果不指定该参数，设备默认升级下一个分区，并在下次启动时切换至下一个分区。

该参数仅对四分区硬件设备生效。



注意：在四分区系统硬盘上装载仅支持双分区的软件版本后，系统将无法启动，因此请勿在四分区硬盘上装载双分区软件版本。

no system fallback

这个命令将取消上一次“**system fallback**”设置。

clear config secondary

该命令用于将设备上除 primary 配置（通过命令“**clear config primary**”重置）以外的所有配置重置为默认值，包括 WebUI、NAT、FWD、SNMP、日志、域名服务器和代理服务器、集群、高可用性配置（不包含 SSF 对端节点配置）和配置同步的安全模式等。

如果启用三权分立功能，执行该命令后，三权分立功能为禁用状态，三权分立管理员用户和角色不会被删除，三权分立管理员用户和角色的关联关系将被删除。

clear config primary

该命令用于将一些基础网络配置重置为默认值，包括 IP 地址、访问列表、访问组、SSH IP 地址、Enable 级别密码以及“admin”用户的登录密码等，同时还将删除“admin”用户以外的其他用户。

如果系统中存在与这些配置相关的其他配置，那么该命令将无法执行。在这种情况下，请先执行“**clear config secondary**”命令清除其他相关配置，再执行“**clear config primary**”命令。

如果启用三权分立功能，执行该命令后，三权分立功能为启用状态，三权分立管理员用户、角色及两者的绑定关系不会被删除。

clear config all

该命令允许使用者重置设备上所有的配置。

clear config factorydefault

这个命令将重置设备的配置为出厂设置。与命令“**clear config all**”不同的是，这个命令还将清除以前的 SSL 私钥文件，同时恢复已导入的自定义 GeoIP 数据库，并删除记录 GeoIP 数据库修改操作的日志，因此以前的配置影响将彻底被消

除。本命令是交互类命令，执行时会提示信息 “Type ‘YES’ to revert the configuration to factory defaults”。使用者需要输入 “YES” 才能继续执行该操作。

show running [pattern]

显示当前设备运行配置以及所有功能的配置信息。

pattern 可选参数。指定用于匹配配置信息的字符串。例如“**show running tcp**”将显示所有包含字符串 tcp 的行。最多支持 100 个字符。

show startup [pattern]

这个命令允许用户查看上次使用命令 “**write memory**” 保存的配置。可选参数 “pattern” 作为命令执行的搜索项。例如 “**show startup tcp**” 将显示所有包含字符串 tcp 的行。

show version

该命令用于显示系统信息，如主机名、当前软件版本、其他分区软件版本、系统 CPU、有效内存和总内存、启用时刻、授权功能和启用时间。

show system partition

该命令用于显示设备各分区软件版本信息。

debug watch

该命令允许用户每间隔几秒钟执行一个命令来观察系统变化情况。这是一个交互式命令，系统将提示用户提供更多的信息。



注意：

- 推荐通过 SSH 或者 WebUI 连接方式运行此命令，而不要通过 Console 连接。
- 如果通过 Console 运行此命令，刷新闻隔（refresh interval）应设置为不小于 10 的整数。
- 管理员可以按 Ctrl+C 键随时停止该命令。按 Enter 键会在所观察子命令结束输出后停止该命令。

webui {on|off}

该命令用于启用或禁用 WebUI。默认情况下，WebUI 为禁用状态。

webui hostcheck {on|off}

该命令用于启用或者禁用 HTTP Host 和 Referer 头部检查功能。启用该功能后，系统检查客户端请求中的 Host 和 Referer 头部和服务器的 IP 地址和端口号是否一致。该功能默认设置为启用。

clear webui hostcheck

该命令用于重置 HTTP Host 和 Referer 头部检查功能。

webui port <port>

该命令用于修改访问 WebUI 的端口号。如不配置该命令，系统使用默认的端口号 8888。

port 该参数指定访问 WebUI 的端口号，取值必须为 1025 至 65,000 之间的整数。

clear webui port

该命令用于将访问 WebUI 的端口号重置为默认值 8888。

webui graph {on|off}

该命令用于启用或禁用 WebUI 的折线图统计功能。启用该功能后，设备会收集和保存统计信息，并通过折线图显示统计信息。禁用该功能后，WebUI 将不能以折线图形式显示统计信息。

webui graph refresh <interval>

该命令用于设置 WebUI 图表的刷新闻隔。

当不配置该命令时，WebUI 图表默认 10 秒钟刷新一次。

interval 该参数指定 WebUI 图表的刷新闻隔，单位为秒。取值必须为 10、20、30、60、180 或 300。

webui graph clear

该命令用来清除现存的图形统计信息。

webui language <login_language>

该命令用来设置 WebUI 接口的语言类型。首次登录时，WebUI 语言会与系统默认语言保持一致。后续登录时，WebUI 将根据管理员配置的语言类型来呈现内容。

login_language 这个参数值可以为 en（英语）、cn（简体中文）、jp（日语）、tw（繁体中文）。系统默认为 en（英语）。

clear webui language

该命令用来将 WebUI 接口的语言类型重置为英语。

webui ip <ip_address>

该命令用于设置允许访问 Web 用户接口的 WebUI IP 地址。执行该命令后，管理员只能通过指定 IP 地址访问设备。系统允许配置最多 8 条该命令。

ip_address 该参数指定 WebUI IP 地址。取值必须为 IPv4 或 IPv6 地址。



注意:

- 只有系统接口的 IP 地址和用于管理的 VIP 地址可以配置为 WebUI IP 地址。
- 当系统业务流量较高时，系统管理流量的通信可能会受到影响。管理员可以通过配置 WebUI IP 地址为管理流量分配独立的带宽来避免发生上述情况。

no webui ip <ip_address>

该命令用于删除一个指定的 WebUI IP 地址。

clear webui ip

清除设置的允许访问 Web 用户接口的 IP 地址。这将允许 Web 用户从任何接口访问 Web 用户接口。

webui source <source_ip> <netmask|prefix> [action]

该命令用于添加一条 WebUI 源 IP 地址限制规则。当参数 “source_ip” 与 “netmask|prefix” 的值与已配置规则的值相同时，该命令还可以修改该规则的动作。WebUI 源 IP 地址限制规则的动作可以为 “permit” 或 “deny”。“permit” 规则允许管理员从指定的源 IP 地址或网段通过 WebUI 方式访问系统；“deny” 规则拒绝管理员从指定的源 IP 地址或网段通过 WebUI 方式访问系统。系统允许配置最多 100 条 WebUI 源 IP 地址限制规则。如果没有配置任何 WebUI 源 IP 地址限制规则，系统对管理员通过 WebUI 方式访问系统使用的源 IP 地址不受限制。如果配置了 WebUI 源 IP 地址限制规则，当管理员通过 WebUI 方式访问系统时：

- 当源 IP 地址匹配上一条 “permit” 规则，且没有匹配任何 “deny” 规则时，系统允许管理员通过 WebUI 方式访问系统。
- 当源 IP 地址匹配上一条 “permit” 规则，但是也匹配上一条 “deny” 规则时，系统拒绝管理员通过 WebUI 方式访问系统。
- 当源 IP 地址没有匹配上任何一条 “permit” 规则，系统拒绝管理员通过 WebUI 方式访问系统。

source_ip 指定通过 WebUI 方式访问系统的源 IP 地址或网段。参数取值可以为 IPv4 或 IPv6。如果参数取值为 “0.0.0.0”，表示所有的 IPv4 地址。

注意: 对于 IPv6 地址，参数取值不能为 “: : ”。

netmask|prefix 指定源 IP 地址或网段对应的子网掩码或前缀长度。

- “netmask” 用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，其

值应是一个 1 到 128 之间的整数。

action

可选，该参数指定通过 WebUI 方式访问系统的源 IP 地址匹配该规则时所采取的动作。参数取值可以为：

- **permit**: 允许指定的源 IP 地址或网段通过 WebUI 方式访问系统。
- **deny**: 拒绝指定的源 IP 地址或网段通过 WebUI 方式访问系统。

默认值为 “permit”。



注意：如果只配置了 “deny” 规则，管理员不能从任何网段通过 WebUI 方式访问系统。

no webui source <source_ip> <netmask|prefix>

该命令用于删除指定的 WebUI 源 IP 地址限制规则。

clear webui source

该命令用于清除所有的 WebUI 源 IP 地址限制规则。

webui idletimeout <timeout>

该命令用于设置 WebUI 连接的闲置超时时间，当 WebUI 连接闲置的时间达到指定的值时，连接将自动断开。

当不配置该命令时，WebUI 连接默认会在闲置 15 分钟后自动断开。

timeout

该参数指定 WebUI 连接的闲置超时时间，单位为分钟。取值必须为 1 至 65535 之间的整数。

clear webui idletimeout

该命令用于将 WebUI 连接的闲置超时时间恢复为默认设置。

webui ssl settings clientauth {enable|disable}

该命令用于为 WebUI 启用或禁用 SSL 客户端认证功能，即 SSL 双向认证功能。启用该功能后，在登录 WebUI 执行 SSL 握手时，客户端和服务端将执行 SSL 双向认证。启用该功能前，需要使用 “**webui ssl import clientca**” 命令为设备 WebUI 导入客户端 CA 证书。该功能默认设置为禁用。

webui ssl settings authmandatory {enable|disable}

该命令用于为 WebUI 启用或禁用 SSL 客户端认证强制模式。开启该模式后，WebUI SSL 客户端必须通过身份认证后才能正常登录设备，否则 WebUI SSL 连

接请求将失败。该功能默认设置为启用。强制模式要在“**webui ssl settings clientauth enable**”命令启用之后再开启才能生效。

webui ssl settings ciphersuites <cipher_string>

该命令用于指定 WebUI 支持的密码套件。当不配置该命令时，默认的密码套件为

“ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384”。

cipher_string

该参数指定 WebUI 支持的密码套件。取值不区分大小写。如果要配置两种或两种以上密码套件，请使用冒号(:)来分隔密码套件。目前，WebUI 支持的密码套件如下：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES256-SHA256

webui ssl settings protocol <version>

该命令用于指定 WebUI 支持的 SSL 协议版本。当不配置该命令时，默认的 SSL 协议版本为“TLSv12”。

version

该参数指定 WebUI 支持的 SSL 协议版本。如果要配置多种版本，请使用冒号(:)来分隔协议版本。取值必须为：

- SSLv3：表示支持 SSLv3 协议版本。

- TLSv1: 表示支持 TLSv1.0 协议版本。
- TLSv11: 表示支持 TLSv1.1 协议版本。
- TLSv12: 表示支持 TLSv1.2 协议版本。
- ALL: 表示支持以上全部协议版本。

webui ssl import certificate [url]

该命令用于通过复制粘贴的方式或者从远端 FTP、TFTP 或 HTTP 服务器为 WebUI 导入 PEM 格式的证书链文件。PEM 格式的证书链文件包括证书链和关联的私钥。

当未指定“url”参数时，可以通过将 PEM 格式的证书链复制粘贴到 CLI 的方式导入证书。证书内容的最后一行必须输入“...”用于标记导入结束。

如果不配置该命令，系统将使用默认的证书。

url 可选。该参数指定导入 PEM 格式的证书链文件的 FTP、TFTP 或 HTTP URL。如果没有指定该参数，可以通过复制粘贴的方式导入证书链文件。

注意：FTP 类型 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。



注意：系统暂不支持导入 SM2 证书和 RSAPSS 证书。

webui ssl import clientca [url]

该命令用于通过复制粘贴的方式或者从远端 FTP、TFTP 或 HTTP 服务器为 WebUI 导入用于 SSL 客户端认证的 CA 证书文件。

当未指定“url”参数时，可以通过将 PEM 格式的证书复制粘贴到 CLI 的方式导入证书。证书内容的最后一行必须输入“...”用于标记导入结束。

url 可选。该参数指定导入证书的 FTP、TFTP 或 HTTP URL。如果没有指定该参数，可以通过复制粘贴的方式导入证书。

注意：FTP 类型 URL

（ftp://user:password@host:port/path）中的“path”需使用相对路径。

show webui ssl certificate

该命令用于显示为 WebUI 导入的证书。

show webui ssl clientca

该命令用于显示为 WebUI 导入的客户端 CA 证书。

clear webui ssl certificate

该命令用于将 PEM 格式的证书重置为默认值。

clear webui ssl clientca

该命令用于删除为 WebUI 导入的客户端 CA 证书。

show webui ssl settings

该命令用于显示所有 WebUI SSL 功能的配置信息。

例如：

```
Demo(config)#show webui ssl settings
webui ssl settings clientauth disable
webui ssl settings authmandatory enable
webui ssl settings ciphersuites
"ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384"
webui ssl settings protocol "TLSv12"
```

clear webui ssl settings

该命令用于将 WebUI SSL 功能恢复为默认配置

show webui settings

该命令用于显示 WebUI 的所有配置。

webui semode on

该命令用于启用 WebUI 安全增强模式。启用 WebUI 安全增强模式后，WebUI 的管理流量也将接受 WAF 防护，并能应对相关漏洞及时添加并调整规则防护。该功能默认配置为启用。

webui semode off

该命令用于禁用 WebUI 安全增强模式。

webui semode custom import <url>

该命令用于为 WebUI 安全增强功能导入自定义攻击签名配置文件。

url 该参数指定导入自定义攻击签名配置文件的 HTTP 或 FTP URL 地址。

clear webui semode custom import

该命令用于清除为 WebUI 安全增强功能导入的自定义攻击签名配置文件。

webui semode custom export <url>

该命令用于为 WebUI 安全增强功能将自定义攻击签名相关配置导出到外部 FTP 服务器。

url 该参数指定存放自定义攻击签名相关配置的 FTP URL 地址。

webui semode log export <url>

该命令用于将 WebUI 安全增强功能生成的日志导出到外部 FTP 服务器。

url 该参数指定用于存放日志的 FTP URL 地址。

xmlrpc on [https|http]

该命令用于启用 XML RPC 功能，以允许管理员从远程访问和配置系统。默认情况下，系统禁用该功能。

https|http 可选，该参数指定用来传输 XML RPC 消息的协议。默认值为“https”。



注意：开启 XML RPC 功能后，如果没有使用“**xmlrpc port**”命令修改 XML RPC 端口，那么系统将侦听默认端口 9999。

xmlrpc off

该命令用于禁用 XML RPC 功能。

xmlrpc ip <ip_address>

该命令用于配置 XML RPC IP 地址，一般设置为接口 IP 地址或用于管理的虚拟 IP 地址。系统只支持配置一个 XML RPC IP 地址。

如果指定了 XML RPC IP 地址，管理员只能使用指定的 IP 地址通过 XML RPC 访问设备。如果不指定 XML RPC IP 地址，管理员可以使用设备的任意 IP 地址通过 XML RPC 访问设备。

ip_address 该参数指定 XML RPC IP 地址。取值必须为 IPv4 或 IPv6 地址。

clear xmlrpc ip

该命令用于清除 XML RPC IP 地址配置。

xmlrpc authentication {on|off}

action 可选，该参数指定通过 XML RPC 方式访问系统的源 IP 地址匹配该规则时所采取的动作。参数取值可以为：

- **permit**: 允许指定的源 IP 地址或网段通过 XML RPC 方式访问系统。
- **deny**: 拒绝指定的源 IP 地址或网段通过 XML RPC 方式访问系统。

默认值为 “permit”。



注意：如果只配置了 “deny” 规则，管理员不能从任何网段通过 XMLRPC 方式访问系统。

no xmlrpc source <source_ip> <netmask|prefix>

该命令用于删除指定的 XML RPC 源 IP 地址限制规则。

clear xmlrpc source

该命令用于清除所有的 XML RPC 源 IP 地址限制规则。

show xmlrpc

该命令用于显示 XML RPC 的所有配置。

clear xmlrpc all

该命令用于将 XML RPC 的所有配置重置为默认值。

system update <url> [immediate|deferred] [partition_number]

该命令用于导入提供的新版本软件。此外，用户也可通过设置可选参数 “immediate|deferred”，立即对系统进行升级或者在下次启动设备时再进行升级。如果可选参数设置为 “immediate”，用户通过该命令导入公司提供的 URL 地址后，设备将从该地址导入升级包，完成升级操作，导入之前的配置信息，然后重启系统。如果该参数设置为 “deferred”，用户运行该命令后，系统在后台进行升级操作及配置信息同步操作，不对当前系统造成影响。但是系统会把当前状态记录为 “deferred”，并且保存升级操作完成后所有新增的配置信息。当设备下次启动时，升级后的系统开始生效，运行命令 “**write all deferred**” 后，之前版本中新增的配置信息也将同步导入新系统。

url 指定 URL 地址。管理员可通过该 URL 地址导入升级包。

注意：FTP 或 SFTP 类型 URL

（ftp://user:password@host:port/path 或 sftp://user:password@host:port/path）中的 “path” 需使用相对路径。

immediate deferred	可选。如果该参数设置为“immediate”，系统会立刻进行升级，然后重启设备。如果该参数设置为“deferred”，系统会在后台进行升级操作及信息同步操作，不对当前系统造成影响；当设备下次启动时，升级后的系统才开始生效。
partition_number	可选。该参数指定待升级的分区的编号，取值必须为 0 至 3 之间的整数，且不允许指定为当前分区的编号。通过“show version”和“show system partition”命令，可以查看各分区软件版本信息。如果不指定该参数，设备默认升级下一个分区，并在下次启动时切换至下一个分区。 该参数仅对四分区硬件设备生效。



注意：

- 在四分区系统硬盘上装载仅支持双分区的软件版本后，系统将无法启动，因此请勿在四分区硬盘上装载双分区软件版本。
- 若 SSH 连接在安装包下载过程中断开，则升级失败；若 SSH 连接在安装包下载完成后断开，则升级成功。

show system update deferred

该命令用于显示当前系统是否存在待完成的延时升级操作。

system patch update <url>

该命令用于为系统安装补丁包。

补丁包是针对特定版本所提供的升级包，只能安装在特定版本上，安装后版本号不变。通过“**show version**”命令，可以到“Patch version”项查看补丁包版本号和安装时间，例如“p1 on Tues May 23 10:48:19 2021”。

补丁包只能向上升级，不能降级，例如从 p1 升级到 p2 后，不能再通过该命令降级到 p1。

安装补丁包后，系统不会重启，但是未保存的配置可能会丢失，因此在安装之前，建议通过“**write memory**”命令保存配置。

url 该参数指定补丁包所在的 URL 地址，支持 HTTP 和 FTP URL。

system patch rollback

该命令用于将当前的补丁版本回退到原版本，即未安装任何补丁包时的版本。例如系统在安装了补丁版本 p1 和 p2 后的版本是 “p2 on Tues May 25 08:32:45 2021”，那么在执行该命令后，系统将回退到未安装任何补丁包时的版本。

write all deferred

该命令用于保存当前配置信息。如果当前系统存在待完成的延时升级操作，则运行该命令后，系统将保存当前系统的配置信息并同步到新的系统。如果当前系统不存在待完成的延时升级操作，则该命令将保存配置信息，即，提供与 “**write memory**” 命令相同的功能。

ssh {on|off}

这个命令用于启用或禁用设备的 SSH 功能。该功能默认是启用的。

ssh ip <ip_address>

该命令用于配置 SSH IP 地址。如果指定了 SSH IP 地址，管理员只能使用指定的 IP 地址通过 SSH 连接访问设备。如果不指定 SSH IP 地址，管理员可以使用设备的任意 IP 地址通过 SSH 连接访问设备。系统允许配置最多 8 条该命令。

当系统业务流量较高时，系统管理流量的通信可能会受到影响。管理员可以通过配置 SSH IP 地址为管理流量分配独立的带宽来避免发生上述情况。

ip_address 该参数指定 SSH IP 地址。取值必须为 IPv4 或 IPv6 地址。



注意：

- 执行命令 “**clear config primary**” 将删除 SSH IP 地址的配置信息。
- 同步节点必须配置相同的 SSH IP 地址。执行命令 “**synconfig to**” 或 “**synconfig from**” 不能同步 SSH IP 地址的配置信息。
- 在集群和 HA 中，如果虚拟 IP 地址被配置为 SSH IP 地址，当主控设备失效时，管理员需要新的主控设备上重新启用 SSH 功能。
- 只有系统接口的 IP 地址和用于管理的 VIP 地址可以配置为 SSH IP 地址，SLB VIP 和 NAT VIP 不能配置为 SSH IP 地址。

no ssh ip <ip_address>

该命令用于删除一个 SSH IP 地址的配置。

clear ssh ip

该命令用于清除所有 SSH IP 地址的配置。

ssh port [port_number]

该命令用于设置 SSH 监听端口。如不配置该命令，管理员通过 SSH 连接设备时需使用默认端口 22。

port_number 可选。该参数指定 SSH 端口号，取值必须为 1 至 65535

之间的整数。

默认值为 22。

ssh source <source_ip> <netmask|prefix> [action]

该命令用于添加一条 SSH 源 IP 地址限制规则。当参数 “source_ip” 与 “netmask|prefix” 的值与已配置规则的值相同时，该命令还可以修改该规则的动作。SSH 源 IP 地址限制规则的动作可以为 “permit” 或 “deny”。“permit” 规则允许管理员从指定的源 IP 地址或网段通过 SSH 方式访问系统；“deny” 规则拒绝管理员从指定的源 IP 地址或网段通过 SSH 方式访问系统。系统允许配置最多 100 条 SSH 源 IP 地址限制规则。如果没有配置任何 SSH 源 IP 地址限制规则，系统对管理员通过 SSH 方式访问系统使用的源 IP 地址不受限制。如果配置了 SSH 源 IP 地址限制规则，当管理员通过 SSH 方式访问系统时：

- 当源 IP 地址匹配上一条 “permit” 规则，且没有匹配任何 “deny” 规则时，系统允许管理员通过 SSH 方式访问系统。
- 当源 IP 地址匹配上一条 “permit” 规则，但是也匹配上一条 “deny” 规则时，系统拒绝管理员通过 SSH 方式访问系统。
- 当源 IP 地址没有匹配上任何一条 “permit” 规则，系统拒绝管理员通过 SSH 方式访问系统。

source_ip 指定通过 SSH 方式访问系统的源 IP 地址或网段。参数取值可以为 IPv4 或 IPv6。如果参数取值为 “0.0.0.0”，表示所有的 IPv4 地址；如果参数取值为 “::”，表示所有 IPv6 地址。

netmask|prefix 指定源 IP 地址或网段对应的子网掩码或前缀长度。

- “netmask” 用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。
- “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。

action 可选，该参数指定通过 SSH 方式访问系统的源 IP 地址匹配该规则时所采取的动作。参数取值可以为：

- **permit**: 允许指定的源 IP 地址或网段通过 SSH 方式访问系统。
- **deny**: 拒绝指定的源 IP 地址或网段通过 SSH 方式访问系统。

默认值为 “permit”。



注意：如果只配置了“deny”规则，管理员不能从任何网段通过 SSH 方式访问系统。

no ssh source <source_ip> <netmask|prefix>

该命令用于删除指定的 SSH 源 IP 地址限制规则。

clear ssh source

该命令用于清除所有的 SSH 源 IP 地址限制规则。

ssh import key <user_name> [url]

该命令用于为指定管理员账户导入一个 SSH 公共密钥。

user_name 该参数指定已存在的管理员账户的用户名。

url 可选。该参数指定用于下载 SSH 公共密钥的 URL 链接，必须为 HTTP、FTP 或 TFTP 类型的 URL。如不指定该参数，则需手动输入 SSH 公共密钥。设备支持导入 SSH 格式或 OpenSSH 格式的公共密钥，公共密钥长度最小为 1024 比特，文件最大不超过 4096 字节。

no ssh key <user_name>

该命令用于删除为指定管理员账户设置的 SSH 公共密钥。

show ssh key [user_name]

该命令用于显示指定管理员账户的 SSH 公共密钥配置信息。当不指定参数“user_name”时，该命令显示所有管理员账户的 SSH 公共密钥配置信息。

clear ssh key

该命令用于删除所有 SSH 公共密钥。

ssh auth key {on|off} <user_name>

该命令用于对指定用户启用或禁用 SSH 公共密钥认证方法。对于一个新建的管理员账户，SSH 公共密钥认证方法默认是关闭的。

ssh auth passwd {on|off} <user_name>

该命令用于对指定管理员账户启用或禁用 SSH 密码认证方法。对于一个新建的管理员账户，SSH 密码认证方法默认是开启的。

ssh cipher <cipher_string>

该命令用于配置支持的 SSH 加密算法。

当不配置该命令时，系统默认支持的 SSH 加密算法是 aes128-ctr、aes192-ctr、aes256-ctr、aes128-gcm@openssh.com 和 aes256-gcm@openssh.com。

cipher_string	该参数指定 SSH 加密算法，取值可以为 aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr、arcfour128、arcfour256、arcfour、blowfish-cbc、cast128-cbc、aes128-gcm@openssh.com、aes256-gcm@openssh.com、chacha20-poly1305@openssh.com 中的一种或多种算法。当需要配置多种算法时，请使用逗号 (,) 来分隔。

clear ssh cipher

该命令用于将 SSH 加密算法配置恢复为默认配置。

ssh alivetime [interval] [max_check_times]

该命令用于配置闲置状态的 SSH 连接的存活时间。

配置该命令后，系统会按照“interval”参数定义的间隔时间发送探测报文，并等待响应，当连续收不到响应的次数达到“max_check_times”参数指定的值时，系统会终止 SSH 连接。

当不配置该命令时，系统将不探测 SSH 连接是否处于闲置状态。

interval	可选，该参数指定探测报文的发送间隔，单位为秒，取值必须为 1 至 86,400 之间的整数。

默认值为 60。

max_check_times	可选，该参数指定探测报文的发送次数，取值必须为 1 至 30 之间的整数。

默认值为 3。

no ssh alivetime

该命令用于删除“ssh alivetime”命令的配置。

ssh idletimeout [timeout]

该命令用于设置 SSH 连接和 Console 连接的闲置超时时间，当 SSH 连接闲置的时间或者 Console 连接闲置的时间达到指定的值时，系统将终止 SSH 连接或 Console 连接。

当不配置该命令时，系统将在 SSH 连接闲置 30 分钟或 Console 连接闲置 30 分钟后断开连接。

timeout	可选。该参数指定 SSH 连接的闲置超时时间和 Console 连接的闲置超时时间，单位为分钟。取值必须为 1 至

65535 之间的整数。默认值为 30。

clear ssh idletimeout

该命令用于将 SSH 连接的闲置超时时间恢复为默认设置。

ssh kex <kex_list>

该命令用于配置 SSH 的密钥交换算法。如果未配置该命令，系统默认的 SSH 的密钥交换算法为 “curve25519-sha256、curve25519-sha256@libssh.org、ecdh-sha2-nistp256、ecdh-sha2-nistp384 和 ecdh-sha2-nistp521”。

kex_list 该参数指定 SSH 密钥交换算法，取值可以为 curve25519-sha256、curve25519-sha256@libssh.org、diffie-hellman-group1-sha1、diffie-hellman-group14-sha1、diffie-hellman-group14-sha256、diffie-hellman-group16-sha512、diffie-hellman-group18-sha512、diffie-hellman-group-exchange-sha1、diffie-hellman-group-exchange-sha256、ecdh-sha2-nistp256、ecdh-sha2-nistp384、ecdh-sha2-nistp521 中的一种或几种算法。

当需要配置几种算法时，请使用逗号“,”来分隔。

注意：当取值包含特殊字符或者同时配置多种算法时需要将其置于双引号内。

clear ssh kex

该命令用于将 SSH 的密钥交换算法恢复为默认算法。

show ssh config

该命令用于显示 SSH 功能的开启状态和相关配置。

18.2 备份管理

25.2.1 配置备份

write file <file_name>

该命令用于在本地磁盘上保存当前运行配置到备份文件。

file_name 该参数指定保存在本地的配置备份文件的文件名。取值必须为长度不大于 182 个字节的字符串，支持大小写字母、数字以及特殊字符 “@”、“-”、“_”、“.” 和

“!”，不允许配置特殊字符“..”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

注意：取值不支持全为“.”。



注意：备份文件小于 100 MB。

write all file <file_name> <password>

该命令用于将当前设备上的所有系统配置、运行配置和分区配置备份到指定的 TGZ 文件中。

file_name

该参数指定保存在本地的配置备份文件的文件名。取值必须为长度不大于 182 个字节的字符串，支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

password

该参数指定 TGZ 配置备份文件的访问密码。取值必须为长度不大于 32 个字节的字符串，支持字母、数字和以下特殊字符：

“~”、“%”、“^”、“*”、“(”、“)”、“_”、“+”、“=”、“ ”、“{”、“}”、“[”、“]”、“!”、“:”、“\”、“.”、“?”、“/”和“!”。

当取值包含特殊字符时，必须置于双引号内。而且，取值的前两位不能使用除“.”、“/”以外的其他特殊字符。

write memory

该命令用于保存当前系统配置到文件并且作为启用的设备配置。需要注意的是，如需保存分区内的配置，需执行“**write segment memory**”命令进行保存。

show memory

该命令允许用户显示和设备有关的内存关键信息。

config file <file_name>

该命令将允许用户从终端改变当前配置，或者从保存在本地的文件中恢复当前配置。

file_name 该参数指定要恢复的本地的配置备份文件的文件名。取值支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”和“!”，不允许配置特殊字符“..”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

config all file <file_name> <password> [mode]

该命令用于加载指定的 TGZ 配置备份文件。

file_name 该参数指定要恢复的本地的配置备份文件的文件名。取值支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

password 该参数指定 TGZ 配置备份文件的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“\”。

mode 可选。该参数指定配置恢复模式。

- 1: 表示只恢复变化的配置。
- 2: 表示恢复全部配置。该模式下，设备将先清除所有配置，再加载导入的配置。

默认值为 1。

config memory

该命令允许用户从上次“**write memory**”命令的结果中恢复配置。需要注意的是，如需恢复分区内的配置，需先在系统模式下执行该命令，再在分区模式下执行该命令。

config net tftp <tftp_server_ip> <config_file_name>

该命令允许用户访问保存在 TFTP 服务器的配置信息。您需要提供 IP 地址或服务器名称和配置文件的名称。

tftp_server_ip 该参数指定远程 TFTP 服务器的 IPv4 地址。

config_file_name 该参数指定要恢复的保存在远程 TFTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许

配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

config net sftp <remote_server_ip> <user_name> <config_file_name>

该命令用于访问保存在远程 SFTP 服务器上的配置信息。要访问远程 SFTP 服务器信息，您需要提供 SFTP 服务器的 IP 地址、远程服务器的访问用户名（将出现提示输入您的服务器用户密码）和配置文件名称。

remote_server_ip	该参数指定远程主机的 IP 地址。
user_name	该参数指定访问远程主机的用户名。
config_file_name	该参数指定要恢复的保存在远程 SFTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

config net scp {remote_server_ip|name} <user_name> <config_file_name>

该命令允许用户访问保存在 SCP 服务器上的配置信息。您需要提供 IP 地址（置于双引号内）或服务器名称、远程服务器的访问用户名（将出现提示输入您的服务器用户密码）和配置文件名称。

remote_server_ip name	该参数指定远程 SCP 服务器的 IP 地址或服务器名称。
user_name	该参数指定访问远程 SCP 服务器的用户名。
config_file_name	该参数指定要恢复的保存在远程 SCP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

config net http <http_url>

该命令允许用户下载保存在 web 服务器的配置文件。例如，如果您需要从“www.xyx.com” Web 服务器上下载一个名称为“example.conf”的配置文件，那么这条命令的“http_url”参数就应该为“http://www.xyz.com/example.conf”。

http_url 该参数指定用于恢复保存在远程 Web 服务器上的配置备份文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”、“!”、“:”。

config net ftp <ftp_ip> <ftp_username> <file_name>

该命令用于将备份至远程 FTP 主机上的配置文件通过 FTP 协议方式导入设备。

ftp_ip 该参数指定远程 FTP 主机的 IP 地址。

ftp_username 该参数指定访问远程 FTP 主机的用户名。

file_name 该参数指定要恢复的保存在远程 FTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

write net tftp <tftp_ip> [file_name]

该命令用于将当前配置备份到远程 TFTP 服务器。

tftp_ip 该参数指定远程 TFTP 服务器的 IPv4 地址。

file_name 可选，该参数指定保存在远程 TFTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。默认值为“ca.cfg”。

write net scp {remote_server_ip|name} <user_name> <config_file_name>

该命令将当前配置保存到远程 SCP 服务器。该远程服务器需开启密码验证功能，在指定该 SCP 服务器的 IP 地址（置于双引号内）或名称、访问用户名和配置文件名称之后，将提示输入该服务器的验证密码。

remote_server_ip|name 该参数指定远程 SCP 服务器的 IP 地址或服务器名称。

user_name 该参数指定远程 SCP 服务器的访问用户名。

config_file_name 该参数指定保存在远程 SCP 服务器的配置备份文件的

名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

write net ftp <ftp_ip> <ftp_username> <file_name>

该命令用于当前配置保存到远程 FTP 服务器。

ftp_ip	该参数指定远程 FTP 主机的 IP 地址。
ftp_username	该参数指定访问远程 FTP 主机的用户名。
file_name	该参数指定保存在远程 SFTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

write net sftp <remote_server_ip> <user_name> <config_file_name>

该命令用于将当前配置保存到远程 SFTP 服务器。该远程服务器需开启密码验证功能，在指定该 SFTP 服务器的 IP 地址（置于双引号内）或名称、访问用户名和配置文件名称之后，将提示输入该服务器的验证密码。

remote_server_ip	该参数指定远程主机的 IP 地址。
user_name	该参数指定访问远程主机的用户名。
config_file_name	该参数指定指定配置文件名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

write all tftp <tftp_ip> <remote_file_name> <password>

该命令用于将设备上的所有系统配置、运行配置和分区配置通过 TFTP 协议备份至一台远程主机。

tftp_ip	该参数指定远程主机的 IP 地址。
remote_file_name	该参数指定保存在远程 TFTP 服务器的配置备份文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

password 该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“`”。

write all sftp <server_name> <user_name> <remote_file_path> <password>

该命令用于将设备上的所有系统配置、运行配置和分区配置通过 SFTP 协议备份至一台远程主机。

server_name 该参数指定远程主机的主机名称或 IP 地址。

user_name 该参数指定访问远程主机的用户名。

remote_file_path 该参数指定远程 SFTP 主机上保存配置备份文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

password 该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“`”。

write all scp <server_name> <user_name> <remote_file_path> <password>

该命令用于将设备上的所有系统配置、运行配置和分区配置通过 SCP 协议备份至一台远程主机。

server_name 该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。

user_name 该参数指定访问远程主机的用户名。

remote_file_path 该参数指定远程主机上存储配置文件的存储路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”。

“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

password

该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“`”。

config all tftp <tftp_ip> <remote_file_name> <password> [mode]

该命令用于将备份至远程主机上的配置文件通过 TFTP 协议方式导入设备。

tftp_ip

该参数指定远程主机的 IP 地址。

remote_file_name

该参数指定存储在远程主机上的配置文件的名称。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。

password

该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“|”和“`”。如果密码输入错误，则无法导入配置文件中的 backup.conf 的内容。

mode

可选。该参数指定配置恢复模式。

- 1：表示只恢复变化的配置。
- 2：表示恢复全部配置。该模式下，设备将先清除所有配置，再加载导入的配置。

默认值为 1。

**config all sftp <server_name> <user_name> <remote_file_path>
<password> [mode]**

该命令用于将备份至远程主机上的配置文件通过 SFTP 协议方式导入设备。

server_name	该参数指定远程主机的主机名称或 IP 地址。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储配置文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。
password	该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“ ”和“`”。如果密码输入错误，则无法导入配置文件中的 backup.conf 的内容。
mode	可选。该参数指定配置恢复模式。 • 1: 表示只恢复变化的配置。 • 2: 表示恢复全部配置。该模式下，设备将先清除所有配置，再加载导入的配置。 默认值为 1。

config all scp <server_name> <user_name> <remote_file_path> <password> [mode]

该命令用于将备份至远程主机上的配置文件通过 SCP 协议方式导入设备。

server_name	该参数指定远程主机的主机名称或 IP 地址。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储配置文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。
password	该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符“\$”、“#”、“,”、“<”、“>”、“&”、“;”、“ ”和“`”。

“,”、“<”、“>”、“&”、“;”、“|”和“`”。

如果密码输入错误，则无法导入配置文件中的 backup.conf 的内容。

mode

可选。该参数指定配置恢复模式。

- 1: 表示只恢复变化的配置。
- 2: 表示恢复全部配置。该模式下，设备将先清除所有配置，再加载导入的配置。

默认值为 1。

no config <file_name>

该命令用于删除指定的配置备份文件。

file_name

该参数指定需要删除的配置备份文件的名称，文件名中必须包含扩展名。

show config file [file_name] [regex]

该命令用于显示指定配置备份文件中匹配过滤字符串的配置信息。

file_name

该参数指定需要显示的配置备份文件的名称，文件名中不包含扩展名。如不指定该参数，则显示所有的配置备份文件。

regex

该参数指定用于过滤配置备份文件中配置信息的字符串，仅在指定了参数“file_name”时才可用。例如，命令行“**show config file new_lb tcp**”将列出配置备份文件“new_lb”中所有包含“tcp”字符串的配置信息。如不指定该参数，则显示指定配置备份文件中的所有配置信息。

clear config file

清除所有用户定义的配置文件。

show config consistency

该命令用于检查配置一致性。

- 系统模式下：执行该命令后，系统将显示设备当前运行的配置和最近一次管理员通过“**write memory**”和“**write segment memory**”命令保存的配置间的差异。

- 分区模式下：执行该命令后，系统只显示该分区当前运行的配置和最近一次管理员通过 “**write memory**” 命令保存的配置间的差异。

如果当前运行的配置和最近一次管理员通过 “**write memory**” 命令保存的配置间存在差异：

- 当前运行的配置比保存的配置少：系统将显示所有缺少的配置，且在配置前面标记[missing]。
- 当前运行的配置比保存的配置多：系统将显示所有额外的配置，且在配置前面标记[added]。



注意：该命令只检查命令行配置。

write regular all<backup_index> <url> <password> [timestamp]
[backup_time]

该命令用于定期自动将设备上的所有系统配置、运行配置和分区配置备份至一台远程主机。

backup_index	该参数指定自动备份的索引。取值为 1 到 15 之间的整数。
url	该参数指定远程主机上存储配置文件的 SCP URL、SFTP URL、TFTP URL、FTP URL 或 HTTP URL 路径。取值支持大小写字母、数字以及特殊字符 “@”、“-”、“_”、“.”、“/” 和 “!”，不允许配置特殊字符 “..”、“./”、“../”，且不能以 “-” 或 “.” 开头。必须置于双引号内。取值格式为： <protocol>://[username]:[password]@<ip>:[port]/[path]/<filename.tgz>。取值文件后缀名必须以.tgz 结尾。 例如： ftp://admin:admin@192.168.1.100:21/home/config.tgz 注意：IPv6 地址需要置于中括号内，TFTP 协议不支持 IPv6。
password	该参数指定存储到远程主机上的配置文件中 backup.conf 的访问密码，取值必须为长度不大于 32 个字节的字符串，但是不能包含以下特殊字符 “\$”、“#”、“,”、“<”、“>”、“&”、“;”、“ ” 和 “`”。
timestamp	可选。该参数指定自动备份的文件名后缀的时间戳（日期和时间）的格式。具体格式遵循标准 strftime，支持的格式包括 “%a”、“%A”、“%b”、“%B”、“%c”、

“%C”、“%d”、“%D”、“%e”、“%F”、“%g”、“%G”、“%h”、“%H”、“%I”、“%j”、“%k”、“%l”、“%m”、“%M”、“%N”、“%p”、“%P”、“%r”、“%R”、“%s”、“%S”、“%t”、“%T”、“%u”、“%U”、“%V”、“%w”、“%W”、“%x”、“%X”、“%y”、“%Y”、“%z”和“%Z”，默认值为“%Y%m%d%H%M”，表示“年份、月份、日期、小时和分钟”。例如自动备份的 URL 中输入的文件名为 backup.tgz，则备份文件名为 backup_202401010000.tgz

backup_time

可选。该参数指定自动备份的时间。取值格式遵循标准的 Crontab 表达式格式，即“minute hour date month week”，各个。其中时间信息项的取值如下：

- minute: 表示分钟，取值范围为 0 到 59。
- hour: 表示小时，取值范围为 0 到 23。
- date: 表示日期，取值范围为 1 到 31。
- month: 表示月份，取值范围为 1 到 12。
- week: 表示星期，可以为两种取值：
 - 0 到 7。0 和 7 到表示星期日。
 - MON、TUE、WED、THU、FRI、SAT 和 SUN。不区分大小写。

各个时间信息项通过空格分隔。上述时间信息项还支持配置为：

- “*”：表示通配符。表示该字段所有可能值。例如“*”在分钟字段中表示“每分钟”。
- “,”：表示逗号，用来指定多个离散值。例如“1,15”表示“1”和“15”。
- “-”：表示连字符，用来指定一个值的范围。例如“1-15”表示从“1”到“15”。
- “/n”：表示每隔 n 个单位执行一次。例如“*/15”在分钟字段，表示每隔 15 分钟执行一次。

默认值为“0 2 * * *”，表示每天 2:00 备份一次。

示例：

每 1 小时定时执行一次规则，配置如下：

```
Demo(config)#write regular all 1 "ftp://test:test@192.168.1.100/backup/config.tgz"
"1234567" "%Y%m%d%H%M" "0 *1 * *"
```

每个月一号 0 点 0 分定时执行一次规则，配置如下：

```
Demo(config)#write regular all 1 "ftp://test:test@192.168.1.100/backup/config.tgz"
"1234567" "%Y%m%d%H%M" "0 0 1 * *"
```

每天 0 点定时执行一次规则，配置如下：

```
Demo(config)#write regular all 1 "ftp://test:test@192.168.1.100/backup/config.tgz"
"1234567" "%Y%m%d%H%M" "0 0 * * *"
```

no write regular all <backup_index>

该命令用于删除指定的自动备份的配置。

show write regular all

该命令用于显示所有自动备份的配置。

clear write regular all

该命令用于清除所有自动备份的配置。

show write regular log forward

该命令用于正序显示所有自动备份结果的日志。

show write regular log backward

该命令用于逆序显示所有自动备份结果的日志。

clear write regular log

该命令用于清除所有自动备份结果的日志。

25.2.2 日志备份

**write cli log ftp <server_name> <user_name> <remote_file_path>
<password>**

该命令用于将设备上的所有 CLI 日志通过 FTP 协议备份至一台远程主机。

server_name 该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。

user_name 该参数指定访问远程主机的用户名。

remote_file_path 该参数指定远程主机上存储配置文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，

且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write clilog scp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 CLI 日志通过 SCP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 CLI 日志文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write clilog sftp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 CLI 日志通过 SFTP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 CLI 日志文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write fastlog ftp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 Fastlog 通过 FTP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 Fastlog 文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write fastlog scp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 Fastlog 通过 SCP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 Fastlog 文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write fastlog sftp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 Fastlog 通过 SFTP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 Fastlog 文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

结尾。

注意：配置文件后缀名必须为 “.tgz”。

write dnslog ftp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 DNS 日志通过 FTP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 DNS 日志文件的路径。支持大小写字母、数字以及特殊字符 “@”、“-”、“_”、“.”、“/” 和 “!”，不允许配置特殊字符 “..”、“./”、“../”，且不能以 “-” 或 “.” 开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为 “.tgz”。

write dnslog scp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 DNS 日志通过 SCP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为 IPv4 地址时必须置于双引号内。
user_name	该参数指定访问远程主机的用户名。
remote_file_path	该参数指定远程主机上存储 DNS 日志文件的路径。支持大小写字母、数字以及特殊字符 “@”、“-”、“_”、“.”、“/” 和 “!”，不允许配置特殊字符 “..”、“./”、“../”，且不能以 “-” 或 “.” 开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为 “.tgz”。

write dnslog sftp <server_name> <user_name> <remote_file_path>
<password>

该命令用于将设备上的所有 DNS 日志通过 SFTP 协议备份至一台远程主机。

server_name	该参数指定远程主机的主机名称或 IP 地址。当取值为

IPv4 地址时必须置于双引号内。

user_name

该参数指定访问远程主机的用户名。

remote_file_path

该参数指定远程主机上存储 DNS 日志文件的路径。支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。当取值只包含数字或包含特殊字符时，必须置于双引号内。文件名以.tgz 结尾。

注意：配置文件后缀名必须为“.tgz”。

write regular cliolog <backup_index> <url> [timestamp] [backup_time]

该命令用于定期自动将设备上的所有 CLI 日志备份至一台远程主机。

bakcup_index

该参数指定自动备份的索引。取值为 1 到 15 之间的整数。

url

该参数指定远程主机上存储 CLI 日志文件的 SCP URL、SFTP URL、TFTP URL、FTP URL 或 HTTP URL 路径。取值支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。必须置于双引号内。取值格式为：

<protocol>://[username]:[password]@<ip>:[port]/[path]/<filename.tgz>。取值文件后缀名必须以.tgz 结尾。

例如：

ftp://admin:admin@192.168.1.100:21/home/cliolog.tgz

注意：IPv6 地址需要置于中括号内，TFTP 协议不支持 IPv6。

timestamp

可选。该参数指定自动备份的文件名后缀的时间戳（日期和时间）的格式。具体格式遵循标准 strftime，支持的格式包括“%a”、“%A”、“%b”、“%B”、“%c”、“%C”、“%d”、“%D”、“%e”、“%F”、“%g”、“%G”、“%h”、“%H”、“%I”、“%j”、“%k”、“%l”、“%m”、“%M”、“%N”、“%p”、“%P”、“%r”、“%R”、“%s”、“%S”、“%t”、“%T”、“%u”、“%U”、“%V”、“%w”、“%W”、“%x”、“%X”、“%y”、“%Y”、“%z”和“%Z”，默认值为“%Y%m%d%H%M”，表示“年份、月份、日期、小时和分钟”。例如自动备份的 URL 中输入的文件名为 backup.tgz，则备份文件名为

backup_202401010000.tgz

backup_time

可选。该参数指定自动备份的时间。取值格式遵循标准的 Crontab 表达式格式，即 “minute hour date month week”，各个。其中时间信息项的取值如下：

- minute: 表示分钟，取值范围为 0 到 59。
- hour: 表示小时，取值范围为 0 到 23。
- date: 表示日期，取值范围为 1 到 31。
- month: 表示月份，取值范围为 1 到 12。
- week: 表示星期，可以为两种取值：
 - 0 到 7。0 和 7 到表示星期日。
 - MON、TUE、WED、THU、FRI、SAT 和 SUN。不区分大小写。

各个时间信息项通过空格分隔。上述时间信息项还支持配置为：

- “*”：表示通配符。表示该字段所有可能值。例如 “*” 在分钟字段中表示 “每分钟”。
- “,”：表示逗号，用来指定多个离散值。例如 “1, 15” 表示 “1” 和 “15”。
- “-”：表示连字符，用来指定一个值的范围。例如 “1-15” 表示从 “1” 到 “15”。
- “/n”：表示每隔 n 个单位执行一次。例如 “*/15” 在分钟字段，表示每隔 15 分钟执行一次。

默认值为 “0 2 * * *”，表示每天 2:00 备份一次。

no write regular cliilog <backup_index>

该命令用于删除指定的 CLI 日志自动备份的配置。

show write regular cliilog

该命令用于显示所有 CLI 日志自动备份的配置。

clear write regular cliilog

该命令用于清除所有 CLI 日志自动备份的配置。

write regular fastlog<backup_index> <url> [timestamp] [backup_time]

该命令用于定期自动将设备上的所有 Fastlog 备份至一台远程主机。

backup_index	该参数指定自动备份的索引。取值为 1 到 15 之间的整数。
url	该参数指定远程主机上存储 Fastlog 文件的 SCP URL、SFTP URL、TFTP URL、FTP URL 或 HTTP URL 路径。取值支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。必须置于双引号内。取值格式为： <pre><protocol>://[username]:[password]@<ip>:[port]/[path]/<filename.tgz></pre> 取值文件后缀名必须以.tgz 结尾。 例如： <pre>ftp://admin:admin@192.168.1.100:21/home/fastlog.tgz</pre> 注意：IPv6 地址需要置于中括号内，TFTP 协议不支持 IPv6。
timestamp	可选。该参数指定自动备份的文件名后缀的时间戳（日期和时间）的格式。具体格式遵循标准 strftime，支持的格式包括“%a”、“%A”、“%b”、“%B”、“%c”、“%C”、“%d”、“%D”、“%e”、“%F”、“%g”、“%G”、“%h”、“%H”、“%I”、“%j”、“%k”、“%l”、“%m”、“%M”、“%N”、“%p”、“%P”、“%r”、“%R”、“%s”、“%S”、“%t”、“%T”、“%u”、“%U”、“%V”、“%w”、“%W”、“%x”、“%X”、“%y”、“%Y”、“%z”和“%Z”，默认值为“%Y%m%d%H%M”，表示“年份、月份、日期、小时和分钟”。例如自动备份的 URL 中输入的文件名为 backup.tgz，则备份文件名为 <pre>backup_202401010000.tgz</pre>
backup_time	可选。该参数指定自动备份的时间。取值格式遵循标准的 Crontab 表达式格式，即“minute hour date month week”，各个。其中时间信息项的取值如下： • minute: 表示分钟，取值范围为 0 到 59。 • hour: 表示小时，取值范围为 0 到 23。 • date: 表示日期，取值范围为 1 到 31。 • month: 表示月份，取值范围为 1 到 12。 • week: 表示星期，可以为两种取值： - 0 到 7。0 和 7 到表示星期日。

- MON、TUE、WED、THU、FRI、SAT 和 SUN。
不区分大小写。

各个时间信息项通过空格分隔。上述时间信息项还支持配置为：

- “*”：表示通配符。表示该字段所有可能值。例如“*”在分钟字段中表示“每分钟”。
- “,”：表示逗号，用来指定多个离散值。例如“1,15”表示“1”和“15”。
- “-”：表示连字符，用来指定一个值的范围。例如“1-15”表示从“1”到“15”。
- “/n”：表示每隔 n 个单位执行一次。例如“*/15”在分钟字段，表示每隔 15 分钟执行一次。

默认值为“0 2 * * *”，表示每天 2:00 备份一次。

no write regular fastlog <backup_index>

该命令用于删除指定的 Fastlog 自动备份的配置。

show write regular fastlog

该命令用于显示所有 Fastlog 自动备份的配置。

clear write regular fastlog

该命令用于清除所有 Fastlog 自动备份的配置。

write regular dnslog <backup_index> <url> [timestamp] [backup_time]

该命令用于定期自动将设备上的所有 DNS 日志备份至一台远程主机。

backup_index 该参数指定自动备份的索引。取值为 1 到 15 之间的整数。

url 该参数指定远程主机上存储 DNS 日志文件的 SCP URL、SFTP URL、TFTP URL、FTP URL 或 HTTP URL 路径。取值支持大小写字母、数字以及特殊字符“@”、“-”、“_”、“.”、“/”和“!”，不允许配置特殊字符“..”、“./”、“../”，且不能以“-”或“.”开头。必须置于双引号内。取值格式为：
<protocol>://[username]:[password]@<ip>:[port]/[path]/<filename.tgz>。取值文件后缀名必须以.tgz 结尾。

例如：

ftp://admin:admin@192.168.1.100:21/home/dnslog.tgz

注意：IPv6 地址需要置于中括号内，TFTP 协议不支持 IPv6。

timestamp

可选。该参数指定自动备份的文件名后缀的时间戳（日期和时间）的格式。具体格式遵循标准 `strftime`，支持的格式包括“%a”、“%A”、“%b”、“%B”、“%c”、“%C”、“%d”、“%D”、“%e”、“%F”、“%g”、“%G”、“%h”、“%H”、“%I”、“%j”、“%k”、“%l”、“%m”、“%M”、“%N”、“%p”、“%P”、“%r”、“%R”、“%s”、“%S”、“%t”、“%T”、“%u”、“%U”、“%V”、“%w”、“%W”、“%x”、“%X”、“%y”、“%Y”、“%z”和“%Z”，默认值为“%Y%m%d%H%M”，表示“年份、月份、日期、小时和分钟”。例如自动备份的 URL 中输入的文件名为 `backup.tgz`，则备份文件名为 `backup_202401010000.tgz`

backup_time

可选。该参数指定自动备份的时间。取值格式遵循标准的 `Crontab` 表达式格式，即“minute hour date month week”，各个。其中时间信息项的取值如下：

- minute: 表示分钟，取值范围为 0 到 59。
- hour: 表示小时，取值范围为 0 到 23。
- date: 表示日期，取值范围为 1 到 31。
- month: 表示月份，取值范围为 1 到 12。
- week: 表示星期，可以为两种取值：
 - 0 到 7。0 和 7 到表示星期日。
 - MON、TUE、WED、THU、FRI、SAT 和 SUN。不区分大小写。

各个时间信息项通过空格分隔。上述时间信息项还支持配置为：

- “*”：表示通配符。表示该字段所有可能值。例如“*”在分钟字段中表示“每分钟”。
- “,”：表示逗号，用来指定多个离散值。例如“1, 15”表示“1”和“15”。
- “-”：表示连字符，用来指定一个值的范围。例如“1-15”表示从“1”到“15”。
- “/n”：表示每隔 n 个单位执行一次。例如“*/15”

在分钟字段，表示每隔 15 分钟执行一次。

默认值为“0 2 * * *”，表示每天 2:00 备份一次。

no write regular dnslog <backup_index>

该命令用于删除指定的 DNS 日志自动备份的配置。

show write regular dnslog

该命令用于显示所有 DNS 日志自动备份的配置。

clear write regular dnslog

该命令用于清除所有 DNS 日志自动备份的配置。

18.3 USB 存储访问

system usbaccess {on|off}

该命令用于设置是否允许系统访问 USB 存储。默认设置为禁止系统访问 USB 存储。

show system usbaccess

该命令用于显示“**system usbaccess**”命令的配置。

ssh regenerate keys

这个命令将重新产生系统的 SSH 服务器的主机密钥。执行该命令后，SSH 服务器将启用新的主机密钥。SSH 客户端必须更新它的公钥才能和 SSH 服务器正常通信。

pager <lines>

该命令用于对终端仿真程序启用分页功能，并设置每次命令输出显示的行数。

lines 该参数指定每次命令输出显示的行数，取值必须为 0 至 255 之间的整数，取值 0 表示采用当前窗口的分页功能设置。

no pager

该命令用于对终端仿真程序禁用分页功能。当禁用分页功能时，系统会一次性显示一条命令的所有输出信息。



注意：当分页功能禁用时，不建议通过 Console 连接执行“**show tech**”、“**show log**”等输出量大的命令。由于 Console 端口的传输速度较慢，系统可能出现卡顿或业务异常。

show pager

该命令用于显示对终端仿真程序的分页功能配置。

18.4 基于角色的权限管理

role name <role_name>

该命令用于创建一个自定义角色。系统允许配置最多 32 个自定义角色。

role_name 该参数指定角色名称。取值区分大小写，最大长度为 20 个字符，且不能为三权分立功能的角色名称，即“role_administrator”、“role_operator”和“role_auditor”。

no role name <role_name>

该命令用于删除指定的自定义角色。

如果启用三权分立功能，该命令不会删除三个三权分立角色。如果禁用三权分立功能，该命令会删除三个三权分立角色。



注意：在删除指定角色之前，请确保该角色没有分配给任何管理员。

show role name [role_name]

该命令用于显示为指定角色配置的“Permit”和“Deny”规则。如果不指定参数“role_name”，系统将显示所有自定义角色。

启用了三权分立功能后，如果不指定参数“role_name”，系统还将显示自动创建的三权分立角色。

clear role name

该命令用于清除所有自定义的角色。执行该命令后，系统将解除所有自定义角色与用户的关联关系，并清除所有自定义角色。

如果启用三权分立功能，该命令不会清除三个三权分立角色及其和管理员账户的绑定关系。如果禁用三权分立功能，该命令会清除三个三权分立角色及其和账户的绑定关系。

执行该命令后，所有的管理员没有绑定任何角色，则具有执行对应管理员账户所允许的所有 CLI 命令。

role permit <role_name> <filter_string>

该命令用于为指定角色自定义一条“Permit”规则。系统允许为每个角色自定义最多 256 个“Permit”规则。

role_name	该参数指定角色名称，取值必须为自定义角色。取值必须为长度不大于 20 个字节的字符串，支持字母、数字和特殊字符。当参数只包含数字或包含特殊字符时，必须置于双引号内。
filter_string	该参数指定“Permit”规则。取值必须为长度不大于 64 个字节的字符串。“Permit”规则必须为标准格式的 CLI 命令或者其前缀。 当具有指定角色的管理员执行该 CLI 命令时，系统会从首字母开始将管理员输入的 CLI 命令的标准格式与“Permit”过滤字符进行匹配。 - 如果未匹配上“Permit”规则，该角色将被禁止执行这条 CLI 命令。 - 如果匹配上“Permit”规则，将根据与“Deny”规则（通过命令“role deny”配置）的匹配情况进行进一步判断是否允许该角色执行这条 CLI 命令。



注意：

- 如果没有为某个角色配置任何“Permit”规则，那么该角色默认情况下禁止执行所有的 CLI 命令。
- 系统不支持通过该命令为预定义的三权分立管理员角色自定义“Permit”规则。

no role permit <role_name> <filter_string>

该命令用于删除为指定角色自定义的“Permit”规则配置。

show role permit [role_name] [filter_string]

该命令用于显示指定角色的特定“Permit”规则配置。

role_name	可选，该参数指定角色的名称，可以是自定义角色、三权分立功能预定义角色或系统预定义角色。 如果指定该参数，系统将显示指定角色的所有“Permit”规则配置。 如果未指定该参数，系统将显示所有角色的所有“Permit”规则配置。
filter_string	可选，该参数指定“Permit”规则。只有当指定了参数“role_name”时，该参数才可用。 如果指定该参数，系统将显示指定角色的特定“Permit”

规则配置。

如果未指定该参数，系统将显示该角色的所有“Permit”规则配置。

clear role permit [role_name]

该命令用于清除指定角色的所有自定义的“Permit”规则配置。如果不指定参数“role_name”，则删除所有自定义的“Permit”规则配置。

role deny <role_name> <filter_string>

该命令用于为指定的角色自定义一条“Deny”规则规则。系统允许为每个角色配置最多 256 个“Deny”规则。

role_name 该参数指定角色名称，取值必须为自定义角色。取值必须为长度不大于 20 个字节的字符串，支持字母、数字和特殊字符。当参数取值为数字或包含特殊字符时，必须置于双引号内。

filter_string 该参数指定“Deny”规则。取值必须为长度不大于 64 个字节的字符串。“Deny”规则必须为标准格式的 CLI 命令或者其前缀。

当具有指定角色的管理员执行该 CLI 命令时且如果该 CLI 命令已匹配上了“Permit”规则，系统会从首字母开始将管理员输入的 CLI 命令的标准格式与“Deny”过滤字符进行匹配。

- 如果匹配上“Deny”规则，该角色将被禁止执行这条 CLI 命令。
- 如果未匹配上“Deny”规则，该角色将被允许执行这条 CLI 命令。



注意：如果没有为某个角色配置任何“Permit”规则，那么该角色默认情况下禁止执行所有的 CLI 命令。

no role deny <role_name> <filter_string>

该命令用于删除为指定角色自定义的“Deny”规则配置。

show role deny [role_name] [filter_string]

该命令用于显示指定角色的特定“Deny”规则配置。

role_name 可选，该参数指定角色的名称，可以是自定义角色、三权分立功能预定义角色或系统预定义角色。

如果指定该参数，系统将显示指定角色的所有“Deny”规则配置。

如果未指定该参数，系统将显示所有自定义的“Deny”规则及角色名称。

filter_string

可选，该参数指定“Deny”规则。只有当指定了参数“role_name”时，该参数才可用。

如果指定该参数，系统将显示指定角色的特定“Deny”规则配置。

如果未指定该参数，系统将显示该角色的所有“Deny”规则配置。

clear role deny [role_name]

该命令用于删除指定角色的所有自定义“Deny”规则配置。如果不指定参数“role_name”，则删除所有自定义的“Deny”规则配置。

role clone <old_role_name> <new_role_name>

该命令用于为已有的自定义角色克隆一个新角色。已有角色的“Deny”和“Permit”规则配置将复制到新角色中。

old_role_name 指定已有的自定义角色的名称。

new_role_name 指定新角色的名称。

role test cli <role_name> <cli_command>

该命令用于测试指定的角色是否具有执行特定 CLI 命令的权限。

role_name 指定角色的名称。

cli_command 指定一条 CLI 命令。该参数取值必须为标准格式的 CLI 命令或标准格式 CLI 命令的前缀，并且必须置于双引号中。

show role predefined

该命令用于显示系统预定义角色、三权分立功能角色及其“Deny”和“Permit”规则。默认情况下，系统预定义了“SLB”和“NETWORK”两个角色。三权分立功能预定义了“role_administrator”、“role_operator”和“role_auditor”三个角色。

例如：

```
Demo(config)#show role predefined
role name "SLB"
```

```
role permit "SLB" "cache"
role permit "SLB" "filter"
role permit "SLB" "health"
role permit "SLB" "http"
role permit "SLB" "sip"
role permit "SLB" "slb"
...

role name "NETWORK"
role permit "NETWORK" "bond"
role permit "NETWORK" "dns"
role permit "NETWORK" "fwd"
role permit "NETWORK" "hostname"
role permit "NETWORK" "interface"
role permit "NETWORK" "ip"
role permit "NETWORK" "ipregion"
role permit "NETWORK" "ipv6"
role permit "NETWORK" "mnet"
...

role name "role_administrator"
role permit "role_administrator" "aaa"
role permit "role_administrator" "accessgroup"
role permit "role_administrator" "accesslist"
role permit "role_administrator" "acl"
role permit "role_administrator" "activationserverRemote"
role permit "role_administrator" "admin"
...

role name "role_operator"
role permit "role_operator" "aaa"
role permit "role_operator" "accessgroup"
role permit "role_operator" "accesslist"
role permit "role_operator" "acl"
role permit "role_operator" "activationserverRemote"
role permit "role_operator" "admin"
...

role name "role_auditor"
role permit "role_auditor" "show"
role permit "role_auditor" "log"
role permit "role_auditor" "no log"
role permit "role_auditor" "clear log"
role permit "role_auditor" "passwd changing"
role permit "role_auditor" "passwd user"
```

...

role user <user_name> <role_name>

该命令用于关联指定用户与指定角色，使该用户具有特定角色中的 CLI 执行权限（由“**role deny**”和“**role permit**”命令设置）。系统允许为一个管理员分配最多 8 个角色。

user_name 该参数指定用户的名称。

role_name 该参数指定角色的名称。该参数的取值可以为自定义的角色名称或者系统预定义的角色名称。



注意：

- 如果没有为某个管理员分配任何角色，则该管理员具有执行该管理员用户所允许的所有 CLI 命令。
- 如果为某个管理员分配了多个角色，当任意一个角色允许执行一条 CLI 命令时，该管理员可以执行该命令；当所有的角色都禁止执行一条 CLI 命令时，该管理员不可以执行该命令。
- 在 WebUI 上，为某个管理员分配特定角色后，必须再为这个角色配置一条“Permit”过滤规则，允许该角色执行“**show...**”命令。否则，该管理员帐户在可能会遇到“500 internal error”报错。

no role user <user_name> <role_name>

该命令用于解除指定用户和指定角色的关联关系。如果删除的角色是用户的最后一个角色，执行该命令后，该用户将成为超级用户，具有执行所有 CLI 命令的权限。

如果启用三权分立功能，该命令不会解除三权分立管理员用户和三权分立角色的关联关系。如果禁用三权分立功能，该命令将解除三权分立管理员用户和三权分立角色的关联关系。

show role user [user_name] [role_name]

该命令用于显示指定用户和指定角色的关联关系

user_name 可选，该参数指定用户的名称。

如果未指定该参数，系统将显示为所有用户分配的所有角色。

role_name 可选，该参数指定角色的名称。只有当指定了参数“**user_name**”，该参数才可用。

如果未指定该参数，系统将显示为指定用户分配的所有角色。

clear role user [user_name]

该命令用于清除指定用户和所有角色的关联关系。如果不指定参数“user_name”，系统将清除所有自定义用户和所有角色的关联关系。

如果启用三权分立功能，该命令不会清除三权分立管理员用户和三权分立角色的关联关系。如果禁用三权分立功能，该命令将清除三权分立管理员用户和三权分立角色的关联关系。

user_name 可选，该参数指定用户的名称。

如果未指定该参数，系统将删除为所有用户分配的所有角色。此时，所有的管理员具有执行对应管理员用户所允许的所有 CLI 命令。

18.5 三权分立功能

admin mode separation on

该命令用于启用三权分立功能。启用该功能后，系统将自动创建三个 Config 级别的三权分立管理员用户：管理员（Administrator）、操作员（Operator）和审计员（Auditor）。同时系统会预定义三个三权分立管理员角色（role_administrator、role_operator、role_auditor），并自动将三个管理员用户分别与三个对应角色关联。启用该功能后，已经存在的 Config 级别用户将成为超级用户，可执行 Config 级别的所有命令行，可修改所有用户的密码；新创建的用户只有关联角色后才可以执行命令行。该功能默认设置为禁用。

三个管理员用户权限如下：

- 管理员：有权限修改（除其他管理员用户外）所有用户的密码，且具有除日志操作以外的所有命令的执行权限。
- 操作员：只能修改自己的账户密码。具有除日志、角色、用户和密码卡管理员操作以外的所有命令的执行权限。
- 审计员：只能修改自己的账户密码。具有“show”相关命令、启用或禁用日志功能、显示日志配置、清除日志缓存的执行权限。

关于三个管理员用户操作权限的更多详细信息，请通过命令“**show role name**”、“**show role permit**”和“**show role deny**”查看。



注意：

- 启用三权分立功能后，请通过“**write memory**”命令保存配置，否则重启后三权分立功能将自动关闭，三权分立功能开启时创建的用户将被自动删除。
- 如果启用三权分立功能时，三个三权分立管理员用户已经存在，则密码将被恢复

为默认密码“admin”。

- 如果启用三权分立功能前系统支持创建的管理员用户数量不足三个，三权分立功能将无法启用。

admin mode separation off

该命令用于禁用三权分立功能。禁用该功能后，在该功能启用时创建的用户都将无法通过 SSH 和 WebUI 方式登录设备。禁用该功能后，如果系统中没有初始登录用户（admin），系统将自动添加初始登录用户；如果存在初始登录用户，其密码将被重置为“admin”。



注意：禁用三权分立功能后，在该功能启用时创建的用户通过 API 方式仍然可以登录，AAA 外部用户仍然可以登录。

show admin mode separation

该命令用于显示三权分立功能的开启状态。

18.6 WebUI 双因素认证登录

webui twofactor on <username>

该命令用于为指定系统管理员启用 WebUI 双因素认证功能。启用该功能后，指定的管理员需要通过双因素认证才能登录设备 WebUI。该功能默认设置为禁用。

username 该参数指定需要启用 WebUI 双因素认证的系统管理员的用户名。

webui twofactor off <username>

该命令用于为指定系统管理员禁用 WebUI 双因素认证功能。

show webui twofactor user [username]

该命令用于显示指定系统管理员的 WebUI 双因素认证功能配置。如果不指定参数“username”，系统将显示所有系统管理员的 WebUI 双因素认证功能配置。

18.7 配置同步命令

设备配置同步功能允许管理员在同一网络的多个设备之间传递配置信息。

18.7.1 配置同步

synconfig secure {on|off}

该命令用于启用或禁用配置同步的安全模式。使用该命令时，请确保本地节点和对端节点上配置同步的安全模式同时启用或者禁用。配置同步的安全模式默认设置为启用。

如果启用配置同步的安全模式，在本地设备上执行“**synconfig from**”或“**synconfig to**”命令前，管理员需要：

- 使用命令“**synconfig challenge**”在本地节点和对端节点上配置相同的 Challenge Code。
- 使用命令“**synconfig peer**”在本地节点和对端节点上配置同步节点。

如果禁用配置同步的安全模式，在本地设备上执行“**synconfig from**”或“**synconfig to**”命令前，管理员需要：

- 使用命令“**synconfig challenge**”在本地节点和对端节点上配置相同的 Challenge Code。
- 使用命令“**synconfig peer**”在本地节点上配置同步节点。



注意：为安全起见，强烈建议管理员保持配置同步安全模式启用。

show synconfig secure

该命令用于显示配置同步的安全模式的状态。当命令输出为“**synconfig secure off**”时表示配置同步的安全模式为禁用状态，空时表示启用状态。

synconfig challenge <code>

该命令用于设置配置同步使用的 Challenge Code。执行配置同步时，本地节点和对端节点上必须配置相同的 Challenge Code；否则配置同步节点不能通信，配置同步将失败。所有设备上都有相同的默认 Challenge Code。为了安全起见，强烈建议管理员设置新的 Challenge Code。

code 指定配置同步使用的 Challenge Code。该参数的取值为 1 到 31 个字符，区分大小写。如果 Challenge Code 以数字开头，必须将该 Challenge Code 置于双引号内。

show synconfig challenge

该命令用于显示当前配置的 Challenge Code。



注意：系统将以加密的形式显示 Challenge Code。管理员需要妥善记录配置的 Challenge Code。

no synconfig challenge

该命令用于删除当前配置的 Challenge Code。

clear synconfig challenge

该命令用于清除当前配置的 Challenge Code。

synconfig peer <peer_name> <peer_ip>

该命令用于定义一个配置同步节点。系统支持定义最多 128 个配置同步节点。

peer_name 该参数指定同步节点的名称。取值长度不大于 63 个字节，不必是 DNS 名称。取值含有特殊字符时应置于双引号内。

peer_ip 该参数指定同步节点的 IPv4 或 IPv6 地址(与接口无关)。

注意：该参数取值不能使用分区模式下配置的 IP 地址，例如：系统接口 IP 地址、VLAN 接口 IP 地址等等。

show synconfig peer

该命令用于显示当前所有同步节点的信息。

no synconfig peer <peer_name>

该命令用于删除指定的节点。

peer_name 指定同步节点的名称。应置于双引号内，不必是 DNS 名称。

clear synconfig peer

该命令用于清除所有的同步节点设置。

synconfig to <peer_name>

该命令用于将本地节点配置同步到对端节点。执行该命令后，对端节点将会收到本地节点的运行配置信息。配置同步结束后，刚刚同步的运行配置将作为对端节点的当前配置。

在分区下执行该命令时，需要在本地节点和对端节点创建名称相同的分区和分区管理员账户，且该分区管理员账户在本地节点和对端节点均具有“Config”权限等级。

peer_name 该参数指定对端节点的名称。如果该参数的取值为“all”，则通过命令“**synconfig peer**”定义的所有节点都将被同步。



注意：

- 在分区下执行该命令同步分区配置时，本地节点和对端节点必须配置相同的分

区名称。此外，执行该命令不能同步分区名称信息。

- 该命令不会同步 “**show config consistency**” 配置。

synconfig from <peer_name> [segment_name]

该命令用于从指定的节点同步所有配置信息。该命令只同步指定节点上已保存的配置，而不是正在运行的配置。节点名称必须为一个已经通过命令“**synconfig peer**”配置的节点。

与“**synconfig to**”命令不同，通过“**synconfig from**”命令同步的配置信息不会被自动写入硬盘，需要执行“**write memory**”命令来将运行配置保存到硬盘中。执行“**synconfig to**”和“**synconfig from**”前，系统会检查软件版本的一致性，只要版本号的前两位相同，即认为版本号一致。

在分区执行该命令时，需要在本地节点和对端节点创建名称相同的分区。

peer_name	该参数指定已存在的同步节点的名称。
segment_name	可选。该参数指定已存在的分区名称。如不指定该参数，该命令会从指定的节点同步所有配置。 默认值为空。



注意：

- 在分区下执行该命令同步分区配置时，本地节点和对端节点必须配置相同的分区名称。此外，执行该命令不能同步分区名称信息。
- 该命令不会同步 “**show config consistency**” 配置。

synconfig increment {enable|disable}

该命令用于启用或禁用增量同步功能。默认设置为禁用。管理员启用该功能后，系统将记录随后的所有配置，直到管理员禁用该功能为止。管理员禁用该功能后，系统将记录的配置根据系统白名单列表进行过滤，形成一个新的列表，再对该列表根据系统黑名单列表进行过滤，从而得到增量同步列表。

之后管理员可以通过执行“**synconfig increment to**”命令将增量同步列表中的配置同步到指定或全部对端节点。

系统白名单列表如下：

```
ssl
no ssl
slb
no slb
http
no http
health
no health
```

```
cache
no cache
diameter
no diameter
epolicy
no epolicy
ftp
no ftp
http2
filter
no filter
acl
no acl
system mode
ha group
no ha group
ip pool
no ip pool
sdns
no sdns
sdns pool method primary
sdns pool method secondary
sdns pool member weight
sdns log query custom
```

系统黑名单列表如下：

```
show config consistency
ssl restore
no ssl sni crlca
no ssl sni interca
ssl activate
sdns config
no sdns config
sdns dps write proximity
```



注意：

- 增量同步功能与 HA 运行时配置同步功能不能同时启用；
- 增量同步功能与 SDNS 运行时配置同步功能不能同时启用。

synconfig increment to <peer_name>

该命令用于将增量配置同步指定的对端节点。执行该操作前，请先通过命令“**synconfig increment disable**”禁用增量同步功能。

peer_name 该参数用于指定同步节点的名称。如果参数“peer_name”的取值为“all”，则增量配置将被同步到所有对端节点。

show synconfig increment config

该命令用于显示增量配置功能的启用状态和用于增量同步的配置信息。

18.7.2 同步回退



注意：在部署了分区功能的应用场景，如果需要通过“**synconfig rollback**”命令恢复分区配置，需先执行“**write segment memory**”命令保存分区配置，否则配置恢复会失败。

synconfig rollback local <peer_name>

该命令用于回退本地节点的配置同步操作。在本地节点执行“**synconfig from**”或在对端节点执行“**synconfig to**”命令后，可以在本地节点上执行该命令将本地节点的配置恢复为同步之前的配置。

peer_name 该参数指定对端节点的名称。

synconfig rollback peer <peer_name>

该命令用于回退对端节点的配置同步操作。在本地节点执行“**synconfig to**”或在对端节点执行“**synconfig from**”命令后，可以在本地节点执行该命令将对端节点的配置恢复为同步之前的配置。

peer_name 该参数指定对端节点的名称，取值为“all”时，所有对端节点的配置将恢复为同步之前的配置。



注意：在分区模式下执行该命令时，管理员需要为本地节点和对端节点配置相同的分区用户名，否则对端节点的配置将回退失败。

18.7.3 其他命令

show synconfig status from [peer_ip]

该命令用于查看本地节点与指定对端节点的同步情况，包括同步时间、远程 IP 和状态信息。

peer_ip 指定对端节点的 IP 地址，可以为 IPv4 或 IPv6 地址。如果未指定“peer_ip”参数，则显示本地节点与所有进行同步的对端节点的同步指令清单。

show synconfig status history

这个命令将显示最近 50 次在本地执行的同步事件，包括命令运行时间、节点信息和命令。如果命令执行失败，将在命令下一行显示错误信息。

clear synconfig status

该命令用于删除所有同步日志。

show synconfig diff <name>

该命令用于显示本地节点的运行配置和指定的同步节点上的正在运行的配置（包括本地节点与指定同步节点的所有分区上正在运行的配置）的差异。对于不支持显示配置差异的命令，系统通过一个黑名单管理。下表列出了黑名单里的所有配置项：

表18 - 1 配置差异黑名单

ip address
ip route
ip dhcp
ssh ip
ssh auth
bond
hostname
mnet
vlan
webui ip
webui twofactor
restapi ip
xmlrpc ip
ip redundant
cluster virtual priority
sdns dps localdetector
interface name
interface speed
interface mac
interface management
interface shutdown
ha ssf peer
user
sdns listener

18.8 SDNS 配置同步命令

设备配置同步功能允许管理员在多个设备之间传递除 SDNS 成员和 SDNS 监听 IP 地址配置信息之外的所有 SDNS 配置信息以及 BIND 9 域文件。

synconfig sdns to <peer_name>

该命令用于同步 SDNS 配置和 BIND 9 域文件到指定远端节点。

peer_name 指定同步 SDNS 配置和 BIND 9 域文件到的远端节点的名称。节点名称必须已经使用 “**synconfig peer <peer_name> <peer_ip>**” 配置。如果参数 “peer_name” 的取值为 “all”，则 SDNS 配置和 BIND 9 域文件将被同步到所有通过 “**synconfig peer**” 命令定义的远端节点。”



注意：在执行 “**synconfig sdns to**” 命令前，您需要使用 “**synconfig peer**” 命令在每台设备上配置全部的同步节点，并使用 “**synconfig challenge**” 命令配置相同的 Challenge Code。

18.9 SNMP 命令

SNMP（简单网络管理协议）是一个被广泛使用的网络监控和控制协议。数据从 SNMP 代理发出，网络中的每个设备（集线器、路由器等）由硬件/软件报告他们的活动状态给工作站的终端。代理返回的信息中包含一个 MIB（基本管理信息）信息，该信息是用来获取和控制设备信息的数据结构。系统当前支持 SNMP GET 和 SET 请求。目前，SNMP SET 请求仅支持设置 APV 设备的主机名和系统的当前时间。

snmp on [default|v3]

该命令用于启用 SNMP 功能，并设定 SNMP 代理所支持的 SNMP 版本。该功能默认为禁用。

default|v3 可选，该参数用于设置 SNMP 代理支持的 SNMP 版本，取值必须为：

- **default:** 表示系统支持 v1, v2c, v3 版本。
- **v3:** 只支持 v3 版本。

当不配置该参数时，默认为 default。

snmp off

该命令用于禁用 SNMP 功能。



注意：系统支持通过 SNMP v2c, v3 版本查看统计信息，不支持通过 SNMP v1 版本查看统计信息。

show snmp

该命令用于显示所有和 SNMP 配置相关的信息。

```
Demo(config)#show snmp
snmp off
snmp community "public"
snmp contact ""
snmp location ""
no snmp enable traps
snmp traps loglevel err
snmp ipcontrol off
```

clear snmp

该命令用于将所有 SNMP 设置恢复为默认值。

slb snmp oid virtual <virtual_service> <index>

该命令用于为指定的虚拟服务配置一个静态 SNMP OID。虚拟服务的静态 SNMP OID 由系统已定义的 SNMP OID 前缀和在该命令的“index”参数中配置的 SNMP OID 索引号组成。例如，虚拟服务的 SNMP OID 前缀是

“.1.3.6.1.4.1.7564.19.1.2.2.1.2”，SNMP OID 索引号是“5000”，则完整的 SNMP OID 为“.1.3.6.1.4.1.7564.19.1.2.2.1.2.5000”。静态 SNMP OID 配置完成后将不会改变。

静态 SNMP OID 的优先级高于自动生成的动态 SNMP OID。如果为虚拟服务配置了静态 SNMP OID，系统将优先使用静态 SNMP OID。如果没有配置静态 SNMP OID，系统将使用动态 SNMP OID。动态 SNMP OID 可能会在使用中发生变化。

virtual_service 该参数指定一个已存在的虚拟服务名称。

index 该参数指定 SNMP OID 的索引号，即 SNMP OID 中的最后一个数字。对于系统内存为 32 GB 以下的设备，该参数取值必须为 4001 到 8000 之间的整数；对于系统内存为 32 GB 或以上的设备，取值必须为 8001 到 16000 之间的整数。

no slb snmp oid virtual <virtual_service>

该命令用于删除指定虚拟服务的静态 SNMP OID。当静态 SNMP OID 删除后，系统将使用动态 SNMP OID。

show slb snmp oid virtual [virtual_service]

该命令用于显示指定虚拟服务的静态 SNMP OID。如果没有配置“virtual_service”参数，将显示所有虚拟服务的静态 SNMP OID。

clear slb snmp oid virtual

该命令用于清除所有虚拟服务的静态 SNMP OID。当静态 SNMP OID 删除后，系统将使用动态 SNMP OID。

slb snmp oid real <real_service> <index>

该命令用于为指定的后台服务配置一个静态 SNMP OID。后台服务的静态 SNMP OID 由系统已定义的 SNMP OID 前缀和在该命令的“index”参数中配置的 SNMP OID 索引号组成。例如，后台服务的 SNMP OID 前缀是

“.1.3.6.1.4.1.7564.19.2.1.1.1.2”，SNMP OID 索引号是“4000”，则完整的 SNMP OID 为 “.1.3.6.1.4.1.7564.19.2.1.1.1.2.4000”。静态 SNMP OID 配置完成后将不会改变。

静态 SNMP OID 的优先级高于自动生成的动态 SNMP OID。如果为后台服务配置了静态 SNMP OID，系统将优先使用静态 SNMP OID。如果没有配置静态 SNMP OID，系统将使用动态 SNMP OID。动态 SNMP OID 可能会在使用中发生变化。

real_service	该参数指定一个已存在的后台服务名称。
index	该参数指定 SNMP OID 的索引号，即 SNMP OID 中的最后一个数字。对于系统内存为 32 GB 以下的设备，该参数取值必须为 4001 到 8000 之间的整数；对于系统内存为 32 GB 或以上的设备，取值必须为 8001 到 16000 之间的整数。

no slb snmp oid real <real_service>

该命令用于删除指定后台服务的静态 SNMP OID。当静态 SNMP OID 删除后，系统将使用动态 SNMP OID。

show slb snmp oid real [real_service]

该命令用于显示指定后台服务的静态 SNMP OID。如果没有配置“virtual_service”参数，将显示所有后台服务的静态 SNMP OID。

clear slb snmp oid real

该命令用于清除所有后台服务的静态 SNMP OID。当静态 SNMP OID 删除后，系统将使用动态 SNMP OID。

snmp community <string>

该命令用于定义 SNMP community 字符串，该字符串作为一个口令用来限制 NMS（Network Management System，网络管理系统）对 SNMP 代理的访问。

当不配置该命令时，默认的 SNMP community 字符串为 public。

只有 SNMP 代理处于禁用状态时才可以修改该字符串。

string 该参数指定 SNMP community 字符串，取值必须为 1 至 32 个字符。



注意：为安全起见，强烈建议您修改默认的 SNMP community 字符串，防止系统信息被非法窃取。

例如：

```
Demo(config)#snmp community reindeer
```

no snmp community

恢复公共串为默认值 public。

snmp contact <contact_name>

这个命令允许用户在系统环境允许的条件下建立个人的联系方式。参数“contact_name”是由 128 个字符组成，需要置于双引号内。

例如：

```
Demo(config)#snmp contact "admin@example.com"
```

no snmp contact

这个命令允许用户删除设定的联系信息。

snmp location <location>

这个命令允许用户输入设备的物理位置。参数“location”可以由多达 128 个字符组成。

例如：

```
Demo(config)#snmp location "server room 6"
```

no snmp location

删除以前设置的设备位置信息。

**snmp host <host_ip> [version] [user_name|community_name] [engine_id]
[auth_password] [authorization_level] [priv_password] [port] [auth_proto]
[priv_proto]**

该命令用于设置一个接收 SNMP Trap 的主机以及与其相关的用户或者分组字符串。系统最多支持配置 10 个接收 SNMP Trap 的主机。

host_ip 该参数指定接收 SNMP Trap 的主机的 IP 地址，可以为 IPv4 或 IPv6 地址。

version	可选，该参数指定 SNMP trap 的版本。取值必须为 1、2 或者 3。默认为 1。
user_name community_name	可选，该参数指定 trap 分组字符串用于 SNMP v1 和 v2，而 trap 用户是用于 SNMP v3。默认为 public。
engine_id	可选，该参数指定远程 SNMPv3 Trap 接收者的 Engine ID。取值必须为采用 16 进制且小于 32 字符的字符串，且字符串取值长度必须为偶数。当参数取值为“default”时，系统使用默认的 Engine ID。该参数只有在参数“version”设置为 3 时才生效。
auth_password	可选，该参数指定验证密码，取值必须为长度 8 到 32 个字符的字符串。该参数只有在参数“version”设置为 3 时才生效。
authorization_level	可选，该参数指定安全授权等级。取值必须为： • authNopriv：不需要私人密码。 • authPriv：需要私人密码。 该参数只有在参数“version”设置为 3 时才生效。默认值为“authNopriv”。
priv_password	可选，该参数指定用于“authPriv”模式下数据加密的私人密码，取值必须为长度 8 到 32 个字符的字符串。该参数只有在参数“version”设置为 3 时才生效。
port	可选，该参数指定用于接收 Trap 消息的 SNMP 主机的端口号。取值必须为 0 到 65535 之间的整数。默认值为 162。
auth_proto	可选，该参数指定 SNMP v3 协议使用的鉴权算法。取值必须为 MD5 或 SHA1，不区分大小写。该参数只有在参数“version”设置为 3 时才生效。默认值为 MD5。
priv_proto	可选，该参数指定 SNMP v3 协议使用的加密算法。取值必须为 AES 或 DES，不区分大小写。该参数只有在参数“authorization_level”设置为“authPriv”且参数“version”设置为 3 时才生效。默认值为 DES。

no snmp host <host_ip>

这条命令删除一个 SNMP 主机。

snmp enable traps

该命令用于允许设备发送普通或企业级的 SNMP 陷阱。启用该功能后，设备会在以下触发条件发生时发送 SNMP 陷阱：

- 接口 Down 或 Up
- Error 及以上级别的系统日志生成(默认设置，日志级别可以通过“**snmp traps loglevel**”命令更改)
- License 在 15 天之内过期
- 系统启动
- 系统关机

no snmp enable traps

该命令用于禁用设备发送普通或企业级的 SNMP 陷阱的功能。

snmp traps loglevel [log_level]

该命令用于设置触发 SNMP 陷阱发送的系统日志级别。当系统产生大于或等于该级别的系统日志时，将触发设备发送 SNMP 陷阱。

当不配置该命令时，触发 SNMP 陷阱发送的默认系统日志级别为 err。

log_level	可选。该参数指定系统日志的级别，取值必须为 emerg、alert、crit、err、warning、notice、info 或 debug。 默认值为 err。

no snmp traps loglevel

该命令用于将触发 SNMP 陷阱发送的系统日志级别重置为 err。

snmp ipcontrol {on|off}

该命令用于启用或禁用基于客户端 IP 地址进行 SNMP 访问控制的功能，该功能基于 VACM（View-based Access Control Model，基于视图的访问控制模型）控制 SNMP GET 请求，对 SNMPv3 GET 请求不生效。该功能的默认设置为禁用。

snmp ippermit <source_ip> {mask|prefix}

该命令用于配置一个源网段，允许接收该网段的客户端的 SNMP GET 请求。该命令对 SNMPv3 GET 请求不生效。

source_ip	指定发送 SNMP GET 请求的主机的 IP 地址，可以为 IPv4 或 IPv6 地址。
netmask prefix	指定发送 SNMP GET 请求的主机的网络屏蔽或前缀长度。 • “mask”用于配置 IPv4 地址对应的子网掩码，可以

为点分地址格式或 0 到 32 之间的整数。

- “prefix” 用于配置 IPv6 地址对应的前缀长度，其值应是一个 0 到 128 之间的整数。

no snmp ippermit <source_ip> <netmask>

从指定的客户端列表中删除指定的源 NET。

snmp v3user <user_name> <auth_password> [authorization_level]
[priv_password] [auth_proto] [priv_proto]

该命令用于添加一个 SNMP v3 用户到 GET 请求身份验证数据库，用于根据 USM（User-based Security Model，基于用户的安全模型）来控制 SNMP GET 请求。系统支持最多添加 16 个 SNMP v3 用户。

user_name 该参数指定用户名。取值必须为长度不大于 32 个字节的字符串。支持字母、数字和特殊字符。取值包含特殊字符或由纯数字组成时，必须置于双引号内。

auth_password 该参数指定身份验证密码，取值必须为长度是 8 到 32 个字符的字符串。取值包含特殊字符或由纯数字组成时，必须置于双引号内。

authorization_level 该参数指定安全授权等级。取值必须为：

- authNopriv：不需要私人密码。
- authPriv：需要私人密码。

默认值为“authNopriv”。

priv_password “authPriv” 模式下用于加密的私人密码，长度不小于 8 个字符。取值包含特殊字符或由纯数字组成时，必须置于双引号内。

auth_proto 可选，该参数指定 SNMP v3 协议使用的鉴权算法。取值必须为 MD5 或 SHA1，不区分大小写。默认值为 MD5。

priv_proto 可选，该参数指定 SNMP v3 协议使用的加密算法。取值必须为 AES 或 DES，不区分大小写。该参数只有在参数“authorization_level”设置为“authPriv”时才生效。默认值为 DES。

no snmp v3user <user_name>

从 SNMP v3 的用户数据库中删除一个指定的用户。

18.10 故障检测命令

ping {ip address|hostname} [gateway_ip] [custom_parameter]

这个命令向指定的 IP 地址或主机发送 ICMP echo 请求网络连接测试包。

hostname	该参数指定主机名或主机 IP 地址。
gateway_ip	可选，该参数指定某一 LLB 链路的网关 IP 地址。该参数设置好后，ping 包可通过由该参数指定的 LLB 链路送至主机。
custom_parameter	可选，该参数指定 ping 包的自定义参数。参数取值必须为“-symbol value”这样的格式，并置于双引号内。其中“symbol”可以为“-s”（包的大小）、“-i”（间隔时间）和“-c”（包的数量）等值，“value”为具体的数值。例如，“-s 32, -i 10”表示 ping 包的大小为 32 字节，间隔时间为 10 秒。多个参数取值间用逗号隔开。默认值为空，表示不指定任何参数。参数取值的详细信息，请参见 ping 工具。

示例：

```
Demo(config)#ping 10.8.1.1 "-s 32, -i 10"
```

traceroute {ip|hostname} [gateway_ip]

该命令用来跟踪发送到指定 IPv4 地址或者主机的三个数据报的路由。执行该命令后，系统将输出数据包的 TTL、所经过节点（路由器或网关）的设备名称和 IPv4 地址，以及与每个节点之间往返时间。

ip hostname	指定主机名或主机 IPv4 地址。
gateway_ip	可选，该参数指定某一 LLB 链路的网关 IPv4 地址。该参数设置好后，数据包通过由该参数指定的 LLB 链路送至指定 IPv4 地址或者主机。

ping6 {ipv6 address|hostname} [gateway_ip]

该命令用于向指定的 IPv6 地址或主机发送 ICMP echo 请求网络连接测试包。当参数“hostname”采用以下格式：“IPv6_link-local_address % port number”（例如：Demo(config)# ping6 "fe80::225:90ff:fe39:9538%port3"）时，该参数可通过指定接口 ping 一个链路本地地址。

hostname	指定主机名或主机 IP 地址。该参数可采用以下形式： “IPv6_address % port”，例如： fe80::225:90ff:fe39:9538%port3。

gateway_ip 可选，该参数指定某一 LLB 链路的网关 IP 地址。该参数设置好后，ping 包可通过由该参数指定的 LLB 链路送至主机。

traceroute6 {ipv6|hostname} [gateway_ip]

该命令用来跟踪发送到指定 IPv6 地址或者主机的三个数据报的路由。执行该命令后，系统将输出数据包的 TTL、所经过节点（路由器或网关）的名称和 IPv6 地址，以及与每个节点之间往返时间。

ip|hostname 指定主机名或主机 IPv6 地址。该参数可采用以下形式：“IPv6_address % port”，例如：
fe80::225:90ff:fe39:9538%port3。

gateway_ip 可选，该参数指定某一 LLB 链路的网关 IPv6 地址。该参数设置好后，数据包通过由该参数指定的 LLB 链路送至指定 IPv6 地址或者主机。

nslookup {ip|hostname} [query_type]

该命令用于查看指定 IP 地址的主机名，或指定主机名对应的 IP 地址。

ip|hostname 指定 IP 地址或者主机名。

- 如果指定参数“ip”，该命令用于查看其对应的主机名。可以为 IPv4 或 IPv6 地址。
- 如果指定参数“hostname”，该命令用于查看其对应的 IP 地址。取值应是一个不超过 63 个字符的字符串。

query_type 指定用于 DNS 查询的资源记录类型。支持的资源记录类型包括 A、NS、MD、MF、CNAME、SOA、MB、MG、MR、NULL、WKS、PTR、HINFO、MINFO、MX、TXT、AAAA、ANY。

support <ip_address> <netmask|prefix>

该命令用于配置允许通过 SSH 或 Console 对设备进行访问和调测的网段。执行该命令后，系统会自动创建调试账号。

ip_address 该参数指定允许的 IP 地址，可以为 IPv4 或 IPv6 地址。

netmask|prefix 该参数指定 IP 地址对应的子网掩码或前缀长度。

- “netmask”用于配置 IPv4 地址对应的子网掩码，可以是点分地址格式或是一个 0 到 32 之间的整数。
- “prefix”用于配置 IPv6 地址对应的前缀长度，其

值应是一个 0 到 128 之间的整数。

no support <ip_address> <netmask|prefix>

该命令用于删除允许通过 SSH 或 Console 对设备进行访问和调测的指定网段。
执行该命令后，系统会删除调试账号。

show support

该命令用于显示允许通过 SSH 或 Console 对设备进行访问和调测的网段。

clear support

该命令用于清除所有允许通过 SSH 或 Console 对设备进行访问和调测的网段。

admin test factor <passwd_factor>

该命令用于设置调试账号的密码因子。

- 如果未执行“**support**”命令，直接执行该命令，则系统仅设置密码因子；
- 如果已执行“**support**”命令，再执行该命令，则系统根据设备序列号和密码因子更新调试账号的密码；
- 如果先执行该命令，再执行“**support**”命令，则系统根据设备序列号和密码因子设置调试账号的密码。

passwd_factor 该参数指定调试账号的密码因子，取值必须为 6 位数字，必须置于双引号内。

no admin test factor

该命令用于删除调试账号的密码因子。

- 如果未执行“**support**”命令，执行该命令后，系统仅删除调试账号的密码因子；
- 如果已执行“**support**”命令，执行该命令后，系统仅根据设备序列号更新调试账号的密码。

show admin test factor

该命令用于加密显示调试账号的密码因子。



注意：在日志中，调试账号密码因子将显示为“*****”形式。在运行配置、启动配置和配置备份文件中，调试账号密码因子将加密显示。

18.11 调试命令

debug enable

该命令用于开始准备收集调试资料。执行该命令之后，设备将首先清除原有的用于存放收集的调试数据的文件，然后在/var/crash/sys_debug 和/var/crash/sslkeylog 目录下生成新的文件来存放调试信息。

debug disable

该命令用于停止收集调试信息。执行该命令之后，设备将生成用于存放所收集的调试信息的.tar.gz 文件，例如 sys_debug.tar.gz、sys_snap.tar.gz、sys_log.tar.gz、sys_core.tar.gz、app_core.tar.gz、sslkeylog.tar.gz，并清除之前收集的调试信息。

如下所示为一个生成的 sys_debug.tar.gz 文件示例，其中只包含从上一次执行“**debug enable**”命令开始到本次执行“**debug disable**”命令结束的这个时间段内的调试信息：

```
/var/crash/sys_debug.tar.gz
tcpdump
ssldump
debug.tar.gz (包含 englog, pipe 和 loopback 信息)
```

debug corefile [core_files_number]

该命令用于设置用户需要获取的系统 corefile 文件的数量，范围为 0~10。默认值为 0，表示不获取任何 corefile 文件。

说明：管理员如果要执行“**debug snapshot system**”命令来获取系统 corefile 文件（sys_core.tar.gz 和 app_core.tar.gz）之前，必须首先执行此命令来设置要获取的文件的数量。如果没有设置该数量，系统默认不获取任何 corefile 文件。

show debug corefile

该命令用于显示“**debug corefile**”命令的配置。

debug log storage {on|off}

该命令用于启用或者禁用生成本地日志压缩文件的功能。启用该功能后，管理员可以执行命令“**debug snapshot system**”生成.tar.gz 格式的本地日志压缩文件。该功能默认设置为禁用。

show debug log storage

该命令用于显示生成本地日志压缩文件功能的配置。

show debug exception

该命令用于显示 SLB 功能的异常状态信息。异常状态信息按级别从低到高依次为 Notice、Warning 和 Emergency。

debug snapshot system

该命令用于为系统活动拍快照，并生成以下五个分别记录不同类型系统活动信息的文件：

- sys_snap.tar.gz
- sys_log.tar.gz
- sys_core.tar.gz
- app_core.tar.gz
- fastlog_backup.tar.gz

这些文件将为管理员进行系统调试提供了更加全面的系统运行信息。管理员可以根据需要获取包含所需信息的文件。



注意：命令“`show system ipmi <sel> <list>`”与命令“`show system ipmi <sdr> <list>`”显示的内容将保存在该命令生成的 sys_snap.tar.gz 压缩包的 system.xxx 文件中。

show debug file

该命令用于显示所有系统调试文件及系统快照文件，包括 sys_debug.tar.gz、sys_snap.tar.gz、sys_log.tar.gz、sys_core.tar.gz、app_core.tar.gz、sslkeylog.tar.gz 和 fastlog_backup.tar.gz。

例如：

Demo(config)#show debug file

File	Size	Time
fastlog_backup	1902455	Mar 31 07:40:36 2024
sys_snap.0	193912	Mar 31 07:33:58 2024
sys_log.1	439270339	Mar 30 02:45:26 2024
app_core	692156	Jan 20 06:54:02 2024
sys_snap.1	158200	Mar 30 02:44:54 2024
sys_snap	193949	Mar 31 07:40:12 2024
sys_log.0	603657442	Mar 31 07:35:04 2024
sys_log	603741684	Mar 31 07:40:36 2024

debug ftp <user_name> <remote_ftp_ip> [file_name]

该命令用于把存放调试数据的文件（例如 sys_snap.tar.gz、sys_log.tar.gz、sys_core.tar.gz、app_core.tar.gz、sys_debug.tar.gz、sslkeylog.tar.gz 或 fastlog_backup.tar.gz）发送到指定的远程 FTP 服务器上。每一个被发送的文件的名称中都会被自动插入一个时间戳，用于与远程 FTP 服务器上的其他存放调试数据的文件进行区分。

user_name 该参数指定远程 FTP 服务器的用户名。

remote_ftp_ip 该参数指定远程 FTP 服务器的 IP 地址，支持 IPv4 和 IPv6 地址，取值必须置于双引号内。

file_name 可选，该参数指定被发送到远程 FTP 服务器上的文件的名称，文件名不包含后缀“.tar.gz”。默认值为“all”，表示将所有最近获取的系统调试文件发送到 FTP 服务器上。

注意: FTP 类型 URL(ftp://user:password@host:port/path) 中的“path”需使用相对路径。



注意: 参数“file_name”取值为“all”时，只有通过命令“debug log storage on”启用本地日志打包文件获取功能后，发送到远程 FTP 服务器上的文件才包含“fastlog_backup.tar.gz”。

debug scp {username@remote_scp_ip|host} [file_name]

该命令用于把存放调试数据的文件(sys_snap.tar.gz、sys_log.tar.gz、sys_core.tar.gz、app_core.tar.gz、sys_debug.tar.gz、sslkeylog.tar.gz 或 fastlog_backup.tar.gz) 发送到指定的远程 SCP 服务器上。每一个被发送的文件的名称中都会被自动插入一个时间戳，用于与远程 SCP 服务器上的其他存放调试数据的文件进行区分。

username@remote_scp_ip|host 该参数指定远程 SCP 服务器的用户名和 IP 地址或主机名，取值必须置于双引号内，例如：“test@172.16.13.12”。

file_name 可选，该参数指定发送到远程 SCP 服务器上的文件的名称，文件名不包含后缀“.tar.gz”。默认值为“all”，表示将所有最近获取的系统调试文件发送到 SCP 服务器上。



注意: 参数“file_name”取值为“all”时，只有通过命令“debug log storage on”启用本地日志打包文件获取功能后，发送到远程 SCP 服务器上的文件才包含“fastlog_backup.tar.gz”。

debug monitor on [module name]

该命令用于启用调试监控功能。这个功能启用后，系统将会跟踪设备的状态，同时这些状态信息将会被记录到预先定义好的名为“monitor.out0”的文件中。如果不指定模块名称，将只启用系统的调试监控功能。如果指定模块名称，将启动系统和指定模块的调试监控功能，状态信息都将记录到预先定义好的名为“monitor.out0”的文件中。

module name 可选参数。指定模块名称。支持的模块包括 SSL, SLB, LLB, GSLB, UProxy (用户代理) 以及 ORCH (流量编排)，不区分大小写。支持配置多个模块，需为每个模块分别配置。

debug monitor off

该命令用于禁用系统和指定模块的调试监控功能。

no debug monitor <module name>

该命令用于删除指定模块的调试监控功能。



注意：运行该命令前需禁用系统和指定模块的调试监控功能。

debug monitor import ftp <user_name> <remote_ftp_ip> <remote_file_path>

允许使用者通过 FTP 方式远程导入一个使用者自定义的脚本。用户可以在脚本中定义能够显示自己想要收集的调试信息的 CLI 命令，然后通过这条命令导入到系统中，用户就可以收集到他想要的信息。执行该命令之前，请先禁用“**debug monitor**”。

user_name 指定导入自定义脚本文件所在远程 FTP 服务器的用户名。

remote_ftp_ip 指定导入自定义脚本文件所在远程 FTP 服务器的 IP 地址。

remote_file_path 指定导入自定义脚本文件在远程 FTP 服务器上的存储路径。

注意：FTP 类型 URL

(ftp://user:password@host:port/path) 中的“path”需使用相对路径。

debug monitor import scp <username@remote_address:filepath>

允许使用者通过 SCP 的方式导入一个使用者自定义的脚本。用户可以在脚本中定义能够显示自己想要收集的调试信息的 CLI 命令，然后通过这条命令导入到系统中，用户就可以收集到他想要的信息。执行该命令之前，请先禁用“**debug monitor**”。

username@remote_address:filepath 这个参数必须置于双引号内，例如：
“test@172.16.13.12:/home/test”。

debug monitor export ftp <user_name> <remote_ftp_ip>

通过 FTP 方式把记录调试监控信息的文件导出到远程服务器上。执行该命令之前，请先禁用“debug monitor”。

debug monitor export scp <username@remote_address:filepath>

通过 SCP 方式把记录调试监控信息的文件导出到远程服务器上。执行该命令之前，请先禁用“debug monitor”。

username@remote address:filepath 这个参数必须置于双引号内，例如：
“test@172.16.13.12:/home/test”。

show debug monitor

显示调试监控的所有配置，包括它的状态和使用者已经导入的自定义脚本。

debug trace live tcp <interface_name> [tcpdump_argument]

该命令用于实况跟踪 TCP 活动。输出结果直接显示在屏幕中。

interface_name	该参数指定接口的名称，接口可以为系统接口、MNET 接口、聚合接口、VLAN 接口或 VXLAN 接口。
tcpdump_argument	该参数指定 TCPDUMP 中的参数。TCPDUMP 是一种数据报分析工具。该参数用于指定哪一类 TCP 活动将会被实况跟踪。其中，设备支持的参数为 c、e、f、n、N、q、T、S、t、v、x 和 X。取值格式为“-argument”，例如“-T”。如不指定该参数，所有 TCP 活动将被实时跟踪。

debug trace tcp all [tcpdump_argument]

该命令用于实时跟踪所有接口上的 TCP 活动，跟踪到的 TCP 活动将存放到 tcpdump 和 sslkeylog（如果有 SSL 连接）文件中。sslkeylog 文件里包含 RSA 或 ECC 的客户端随机数和主密钥信息。

tcpdump_argument	可选，该参数指定 TCPDUMP 中的参数，表示将被实时跟踪的 TCP 活动的类型。TCPDUMP 是一种数据报分析工具，设备支持的 TCPDUMP 参数包括 c、e、f、n、N、q、T、S、t、v、x 和 X。取值格式为“-argument”，例如“-T”。如不指定该参数，所有 TCP 活动将被实时跟踪。

debug trace tcp loopback [tcpdump_argument]

该命令用于跟踪环回接口上的 TCP 活动。输出结果被写入 /var/crash/sys_debug/debug 目录下的一个新生成的文件（例如 tcpdump_lo0.20090810_160302）中。

tcpdump_argument	TCPDUMP 中的参数。TCPDUMP 是一种数据报分析工具。该参数用于指定哪一类 TCP 活动将会被实况跟踪。其中，设备支持的参数为 c、e、f、n、N、q、T、S、t、v、x 和 X。取值格式为“-argument”，例如“-T”。如

不指定该参数，所有 TCP 活动将被实时跟踪。

debug trace tcp nic [tcpdump_argument]

该命令用于跟踪所有 NIC 上的 TCP 活动。输出结果被写入 /var/crash/sys_debug/nic_trace 目录下一个新生成的文件（例如 tcpdump_port1.20090810_160508）中。

tcpdump_argument TCPDUMP 中的参数。TCPDUMP 是一种数据报分析工具。该参数用于指定哪一类 TCP 活动将会被实况跟踪。其中，设备支持的参数为 c、e、f、n、N、q、T、S、t、v、x 和 X。取值格式为“-argument”，例如“-T”。如不指定该参数，所有 TCP 活动将被实时跟踪。

debug trace tcp pipe0 [tcpdump_argument]

该命令用于跟踪 pipe0 上的 TCP 活动。输出结果被写入 /var/crash/sys_debug/debug 目录下一个新生成的文件（例如 tcpdump_pipe0.20090810_160410）中。

tcpdump_argument TCPDUMP 中的参数。TCPDUM 是一种数据报分析工具。该参数用于指定哪一类 TCP 活动将会被实况跟踪。其中，设备支持的参数为 c、e、f、n、N、q、T、S、t、v、x 和 X。取值格式为“-argument”，例如“-T”。如不指定该参数，所有 TCP 活动将被实时跟踪。

debug usage memory

该命令用于启用跟踪系统 mbuf 和内存池（mpool）的使用情况。执行该命令后，管理员可以使用“show debug usage mbuf”和“show debug usage mpool”命令查看系统 mbuf 和内存池的使用信息。

如果要停止跟踪，使用“no debug usage memory”命令。

```
Demo#show debug usage mbuf
```

```
Mbuf usage Statistics
```

```
index: 1, app: 0x201993a8
```

```
Total mbufs: 2094848
```

Module Name	no of mbufs (col 1)	no of mbufs (col 2)
ID_0:	2094847	2094847
ID_1:	1	0
ID_21:	0	1

no debug usage memory

该命令用于停止跟踪系统 mbuf 和内存池（mpool）的使用情况。

show debug usage mbuf

该命令用于显示 mbuf 的使用信息。

show debug usage mpool

该命令用于显示内存池的使用信息。

show debug usage cpu

该命令用于显示每个 CPU 内核的使用信息。该命令可在 enable 及以上的访问控制级别下执行。

debug trace proxy

该命令用于跟踪 proxy 活动。输出结果被写入 englog 文件中。

debug trace live proxy [src_ip] [src_port] [dst_ip] [dst_port] [and|or]

该命令用于实况跟踪 proxy 活动。输出结果直接显示在屏幕中。

src_ip	被跟踪的源 IP 地址。默认值为 0.0.0.0，该默认值表示所有源 IP 地址都会被实况跟踪。
src_port	被跟踪的源端口号。默认值为 0，该默认值表示所有源端口都会被实况跟踪。
dst_ip	被跟踪的目的 IP 地址。默认值为 0.0.0.0，该默认值表示所有的目的 IP 地址都会被实况跟踪。
dst_port	被跟踪的目的端口号。默认值为 0，该默认值表示所有的目的端口都会被实况跟踪。
and or	配置参数（源地址、源端口、目的地址、目的端口）之间的关系。“and”表示必须同时与所有配置参数（源地址、源端口、目的地址、目的端口）匹配的输出结果才会被显示在屏幕上。“or”则表示与任意一个配置参数匹配的输出结果都会被显示在屏幕上。

debug trace live event backward <regular_expression>

该命令用于以时间的反向顺序显示调试日志缓存中的信息。

debug trace live event forward <regular_expression>

该命令用于以时间的正向顺序显示调试日志缓存中的信息。

debug hardware diagnostics [nic_reset_threshold] [memory_error_threshold] [led_on_duration]

该命令用于检测设备硬件状态的判定条件。运行该命令后，管理员可运行“show hardware diagnostics”命令查看检测结果。

nic_reset_threshold	可选。该参数指定网卡重启阈值。其取值范围为 10 到 60,000 之间的整数。默认值为 500。
memory_error_threshold	可选。该参数指定内存错误阈值。其取值范围为 1000 到 60,000 之间的整数。默认值为 1000。
led_on_duration	可选。该参数指定 LED 灯常亮时间。其取值范围为 0 到 65,535 之间的整数，单位为秒。默认值为 300。

show hardware [diagnostics]

该命令用于显示设备硬件配置或硬件状态检测结果。如果不指定参数“diagnostics”，则将显示设备硬件配置。

diagnostics	可选。该参数用于指定系统显示硬件检测结果。其取值必须为“diagnostics”或空。 默认值为空。

18.12 远程管理命令

telnet <host port>

该命令用于建立一个 Telnet 远程会话。设备支持 Unix 系统下的所有 Telnet 命令的标准参数，详情可参考 Telnet 命令的相关技术文文件。这条命令可以在 Enable 级别下执行。

host port	指定远程主机的 IP 地址及端口号。



注意：该命令的所有参数都必须置于双引号内。如果需要为参数设置属性值，则参数及属性值要先置于单引号内，再置于双引号内。例如：telnet “‘192.168.1.24 -l admin’”。

下面是一个关于“telnet”命令的示例：

```
Demo# telnet “‘172.16.2.182 -4’”
Trying 172.16.2.182...
Connected to 172.16.2.182 -4.
Escape character is '^]'.
Trying SRA secure login:
User (root): admin
Password:
[ SRA accepts you ].....succeed
```

ssh remote <user@hostname>

该命令用于建立一条连接远程主机的 SSH 连接。设备支持 Unix 系统下的所有 SSH 命令的标准参数，详情可参考 OpenSSH 命令的相关技术文文件。这条命令可以在 Enable 级别下执行。

`user@hostname` 指定远程主机的用户名及主机名或主机 IP 地址。



注意：该命令的所有参数都必须置于双引号内。如果需要为参数设置属性值，可将参数及属性值一同置于双引号内。例如：`ssh remote "user@192.168.1.24 -p 8888"`。

下面是一个关于 “**ssh remote**” 命令的示例：

```
Demo#ssh remote "root@172.16.85.240"
root@172.16.85.240's password:
Linux libh-server1 2.6.32-22-generic #33-Ubuntu SMP Wed Apr 28 13:27:30 UTC 2010 i686
GNU/Linux

Welcome to Ylmf_OS!
* Information:  http://www.ymf.com/

0 packages can be updated.
0 updates are security updates.

Last login: Wed Apr 20 00:39:35 2011 from 10.3.46.1
root@libh-server1:~#
```

18.13 自定义配置脚本

custom script import <url>

该命令用于从指定的 URL 地址导入自定义的配置脚本文件。导入自定义脚本前，请先联系公司技术支持对脚本进行签名。

`url` 该参数指定脚本文件的 URL 地址，支持 FTP、HTTP、SCP 和 TFTP。在 URL 中，脚本文件名称取值必须为长度不大于 32 个字符的字符串（不包含 URL 的路径和文件名后缀）。脚本文件名称取值仅支持字母、数字、“.”、“_”和“-”。文件名的后缀必须为 “.signed.tar.gz”。

例如：SCP 类型 URL “`scp user_name@ip:/path`” 和 TFTP 类型 URL “`tftp ip:/path`”。

注意：FTP 类型 URL (`ftp://user:password@host:port/path`) 中的 “path” 需使用相对路径。

custom script export <file_name> <url>

该命令用于将指定的自定义配置脚本文件导出到指定的 URL 地址。

file_name 该参数指定脚本文件的名称。

- 如果参数取值为脚本文件名称，取值应与通过“**custom script import**”命令导入的脚本文件名称相同（不带后缀“.signed.tar.gz”）。
- 如果参数取值为“all”，系统将会导出所有的脚本文件。

url 该参数指定 URL 地址，支持 FTP、SCP 和 TFTP。

注意：FTP 类型 URL：ftp user@ip。

custom script exec <file_name> [para_string]

该命令用于执行指定的自定义配置脚本文件，并设置相关参数。

file_name 该参数指定已导入的脚本文件的名称。脚本文件通过命令“**custom script import**”导入，已导入的文件名称通过“**show custom script**”命令查看。

para_string 该参数指定脚本的相关参数。取值必须为长度不大于 512 个字符的字符串，仅支持字母、数字、“.”、“:”、“_”、“-”和“ ”。

注意：通过脚本批量启用或禁用后台服务时，如果其中的某个后台服务在脚本执行之前已经被启用或禁用，那么在执行脚本时将对除了该后台服务之外的其他后台服务执行启用或禁用操作。

no custom script <file_name>

该命令用于删除指定的自定义配置脚本文件。

show custom script [file_name] [mode]

该命令用于显示指定的自定义配置脚本文件的相关信息。

file_name 可选，该参数指定脚本文件的名称，取值为空（使用“ ”表示）时，该命令将显示所有脚本文件的相关信息。

默认值为空。

mode 可选，该参数指定显示模式，取值必须为：

- **verbose**：表示显示脚本文件的内容。
- **summary**：表示只显示脚本文件的名称。

默认值为“summary”。



注意：通过脚本批量启用或禁用后台服务时，如果其中的某个后台服务已经被启用或禁用，那么在执行脚本后，通过该命令显示脚本内容时，将只显示该后台服务。

clear custom script

该命令用于清除系统中所有通过“**custom script import**”命令导入的自定义配置脚本文件。

18.14 带宽管理命令

show bandwidth usage [start_date] [end_date]

该命令用来显示带宽使用信息，最多可显示 400 日之内的信息。用户既可以浏览自起始日期起所有天数的带宽使用信息，也可以只浏览指定期限内的带宽使用信息。如果不指定起始与结束日期，则系统默认显示从设备开始运行之日起到当前日期的所有相关信息。

start_date 指定起始日期，默认值为空。参数格式为“yyyymmdd”，其中，“yyyy”表示年份，“mm”表示月份，而“dd”表示日。比如：“20100129”表示 2010 年 1 月 29 日。“yyyy”的取值范围为 2000~2037。

注意：参数“start_date”的取值必须小于参数“end date”的取值。

end_date 指定结束日期，默认值为空。参数的格式和取值范围与“start_date”参数相同。

show bandwidth violation

该命令用于显示系统带宽超出 license 规定的带宽上限时，系统记录的全部信息。



注意：带宽上限只针对 vAPV 有效。因此，上述两条命令的输出信息中，“Licensed Bandwidth”一项在物理机上的内容总是 0 bps。

18.15 登录界面管理命令

system motd {enable|disable}

该命令用于启用或禁用 MOTD（Message of the Day，每日提示）功能。启用该功能之前，需导入 MOTD 的配置文件，系统才会在 CLI 和 WebUI 登录界面上显示每日提示信息。管理员可以通过配置文件自定义需要显示的每日提示信息。该功能默认设置为禁用。

system motd import <url>

该命令用于导入 MOTD 配置文件。每个系统只能导入一个 MOTD 配置文件。

url 该参数指定需要导入的 MOTD 配置文件的 HTTP 或 FTP URL 地址。

注意: FTP 类型 URL(ftp://user:password@host:port/path) 中的 “path” 需使用相对路径。

no system motd import

该命令用于删除 MOTD 配置文件。执行该命令后, MOTD 功能将变为禁用状态。

show system motd config

该命令用于显示当前的 MOTD 配置。

18.16 网卡管理命令

system portmap

该命令用于将网口排序信息保存到配置文件, 仅适用于物理设备。

保存网口排序信息后, 系统再次启动时, 会加载配置文件并检测网卡。

- 如果检测到新增网卡或者更换网卡, 系统会对所有网卡对应的网口进行重新排序。
- 如果检测到的网口数量小于配置文件中的网口数量且没有新增网卡, 则采用保存的排序。
- 如果检测到相同类型和速率的网卡发生了位置调换, 系统会认为存在网口乱序, 将对所有网卡对应的网口进行重新排序。

no system portmap

该命令用于清除保存的网口排序信息。

当需要重新保存网口排序信息时, 如果存在新增网卡, 必须先清除已存在的网口排序信息; 如果存在故障网卡, 不仅要清除已存在的网口排序信息还要重启系统。

show system portmap

该命令用于显示保存的网口排序及网口状态信息, 包括网口数量、网卡对应的网口序号及 MAC 地址。

18.17 文件系统救援

system rescue file backup <password>[partiton_number]

该命令用于在当前分区备份需要进行文件系统救援的分区文件。

password

该参数指定需要备份的文件的密码，取值必须为长度不大于 32 个字节的字符串，支持字母、数字和特殊字符（“~”、“#”、“%”、“^”、“&”、“*”、“(”、“)”、“-”、“_”、“+”、“=”、“ ”、“{”、“}”、“[”、“]”、“!”、“:”、“;”、“\”、“|”、“<”、“>”、“,”、“.”、“?”、“/”和“\$”）。当取值包含特殊字符时，必须置于双引号内且取值的前两位不能使用除“.”、“/”以外的其他特殊字符。

partition_number

可选，该参数指定需要救援的分区号。双分区系统取值必须为默认值，四分区系统取值必须为 0 至 3 之间的整数。

默认值为当前分区号的下一个分区号。



注意：

- 视文件系统损坏程度而异，执行该命令备份文件不一定成功。
- 不支持在分区模式下执行该命令。
- 当前分区空间不足时备份失败。

system rescue partition <mode> [partition_number]

该命令用于在当前分区救援文件系统受损的其他分区。

mode

该参数指定救援模式，取值必须为：

- **repair**：修复模式。系统将检测并修复原文件系统。
- **rebuild**：重建模式。系统将格式化原文件系统并构建目录结构。

partition_number

可选，该参数指定需要救援的分区号。双分区系统取值必须为默认值，四分区系统取值必须为 0 至 3 之间的整数。

默认值为当前分区号的下一个分区号。



注意：

- 不支持在分区模式下执行该命令。
- 执行此命令前需先执行“**system rescue file backup**”命令保存分区文件。
- 修复模式不保证能修复成功。

system rescue file restore <passwd>[partition_number]

该命令用于在当前分区恢复文件系统受损的分区。

passwd	该参数指定备份文件的密码，取值必须为长度不大于 32 个字节的字符串，支持字母、数字和特殊字符（“~”、“#”、“%”、“^”、“&”、“*”、“(”、“)”、“-”、“_”、“+”、“=”、“ ”、“{”、“}”、“[”、“]”、“'”、“:”、“;”、“\”、“ ”、“<”、“>”、“,”、“.”、“?”、“/”和“\$”）。当取值包含特殊字符时，必须置于双引号内且取值的前两位不能使用除“.”、“/”以外的其他特殊字符。
partition_number	可选，该参数指定需要救援的分区号。双分区系统取值必须为默认值，四分区系统取值必须为 0 至 3 之间的整数。 默认值为当前分区号的下一个分区号。



注意：不支持在分区模式下执行该命令。

18.18 一键巡检命令

system inspection regular task <task_name> <task_type> <task_interval>
<crontab_expression> <report_number> <overlap>

该命令用于创建一个定时一键巡检任务。

task_name	该参数指定定时一键巡检任务的名称，取值必须为长度不大于 64 个字节的字符串，区分大小写。参数取值仅支持数字，字母，下划线，中划线。当参数取值包含特殊字符时，必须置于双引号内。
task_type	该参数指定定时一键巡检任务的类型。取值必须为： • primary：表示日常巡检。 • intermediate：表示应急巡检。 • deep：表示深度巡检。
task_interval	该参数指定定时一键巡检任务的巡检间隔，取值必须为“daily”、“weekly”、“monthly”或“yearly”。
crontab_expression	该参数指定 Crontab 功能执行定时一键巡检任务的周期表达式，格式必须为：“Month: XX; Week: XX; Day: XX; Hour: XX; Minute: XX”。关于时间信息项“Month”、“Week”、“Day”、“Hour”和“Minute”的取值见

下面的表格。

report_number	该参数指定定时一键巡检任务可以保存的巡检报告的个数。取值必须为 1 到 30 之间的整数。
overlap	该参数指定定时一键巡检任务执行的次数达到参数“report_number”指定的个数后，该任务停止执行或者覆盖历史报告。取值必须为： 0：表示达到指定的个数后，任务将停止执行。 1：表示达到指定的个数后，系统将覆盖历史报告。

表18 - 2 时间信息项参数取值范围

时间信息项	参数取值范围
Minute	00-59
Hour	00-23
Day	01-31
Month	01-12
Week	0 到 6：1 到 6 表示星期一到星期六；“0”表示星期日。

示例：

创建一个每周六 10：20 定期执行的一键巡检任务，配置如下：

```
system inspection regular task "task1" deep weekly "Week:6;Hour:10;Minute:20" 20 0
```

no system inspection regular task <task_name>

该命令用于删除指定的定时一键巡检任务，同时删除该任务的历史报告。

show system inspection regular task [task_name]

该命令用于显示指定的定时一键巡检任务的配置。如果不指定参数“task_name”的值，将显示所有定时一键巡检任务的配置。

clear system inspection regular task

该命令用于清除所有的定时一键巡检任务。

附录一 SNMP OID 列表

SNMP OID	描述
.1.3.6.1.4.1.7564	此档定义了私有的 CA SNMP MIB 扩展。 添加了 RAW CPU 和 IO 计数器。 从早期 MIB 定义转换过来的 SMIv2 版本。
.1.3.6.1.4.1.7564.3.1	设备的序号。
.1.3.6.1.4.1.7564.3.2	CPU 内核使用率表格，包含内核 ID 和内核使用率。
.1.3.6.1.4.1.7564.3.2.1	CPU 内核使用率表格的一个概念行，包含每个 CPU 内核的使用率信息。
.1.3.6.1.4.1.7564.3.2.1.1	每个 CPU 内核的引用索引。
.1.3.6.1.4.1.7564.3.2.1.2	每个 CPU 内核的 ID。
.1.3.6.1.4.1.7564.3.2.1.3	每个 CPU 内核的使用率。
.1.3.6.1.4.1.7564.3.3	设备的软件版本号。
.1.3.6.1.4.1.7564.3.4	设备的设备型号。
.1.3.6.1.4.1.7564.3.5	设备硬盘总空间（单位 MB）。
.1.3.6.1.4.1.7564.3.6	设备已使用的硬盘空间（单位 MB）。
.1.3.6.1.4.1.7564.3.7	设备可用的硬盘空间（单位 MB）。
.1.3.6.1.4.1.7564.3.8	设备已使用的硬盘空间百分比。
.1.3.6.1.4.1.7564.3.9	设备可用的硬盘空间百分比。
.1.3.6.1.4.1.7564.3.10	NTP 状态，0 为不可用，1 为可用。
.1.3.6.1.4.1.7564.3.11	设备第二分区的软件版本。
.1.3.6.1.4.1.7564.3.12	系统运行时间。
.1.3.6.1.4.1.7564.3.13	系统硬盘分区使用率。
.1.3.6.1.4.1.7564.3.14	数据硬盘分区使用率。
.1.3.6.1.4.1.7564.3.15.0	许可密钥开始时间，不支持 83 位许可密钥。
.1.3.6.1.4.1.7564.3.16.0	许可密钥到期时间。
.1.3.6.1.4.1.7564.3.17.0	许可密钥状态，0 为在有效期内，1 为未激活，2 为过期。
.1.3.6.1.4.1.7564.3.18.0	CPU 核数。
.1.3.6.1.4.1.7564.4.1	当前的系统全部可用内存。
.1.3.6.1.4.1.7564.4.2	当前的网络内存使用率百分比。
.1.3.6.1.4.1.7564.4.3	当前使用的 Swap 空间（单位 MB）。
.1.3.6.1.4.1.7564.4.4	当前 Swap 空间使用率。
.1.3.6.1.4.1.7564.4.5	当前的系统内存使用率百分比。
.1.3.6.1.4.1.7564.4.6	当前的连接内存使用率百分比
.1.3.6.1.4.1.7564.4.7.0	设备已使用的系统内存空间（单位 KB）。
.1.3.6.1.4.1.7564.4.8.0	设备剩余的系统内存空间（单位 KB）。
.1.3.6.1.4.1.7564.16.1.1	当前的反向代理缓存的状态，开启或关

	闭。
.1.3.6.1.4.1.7564.16.1.2	反向代理缓存接收到的请求总数。
.1.3.6.1.4.1.7564.16.1.3	反向代理缓存接收到的所有 GET 请求。
.1.3.6.1.4.1.7564.16.1.4	反向代理缓存接收到的所有 HEAD 请求。
.1.3.6.1.4.1.7564.16.1.5	反向代理缓存接收到的所有 PURGE 请求。
.1.3.6.1.4.1.7564.16.1.6	反向代理缓存接收到的所有 POST 请求。
.1.3.6.1.4.1.7564.16.1.7	当前客户端连接数（例如来自浏览器）。
.1.3.6.1.4.1.7564.16.1.8	当前后端服务器的连接数。
.1.3.6.1.4.1.7564.16.1.9	复位向到 HTTPS 的请求。
.1.3.6.1.4.1.7564.16.1.10	基于正则表达式匹配复位向的请求。
.1.3.6.1.4.1.7564.16.1.11	通过重写 URL 转发的请求。
.1.3.6.1.4.1.7564.16.1.12	改写到 HTTPS 的位置。
.1.3.6.1.4.1.7564.16.1.13	基于正则表达式匹配做改写的位置。
.1.3.6.1.4.1.7564.16.1.14	缓存跳过，缓存关闭。
.1.3.6.1.4.1.7564.16.1.15	我们发现请求的 URL 在缓存中。对象是新的，我们没有必要重新验证，为其提供了缓存的内容。
.1.3.6.1.4.1.7564.16.1.16	我们收到的请求含有 IMS 头部。我们验证了时间戳，确定该对象的客户端副本是新的。因此，我们生成一个 304 响应并发给客户端。
.1.3.6.1.4.1.7564.16.1.17	缓存命中，以先决条件失败（Precondition Failed）回复。
.1.3.6.1.4.1.7564.16.1.18	被请求的对象在缓存中存在。但是，请求要求重新校验（由于客户端产生的重新校验，代理产生的重新校验或代理产生的强制不使用缓存）。
.1.3.6.1.4.1.7564.16.1.19	请求在缓存表中搜索不到结果。请求的一些内容是我们认为是不可缓存的（例如过长的 URL，Cache-Control: no-store 头部等等）。
.1.3.6.1.4.1.7564.16.1.20	搜索缓存表，发现没有匹配的条目并创建一个新条目的次数。需要注意的是，有时只是临时创建一个条目（例如，对于一个导致 304 错误的 IMS 请求）发送到客户端后删除（延迟删除）。
.1.3.6.1.4.1.7564.16.1.21	缓存未命中，创建新条目，不可缓存的回应。
.1.3.6.1.4.1.7564.16.1.22	命中使用缓存回复以及通过缓存回复“未修改”。
.1.3.6.1.4.1.7564.17.1	HA 分组数量。

.1.3.6.1.4.1.7564.17.15	HA 节点表。
.1.3.6.1.4.1.7564.17.15.1	包含 HA 节点信息的表项。
.1.3.6.1.4.1.7564.17.15.1.1	每个 HA 节点的引用索引。
.1.3.6.1.4.1.7564.17.15.1.2	HA 节点名称。
.1.3.6.1.4.1.7564.17.15.1.3	HA 节点 IP 地址的类型。
.1.3.6.1.4.1.7564.17.15.1.4	HA 节点的 IP 地址。
.1.3.6.1.4.1.7564.17.15.1.5	主链路用于同其他 HA 节点通信的端口。
.1.3.6.1.4.1.7564.17.15.1.6	备用链路的数量。
.1.3.6.1.4.1.7564.17.15.1.7	HA 节点状态: DOWN (0)、INIT (1)、FFO_LOGIN (2)、NETWORK_LOGIN (3)、SYNC_HA_LINK (4)、SYNC_CONFIG (5)、SYNC_CONN (6)、READY (7)、UP (8)、CLOSING (9)、UNKNOWN (-1)。
.1.3.6.1.4.1.7564.17.25	HA 分组表。
.1.3.6.1.4.1.7564.17.25.1	包含 HA 分组信息的表项。
.1.3.6.1.4.1.7564.17.25.1.1	HA 分组表索引。
.1.3.6.1.4.1.7564.17.25.1.2	HA 分组 ID。
.1.3.6.1.4.1.7564.17.25.1.3	在本地 HA 节点上 HA 分组的优先级。
.1.3.6.1.4.1.7564.17.25.1.4	抢占功能的状态, 控制高优先级节点是否抢占低优先级节点。
.1.3.6.1.4.1.7564.17.25.1.5	HA 分组状态: disabled (0)、incomplete (1)、init (2)、standby (3)或 active (4)。
.1.3.6.1.4.1.7564.17.25.1.6	HA 分组的启用状态。
.1.3.6.1.4.1.7564.17.26	浮动 IP 地址表。
.1.3.6.1.4.1.7564.17.26.1	包含浮动 IP 地址信息的表项。
.1.3.6.1.4.1.7564.17.26.1.1	浮动 IP 地址表索引。
.1.3.6.1.4.1.7564.17.26.1.2	包含该浮动 IP 地址的 HA 分组。
.1.3.6.1.4.1.7564.17.26.1.3	浮动 IP 地址的类型。
.1.3.6.1.4.1.7564.17.26.1.4	HA 分组中包含的浮动 IP 地址。
.1.3.6.1.4.1.7564.18.1.1	VRRP 表中当前可能的最大条目数, 计算方式是“255 乘以集群定义的接口数”。集群中 VIP 的最大个数是 255。
.1.3.6.1.4.1.7564.18.1.2	VRRP 表当前条目数。
.1.3.6.1.4.1.7564.18.1.3	包含集群配置的表。
.1.3.6.1.4.1.7564.18.1.3.1	VRRP 表中的一个条目。每个条目表示一个集群 VIP 而非集群本身。如果一个集群有 n 个 VIP, 那么 VRRP 表中这个集群有 n 个条目 (0 ≤ n ≤ 255)。在 VRRP 表中属于同一个集群的所有条目除了集群 VirIndex 和集群 VirAddr 其它所有字段具有相同的值。

.1.3.6.1.4.1.7564.18.1.3.1.1	集群虚拟表的索引。
.1.3.6.1.4.1.7564.18.1.3.1.2	集群 ID。
.1.3.6.1.4.1.7564.18.1.3.1.3	集群的当前状态。
.1.3.6.1.4.1.7564.18.1.3.1.4	定义了集群的接口名称。
.1.3.6.1.4.1.7564.18.1.3.1.5	集群中的一个虚拟 IP 地址（VIP）。
.1.3.6.1.4.1.7564.18.1.3.1.6	正在使用的集群验证类型。无（0）：不进行验证；简单文本密码（1）：使用集群指定的密码进行验证。
.1.3.6.1.4.1.7564.18.1.3.1.7	用于集群认证的密码。
.1.3.6.1.4.1.7564.18.1.3.1.8	用于控制较高优先级的 VRRP 备用设备是否抢占较低优先级的主设备。
.1.3.6.1.4.1.7564.18.1.3.1.9	VRRP 广播间隔。
.1.3.6.1.4.1.7564.18.1.3.1.10	集群中本地节点的优先级。
.1.3.6.1.4.1.7564.18.1.3.1.11	集群虚拟 IP 地址的类型。
.1.3.6.1.4.1.7564.18.1.3.1.12	集群中的虚拟 IP 地址。
.1.3.6.1.4.1.7564.19.1.1.1	当前已配置的后台服务的数量。
.1.3.6.1.4.1.7564.19.1.1.2	包含后台服务配置的表。
.1.3.6.1.4.1.7564.19.1.1.2.1	包含一个后台服务信息的表项。
.1.3.6.1.4.1.7564.19.1.1.2.1.1	每个后台服务的引用索引。
.1.3.6.1.4.1.7564.19.1.1.2.1.2	后台服务的名称。
.1.3.6.1.4.1.7564.19.1.1.2.1.3	后台服务的协议。
.1.3.6.1.4.1.7564.19.1.1.2.1.4	后台服务 IP 地址。
.1.3.6.1.4.1.7564.19.1.1.2.1.5	后台服务端口号。
.1.3.6.1.4.1.7564.19.1.1.2.1.6	每个后台服务的最大连接数。
.1.3.6.1.4.1.7564.19.1.1.2.1.8	后台服务当前的状态，Up 或 Down。
.1.3.6.1.4.1.7564.19.1.1.2.1.9	服务器的平均响应时间（微秒）。
.1.3.6.1.4.1.7564.19.1.1.2.1.10	后台服务 IP 地址的类型。
.1.3.6.1.4.1.7564.19.1.1.2.1.11	后台服务的 IP 地址。
.1.3.6.1.4.1.7564.19.1.2.1	当前已配置的虚拟服务的数量。
.1.3.6.1.4.1.7564.19.1.2.2	包含虚拟服务配置的表。
.1.3.6.1.4.1.7564.19.1.2.2.1	包含一个虚拟服务配置的表项。
.1.3.6.1.4.1.7564.19.1.2.2.1.1	每个虚拟服务的引用索引。
.1.3.6.1.4.1.7564.19.1.2.2.1.2	虚拟服务的名称。
.1.3.6.1.4.1.7564.19.1.2.2.1.3	虚拟服务的协议。
.1.3.6.1.4.1.7564.19.1.2.2.1.4	虚拟服务的 IP 地址。
.1.3.6.1.4.1.7564.19.1.2.2.1.5	虚拟服务的端口号。
.1.3.6.1.4.1.7564.19.1.2.2.1.6	虚拟服务的最大连接数。
.1.3.6.1.4.1.7564.19.1.2.2.1.7	虚拟服务的 IP 地址类型。
.1.3.6.1.4.1.7564.19.1.2.2.1.8	虚拟服务的 IP 地址。
.1.3.6.1.4.1.7564.19.1.3.1	当前已配置的服务组数量。
.1.3.6.1.4.1.7564.19.1.3.2	包含服务组成员配置的表。

.1.3.6.1.4.1.7564.19.1.3.2.1	包含一个服务组成员配置的表项。
.1.3.6.1.4.1.7564.19.1.3.2.1.1	每个服务组成员的引用索引。
.1.3.6.1.4.1.7564.19.1.3.2.1.2	服务组的名称。
.1.3.6.1.4.1.7564.19.1.3.2.1.3	后台服务的名称。
.1.3.6.1.4.1.7564.19.1.3.2.1.4	用于服务组中负载均衡的算法。
.1.3.6.1.4.1.7564.19.1.4.1	当前已配置的主机节点数量。
.1.3.6.1.4.1.7564.19.1.4.2	包含主机节点成员配置的表。
.1.3.6.1.4.1.7564.19.1.4.2.1	包含一个主机节点信息的表项。
.1.3.6.1.4.1.7564.19.1.4.2.1.1	每个主机节点的引用索引。
.1.3.6.1.4.1.7564.19.1.4.2.1.2	主机节点的名称。
.1.3.6.1.4.1.7564.19.1.4.2.1.3	主机节点的 IP 地址。
.1.3.6.1.4.1.7564.19.2.1.1.1.22	后台服务的 SSL 握手成功率。
.1.3.6.1.4.1.7564.19.2.1.1.1.23	后台服务的 SSL 握手成功数。
.1.3.6.1.4.1.7564.19.2.1.1.1.24	后台服务的 SSL 握手总数。
.1.3.6.1.4.1.7564.19.2.1.1.1.25	后台服务的 SNAT 端口使用率（小于 1% 时显示为 0）。除 “l2ip” 和 “l2mac” 类型的后台服务用于二层负载均衡以外，其它类型的后台服务都支持 SNAT 端口使用率统计量。
.1.3.6.1.4.1.7564.19.2.2.1.1.42	虚拟服务的 SSL 握手成功率。
.1.3.6.1.4.1.7564.19.2.2.1.1.43	虚拟服务的 SSL 握手成功数。
.1.3.6.1.4.1.7564.19.2.2.1.1.44	虚拟服务的 SSL 握手总数。
.1.3.6.1.4.1.7564.19.2.4.1	主机节点的统计表。
.1.3.6.1.4.1.7564.19.2.4.1.1	包含一个主机节点统计信息的表项。
.1.3.6.1.4.1.7564.19.2.4.1.1.1	每个主机节点的引用索引。
.1.3.6.1.4.1.7564.19.2.4.1.1.2	主机节点的名称。
.1.3.6.1.4.1.7564.19.2.4.1.1.3	主机节点的当前连接数。
.1.3.6.1.4.1.7564.19.2.4.1.1.4	主机节点的每秒新建连接数。
.1.3.6.1.4.1.7564.19.2.4.1.1.5	主机节点的每秒请求连接数。
.1.3.6.1.4.1.7564.19.2.4.1.1.6	按照一定间隔统计的主机节点吞吐率（bits/s）。
.1.3.6.1.4.1.7564.19.2.1.1	后台服务的统计表。
.1.3.6.1.4.1.7564.19.2.1.1.1	包含一个后台服务统计信息的表项。
.1.3.6.1.4.1.7564.19.2.1.1.1.1	每个后台服务的引用索引。
.1.3.6.1.4.1.7564.19.2.1.1.1.2	后台服务的名称。
.1.3.6.1.4.1.7564.19.2.1.1.1.3	后台服务的 IP 地址。
.1.3.6.1.4.1.7564.19.2.1.1.1.4	后台服务的端口号。
.1.3.6.1.4.1.7564.19.2.1.1.1.5	后台服务的未完成请求数量。
.1.3.6.1.4.1.7564.19.2.1.1.1.6	到后台服务开启的连接数量。
.1.3.6.1.4.1.7564.19.2.1.1.1.7	发送到后台服务的全部请求的数量。
.1.3.6.1.4.1.7564.19.2.1.1.1.8	后台服务的健康状态（Up 或 Down）。

.1.3.6.1.4.1.7564.19.2.1.1.1.9	后台服务的 IP 地址类型。
.1.3.6.1.4.1.7564.19.2.1.1.1.10	后台服务的 IP 地址。
.1.3.6.1.4.1.7564.19.2.1.1.1.11	后台服务的入向带宽（Kbps）。
.1.3.6.1.4.1.7564.19.2.1.1.1.12	后台服务的出向带宽（Kbps）。
.1.3.6.1.4.1.7564.19.2.1.1.1.13	后台服务每秒新建连接数。
.1.3.6.1.4.1.7564.19.2.1.1.1.14	后台服务的每秒入向字节数。
.1.3.6.1.4.1.7564.19.2.1.1.1.15	后台服务的每秒出向字节数。
.1.3.6.1.4.1.7564.19.2.1.1.1.16	后台服务的每秒入向报文数。
.1.3.6.1.4.1.7564.19.2.1.1.1.17	后台服务的每秒出向报文数。
.1.3.6.1.4.1.7564.19.2.1.1.1.18	后台服务的入向字节总数。
.1.3.6.1.4.1.7564.19.2.1.1.1.19	后台服务的出向字节总数。
.1.3.6.1.4.1.7564.19.2.1.1.1.20	后台服务的入向报文总数。
.1.3.6.1.4.1.7564.19.2.1.1.1.21	后台服务的出向报文总数。
.1.3.6.1.4.1.7564.19.2.1.2	健康状态为 Up 的可用后台服务数量。
.1.3.6.1.4.1.7564.19.2.1.3	所有后台服务的连接总数。
.1.3.6.1.4.1.7564.19.2.2.1	虚拟服务的统计表。
.1.3.6.1.4.1.7564.19.2.2.1.1	包含一个虚拟服务统计信息的表项。
.1.3.6.1.4.1.7564.19.2.2.1.1.1	每个虚拟服务的引用索引。
.1.3.6.1.4.1.7564.19.2.2.1.1.2	虚拟服务的名称。
.1.3.6.1.4.1.7564.19.2.2.1.1.3	虚拟服务的 IP 地址。
.1.3.6.1.4.1.7564.19.2.2.1.1.4	虚拟服务的端口号。
.1.3.6.1.4.1.7564.19.2.2.1.1.5	虚拟服务 QoS URL 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.6	虚拟服务 QoS Hostname 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.7	虚拟服务 Persistent Cookie 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.8	虚拟服务 QoS Cookie 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.9	虚拟服务 Default 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.10	虚拟服务 Persistent URL 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.11	虚拟服务 Static 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.12	虚拟服务 QoS Network 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.13	虚拟服务 QoS URL 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.14	虚拟服务 Backup 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.15	虚拟服务缓存的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.16	虚拟服务 Regex 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.17	虚拟服务 Rewrite Cookie 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.18	虚拟服务 Insert Cookie 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.19	虚拟服务开启的连接数量。
.1.3.6.1.4.1.7564.19.2.2.1.1.20	虚拟 IP 地址的类型。
.1.3.6.1.4.1.7564.19.2.2.1.1.21	虚拟服务的 IP 地址。
.1.3.6.1.4.1.7564.19.2.2.1.1.22	虚拟服务 QoS Client Port 策略的命中次数。

	数。
.1.3.6.1.4.1.7564.19.2.2.1.1.23	虚拟服务 QoS Body 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.24	虚拟服务 Header 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.25	虚拟服务 Hash URL 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.26	虚拟服务 Redirect 策略的命中次数。
.1.3.6.1.4.1.7564.19.2.2.1.1.27	虚拟服务接收的字节总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.28	虚拟服务发出的字节总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.29	虚拟服务接收的入向报文总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.30	虚拟服务发出的出向报文总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.31	虚拟服务每秒新建连接数。
.1.3.6.1.4.1.7564.19.2.2.1.1.32	虚拟服务的入向吞吐率（Kbps）。
.1.3.6.1.4.1.7564.19.2.2.1.1.33	虚拟服务的出向吞吐率（Kbps）。
.1.3.6.1.4.1.7564.19.2.2.1.1.34	虚拟服务每秒接收的入向报文数。
.1.3.6.1.4.1.7564.19.2.2.1.1.35	虚拟服务每秒发出的出向报文数。
.1.3.6.1.4.1.7564.19.2.2.1.1.36	虚拟服务健康状态。
.1.3.6.1.4.1.7564.19.2.2.1.1.37	每个虚拟服务的 TCP 连接统计
.1.3.6.1.4.1.7564.19.2.2.1.1.38	虚拟服务收到的入向字节总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.39	虚拟服务发送的出向字节总数。
.1.3.6.1.4.1.7564.19.2.2.1.1.40	虚拟服务的吞吐量。
.1.3.6.1.4.1.7564.19.2.2.1.1.41	虚拟服务的 SSL 并发会话数。
.1.3.6.1.4.1.7564.19.2.2.1.1.45	虚拟服务的总连接数。
.1.3.6.1.4.1.7564.19.2.2.2	所有虚拟服务的连接总数。
.1.3.6.1.4.1.7564.19.2.3.1	服务组的统计表。
.1.3.6.1.4.1.7564.19.2.3.1.1	包含一个服务组统计信息的表项。
.1.3.6.1.4.1.7564.19.2.3.1.1.1	每个服务组的引用索引。
.1.3.6.1.4.1.7564.19.2.3.1.1.2	服务组的名称。
.1.3.6.1.4.1.7564.19.2.3.1.1.3	服务组的命中总数。
.1.3.6.1.4.1.7564.19.2.3.1.1.4	服务组状态，如果组里的服务全部为 Down，则服务组为 Down，否则为 Up。
.1.3.6.1.4.1.7564.19.2.3.1.1.5	服务组的后台服务总数。
.1.3.6.1.4.1.7564.19.2.3.1.1.6	服务组的每秒连接数。
.1.3.6.1.4.1.7564.19.2.3.1.1.7	后台服务组使用的算法。
.1.3.6.1.4.1.7564.20.1.2	当前配置的 SSL 主机数量。
.1.3.6.1.4.1.7564.20.2.1	开启的 SSL 连接总数（所有 SSL 主机）。
.1.3.6.1.4.1.7564.20.2.2	接受的 SSL 连接总数（所有 SSL 主机）。
.1.3.6.1.4.1.7564.20.2.3	请求的 SSL 连接的总数（所有 SSL 主机）。
.1.3.6.1.4.1.7564.20.2.4	SSL 主机统计表。
.1.3.6.1.4.1.7564.20.2.4.1	包含一个 SSL 主机统计的表项。
.1.3.6.1.4.1.7564.20.2.4.1.1	SSL 表索引。
.1.3.6.1.4.1.7564.20.2.4.1.2	SSL 主机的名称。
.1.3.6.1.4.1.7564.20.2.4.1.3	SSL 主机上开启的 SSL 连接。

.1.3.6.1.4.1.7564.20.2.4.1.4	一个 SSL 主机上接受的 SSL 连接的数量。
.1.3.6.1.4.1.7564.20.2.4.1.5	一个 SSL 主机上请求的 SSL 连接的数量。
.1.3.6.1.4.1.7564.20.2.4.1.6	一个 SSL 主机上复用的 SSL 会话数量。
.1.3.6.1.4.1.7564.20.2.4.1.7	一个 SSL 主机上可复用的 SSL 会话数量。
.1.3.6.1.4.1.7564.20.2.4.1.8	一个 SSL 主机上未命中的 SSL 会话数量。
.1.3.6.1.4.1.7564.20.2.4.1.9	每秒建立的 SSL 连接数。
.1.3.6.1.4.1.7564.20.2.4.1.10	一个 SSL 主机的 SSL 握手成功率。
.1.3.6.1.4.1.7564.20.2.4.1.11	一个 SSL 主机的 SSL 握手成功数。
.1.3.6.1.4.1.7564.20.2.4.1.12	一个 SSL 主机的 SSL 握手总数。
.1.3.6.1.4.1.7564.20.2.5	每秒新建连接总数。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.6	设备的总吞吐量。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.7	设备的可复用会话数。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.8	设备的总并发会话数。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.9	SSL 握手成功率。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.10	SSL 握手成功数。（所有 SSL 主机）
.1.3.6.1.4.1.7564.20.2.11	SSL 握手总数。（所有 SSL 主机）
.1.3.6.1.4.1.7564.22.1	VIP 统计功能的状态，启用或禁用。
.1.3.6.1.4.1.7564.22.2	VIP 代表的主机名（设备主机名）。
.1.3.6.1.4.1.7564.22.3	当前时间，格式为月份/日期/年份 小时：分钟。
.1.3.6.1.4.1.7564.22.4	所有 VIP 收到的 IP 报文的总数。
.1.3.6.1.4.1.7564.22.5	所有 VIP 发送的 IP 报文的总数。
.1.3.6.1.4.1.7564.22.6	所有 VIP 收到的 IP 字节总数。
.1.3.6.1.4.1.7564.22.7	所有 VIP 发送的 IP 字节总数。
.1.3.6.1.4.1.7564.22.8	VIP 统计信息表。
.1.3.6.1.4.1.7564.22.8.1	在 VIP 统计表中为每个 VIP 创建的一个表项。
.1.3.6.1.4.1.7564.22.8.1.1	VIP 统计信息表索引。
.1.3.6.1.4.1.7564.22.8.1.2	VIP 地址。
.1.3.6.1.4.1.7564.22.8.1.3	VIP 收到的 IP 报文总数。
.1.3.6.1.4.1.7564.22.8.1.4	VIP 收到的字节总数。
.1.3.6.1.4.1.7564.22.8.1.5	VIP 发送的报文总数。
.1.3.6.1.4.1.7564.22.8.1.6	VIP 发送的字节总数。
.1.3.6.1.4.1.7564.22.8.1.7	VIP 启用了时间统计信息收集。
.1.3.6.1.4.1.7564.22.8.1.8	IP 地址类型。
.1.3.6.1.4.1.7564.22.8.1.9	VIP 地址。
.1.3.6.1.4.1.7564.23.1	呈现在此系统上的网络接口数量。
.1.3.6.1.4.1.7564.23.2	所有活动接口收到的八位字节累计总数（环回接口不包括在内）。
.1.3.6.1.4.1.7564.23.3	所有活动接口发出的八位字节累计总数（环回接口不包括在内）。

.1.3.6.1.4.1.7564.23.4	接口统计信息表。表项数由界面数量的值确定。
.1.3.6.1.4.1.7564.23.4.1	一个界面统计表项。
.1.3.6.1.4.1.7564.23.4.1.1	每个接口的唯一值。它的取值范围在 1 到接口数的值之间。每个接口的值，至少要从该实体的网络管理系统的一次重新初始化到下一次重新初始化之间，始终保持不变。
.1.3.6.1.4.1.7564.23.4.1.2	接口名称。
.1.3.6.1.4.1.7564.23.4.1.3	界面当前运行状态（开启或关闭）。
.1.3.6.1.4.1.7564.23.4.1.4	接口 IP 地址。
.1.3.6.1.4.1.7564.23.4.1.5	接口收到的八位字节累计总数，包括帧字符。
.1.3.6.1.4.1.7564.23.4.1.6	由该子层向更高（子）层传送的，但不是发往该子层的多播、广播地址的报文数量。
.1.3.6.1.4.1.7564.23.4.1.7	由该子层向更高（子）层传送的发往该子层的多播或广播地址的报文数量。
.1.3.6.1.4.1.7564.23.4.1.8	被选为要丢弃的、未向更高协议层传送的入向报文的数量，即使这些报文未检测到错误。丢弃这样的报文的一个可能原因是为了释放缓存空间。
.1.3.6.1.4.1.7564.23.4.1.9	对于面向报文的接口，是指包含错误而未被传送到更高协议层的入向报文数量。对于面向字符或固定长度的接口，是指包含错误而未被传送到更高协议层的入向传输单元的数量。
.1.3.6.1.4.1.7564.23.4.1.10	对于面向报文的接口，是指通过该接口接收，但是因为协议未知或不支持而被丢弃的报文数量。对于面向字符或固定长度的支持协议多任务的接口，是指通过该接口接收，但是因为协议未知或不支持而被丢弃的报文数量。对于不支持协议多任务的任何接口，该计数器都始终为 0。
.1.3.6.1.4.1.7564.23.4.1.11	接口传输出去的八位字节累计总数，包括帧字符。
.1.3.6.1.4.1.7564.23.4.1.12	更高层协议要求传送，但不是发往该子层多播或广播地址的报文总数，包括丢弃的或没发出的报文。
.1.3.6.1.4.1.7564.23.4.1.13	更高层协议要求传送的发往该子层多播或广播地址的报文总数，包括丢弃的或没发出的报文。

.1.3.6.1.4.1.7564.23.4.1.14	对于面向报文的接口，是指因为错误而未传输的出向报文数量。对于面向字符或固定长度的接口，是指因为错误而无法传送的传输单元数量。
.1.3.6.1.4.1.7564.23.4.1.15	接口 IPv4 地址的地址类型（应为 IPv4）。
.1.3.6.1.4.1.7564.23.4.1.16	接口的 IPv4 地址。
.1.3.6.1.4.1.7564.23.4.1.17	接口 IPv6 地址的地址类型（应为 IPv6）。
.1.3.6.1.4.1.7564.23.4.1.18	接口的 IPv6 地址。
.1.3.6.1.4.1.7564.23.4.1.19	按照一定间隔统计的接口入向吞吐率（Kbps）。
.1.3.6.1.4.1.7564.23.4.1.20	按照一定间隔统计的接口出向吞吐率（Kbps）。
.1.3.6.1.4.1.7564.23.4.1.21	由该子层向更高（子）层传送的发往该子层的多播或的报文数量。
.1.3.6.1.4.1.7564.23.4.1.22	更高层协议要求传送的发往该子层多播地址的报文总数，包括丢弃的或没发出的报文。
.1.3.6.1.4.1.7564.23.4.1.23	由该子层向更高子层传送的发往该子层广播地址的报文数量。
.1.3.6.1.4.1.7564.23.4.1.24	更高层协议要求传送的发往该子层广播地址的报文总数，包括丢弃的或没发出的报文。
.1.3.6.1.4.1.7564.23.4.1.25	被选为要丢弃的、未向更高层协议层传送的出向报文的数量，即使这些报文未检测到错误。丢弃这样的报文的一个可能原因是为了释放缓存空间。
.1.3.6.1.4.1.7564.23.4.1.26	以 1,000,000 bits/s 为单位估算的接口当前带宽。对于带宽不变或者无法准确估算带宽的接口，该项应包含标称带宽。对于没有带宽概念的子层，该项 OID 值应为 0。
.1.3.6.1.4.1.7564.23.4.1.27	按照一定间隔统计的接口吞吐率（bits/s）。
.1.3.6.1.4.1.7564.23.4.1.28	按照一定间隔统计的接口每秒报文数（PPS）。
.1.3.6.1.4.1.7564.23.5	在所有活动接口上收到的累积八位字节总数的带宽，不包含 Loopback 接口。
.1.3.6.1.4.1.7564.23.6	在所有活动接口上发出的累积八位字节总数的带宽，不包含 Loopback 接口。
.1.3.6.1.4.1.7564.23.7	系统级别的每秒报文数。
.1.3.6.1.4.1.7564.23.8	入向整机每秒报文数（PPS）。
.1.3.6.1.4.1.7564.23.9	出向整机每秒报文数（PPS）。
.1.3.6.1.4.1.7564.23.10	按照一定间隔统计的整机吞吐率（bits/s）。
.1.3.6.1.4.1.7564.23.11	聚合接口统计信息表。表项数由聚合接口

	数量的值确定。
.1.3.6.1.4.1.7564.23.11.1	一个聚合接口统计表项。
.1.3.6.1.4.1.7564.23.11.1.1	每个聚合接口的唯一值。它的取值范围在 1 到聚合接口数的值之间。每个聚合接口的值，至少要从该实体的网络管理系统的一次重新初始化到下一次重新初始化之间，始终保持不变。
.1.3.6.1.4.1.7564.23.11.1.2	聚合接口名称。
.1.3.6.1.4.1.7564.23.11.1.3	聚合接口当前运行状态（开启或关闭）。
.1.3.6.1.4.1.7564.23.11.1.4	添加到聚合接口的接口。
.1.3.6.1.4.1.7564.23.11.1.5	聚合接口 IP 地址。
.1.3.6.1.4.1.7564.23.11.1.6	聚合接口 IPv4 地址的地址类型（应为 IPv4）。
.1.3.6.1.4.1.7564.23.11.1.7	聚合接口的 IPv4 地址。
.1.3.6.1.4.1.7564.23.11.1.8	聚合接口 IPv6 地址的地址类型（应为 IPv6）。
.1.3.6.1.4.1.7564.23.11.1.9	聚合接口的 IPv6 地址。
.1.3.6.1.4.1.7564.23.11.1.10	聚合接口收到的八位字节累计总数，包括帧字符。
.1.3.6.1.4.1.7564.23.11.1.11	由该子层向更高（子）层传送的，但不是发往该子层的多播、广播地址的聚合接口报文数量。
.1.3.6.1.4.1.7564.23.11.1.12	由该子层向更高（子）层传送的发往该子层的多播或广播地址的聚合接口报文数量。
.1.3.6.1.4.1.7564.23.11.1.13	被选为要丢弃的、未向更高协议层传送的聚合接口入向报文的数量，即使这些报文未检测到错误。丢弃这样的报文的一个可能原因是为了释放缓存空间。
.1.3.6.1.4.1.7564.23.11.1.14	对于面向报文的聚合接口，是指包含错误而未被传送到更高协议层的入向报文数量。对于面向字符或固定长度的聚合接口，是指包含错误而未被传送到更高协议层的入向传输单元的数量。
.1.3.6.1.4.1.7564.23.11.1.15	对于面向报文的聚合接口，是指通过该聚合接口接收，但是因为协议未知或不支持而被丢弃的报文数量。对于面向字符或固定长度的支持协议多路复用的聚合接口，是指通过该聚合接口接收，但是因为协议未知或不支持而被丢弃的报文数量。对于不支持协议多路复用的任何聚合接口，该计数器都始终为 0。

.1.3.6.1.4.1.7564.23.11.1.16	聚合接口传输出去的八位字节累计总数，包括帧字符。
.1.3.6.1.4.1.7564.23.11.1.17	更高层协议要求传送，但不是发往该子层多播或广播地址的报文总数，包括丢弃的或没发出的聚合接口报文。
.1.3.6.1.4.1.7564.23.11.1.18	更高层协议要求传送的发往该子层多播或广播地址的报文总数，包括丢弃的或没发出的聚合接口报文。
.1.3.6.1.4.1.7564.23.11.1.19	对于面向报文的聚合接口，是指因为错误而未传输的出向报文数量。对于面向字符或固定长度的聚合接口，是指因为错误而无法传送的传输单元数量。
.1.3.6.1.4.1.7564.23.11.1.20	按照一定间隔统计的聚合接口入向吞吐率（bits/s）。
.1.3.6.1.4.1.7564.23.11.1.21	按照一定间隔统计的聚合接口出向吞吐率（bits/s）。
.1.3.6.1.4.1.7564.23.11.1.22	由该子层向更高（子）层传送的发往该子层的多播地址的聚合接口报文数量。
.1.3.6.1.4.1.7564.23.11.1.23	更高层协议要求传送的发往该子层多播地址的报文总数，包括丢弃的或没发出的聚合接口报文。
.1.3.6.1.4.1.7564.23.11.1.24	由该子层向更高（子）层传送的发往该子层广播地址的聚合接口报文数量。
.1.3.6.1.4.1.7564.23.11.1.25	更高层协议要求传送的发往该子层广播地址的报文总数，包括丢弃的或没发出的聚合接口报文。
.1.3.6.1.4.1.7564.23.11.1.26	被选为要丢弃的、未向更高协议层传送的聚合接口出向报文的数量，即使这些报文未检测到错误。丢弃这样的报文的一个可能原因是为了释放缓存空间。
.1.3.6.1.4.1.7564.23.11.1.27	按照一定间隔统计的聚合接口吞吐率（bits/s）。
.1.3.6.1.4.1.7564.23.11.1.28	按照一定间隔统计的聚合接口每秒报文数（PPS）。
.1.3.6.1.4.1.7564.23.12	VLAN 接口统计信息表。表项数由 VLAN 接口数量的值确定。
.1.3.6.1.4.1.7564.23.12.1	一个 VLAN 接口统计表项。
.1.3.6.1.4.1.7564.23.12.1.1	每个 VLAN 接口的唯一值。它的取值范围在 1 到 VLAN 接口数的值之间。每个接口的值，至少要从该实体的网络管理系统的一次重新初始化到下一次重新初始化之间，始终保持不变。

.1.3.6.1.4.1.7564.23.12.1.2	VLAN 接口名称。
.1.3.6.1.4.1.7564.23.12.1.3	VLAN 接口当前运行状态（开启或关闭）。
.1.3.6.1.4.1.7564.23.12.1.4	VLAN 父接口名称。
.1.3.6.1.4.1.7564.23.12.1.5	VLAN 接口 IP 地址。
.1.3.6.1.4.1.7564.23.12.1.6	VLAN 接口 IPv4 地址的地址类型（应为 IPv4）。
.1.3.6.1.4.1.7564.23.12.1.7	VLAN 接口的 IPv4 地址。
.1.3.6.1.4.1.7564.23.12.1.8	VLAN 接口 IPv6 地址的地址类型（应为 IPv6）。
.1.3.6.1.4.1.7564.23.12.1.9	VLAN 接口的 IPv6 地址。
.1.3.6.1.4.1.7564.23.13	VXLAN 接口统计信息表。表项数由 VXLAN 接口数量的值确定。
.1.3.6.1.4.1.7564.23.13.1	一个 VXLAN 接口统计表项。
.1.3.6.1.4.1.7564.23.13.1.1	每个 VXLAN 接口的唯一值。它的取值范围在 1 到 VXLAN 接口数的值之间。每个 VXLAN 接口的值，至少要从该实体的网络管理系统的一次重新初始化到下一次重新初始化之间，始终保持不变。
.1.3.6.1.4.1.7564.23.13.1.2	VXLAN 接口名称。
.1.3.6.1.4.1.7564.23.13.1.3	VXLAN 接口当前运行状态（开启或关闭）。
.1.3.6.1.4.1.7564.23.13.1.4	VXLAN 绑定的 VXLAN 隧道。
.1.3.6.1.4.1.7564.23.13.1.5	VXLAN 接口 IP 地址。
.1.3.6.1.4.1.7564.23.13.1.6	VXLAN 接口 IPv4 地址的地址类型（应为 IPv4）。
.1.3.6.1.4.1.7564.23.13.1.7	VXLAN 接口的 IPv4 地址。
.1.3.6.1.4.1.7564.23.13.1.8	VXLAN 接口 IPv6 地址的地址类型（应为 IPv6）。
.1.3.6.1.4.1.7564.23.13.1.9	VXLAN 接口的 IPv6 地址。
.1.3.6.1.4.1.7564.24.1.1	已经发送的系统日志通知消息数量。这个数量可以包括因资源限制和/或无连接而被阻止传输的消息。对于通知接受者来说，可以定期轮询该对象以确定是否错过任何信息。如果是这样，则轮询历史日志表更恰当。
.1.3.6.1.4.1.7564.24.1.2	表示当设备生成系统日志时，是否发送相应的通知消息。禁用通知不能阻止系统日志被添加到历史日志表。
.1.3.6.1.4.1.7564.24.1.3	表示哪种严重性级别的系统日志会被处理。任何大于该严重性级别值的系统日志信息会被代理忽略。注意：数值越大严重性级别越低，例如 error (3)比 debug (7)严

	重性级别更高。
.1.3.6.1.4.1.7564.24.2.1	历史日志表可包含的表项数目上限。值为 0 会阻止任何历史日志被保存。当这个表满了，最早的表项将被删除，新的会被创建。
.1.3.6.1.4.1.7564.24.2.2	设备产生的系统日志信息表。所有需要关注的系统日志信息都会被输入到这个表（即严重性级别小于或等于日志最高严重性级别）。
.1.3.6.1.4.1.7564.24.2.2.1	设备之前生成的系统日志信息。每个表项为一个信息索引。
.1.3.6.1.4.1.7564.24.2.2.1.1	以索引信息为唯一目的的一个单调递增整数。当它达到最大值，代理会刷新表并将值置为 1。
.1.3.6.1.4.1.7564.24.2.2.1.2	消息严重性级别。
.1.3.6.1.4.1.7564.24.2.2.1.3	消息的文本。如果消息文本超过 255 位元组，消息将被截为 254 字节并附加一个“*”，表明该消息被截断。
.1.3.6.1.4.1.7564.24.3.1	当设备生成 syslogTrap 消息时，会触发一条 SNMP Trap 消息。可以通过 logNotifications Enabled 对象启用或禁用这些消息的发送。
.1.3.6.1.4.1.7564.25.1	ClickTCP 连接直接从 CLOSED 状态切换到 SYN-SENT 状态的次数。
.1.3.6.1.4.1.7564.25.2	ClickTCP 连接直接从 LISTEN 状态切换到 SYN-RCVD 状态的次数。
.1.3.6.1.4.1.7564.25.3	ClickTCP 连接直接从 SYN-SENT 或 SYN-RCVD 状态切换到 CLOSED 状态的次数，加上 TCP 连接直接从 SYN-RCVD 状态切换到 LISTEN 状态的次数。
.1.3.6.1.4.1.7564.25.4	ClickTCP 连接直接从 ESTABLISHED 状态或 CLOSE-WAIT 状态切换到 CLOSED 状态的次数。
.1.3.6.1.4.1.7564.25.5	当前状态是 ESTABLISHED 或 CLOSE-WAIT 的 ClickTCP 连接的数量。
.1.3.6.1.4.1.7564.25.6	所有收到的 ClickTCP 分段的总数，包括已收到的有错误的。该计数包括当前已建立连接上收到的分段。
.1.3.6.1.4.1.7564.25.7	所有发送的 ClickTCP 分段的总数，包括在当前的连接上发送的，但不包括那些只包含重发的八位字节。
.1.3.6.1.4.1.7564.25.8	重发的分段总数，即包含一个或多个先前

	发送的八位字节的 ClickTCP 分段的数量。
.1.3.6.1.4.1.7564.25.9	接收到的错误分段的总数（例如 ClickTCP 校验错误）。
.1.3.6.1.4.1.7564.25.10	发送的包含 RST 标签的 ClickTCP 分段数量。
.1.3.6.1.4.1.7564.25.11	包含 ClickTCP 连接特定信息的表。
.1.3.6.1.4.1.7564.25.11.1	ClickTCP 连接表中的一个概念行，包含一个当前 TCP 连接相关的信息。该表的每行很短，当连接转换到 CLOSED 状态后（或之后不久）它就不复存在了。
.1.3.6.1.4.1.7564.25.11.1.1	每个 ClickTCP 连接的唯一值。
.1.3.6.1.4.1.7564.25.11.1.2	该 TCP 连接的状态。
.1.3.6.1.4.1.7564.25.11.1.3	该 TCP 连接的本地 IP 地址。当一个连接处于 LISTEN 状态且愿意在该节点关联的任何 IP 接口接受连接时，使用 0.0.0.0。
.1.3.6.1.4.1.7564.25.11.1.4	该 TCP 连接的本地端口号。
.1.3.6.1.4.1.7564.25.11.1.5	该 TCP 连接的远程 IP 地址。
.1.3.6.1.4.1.7564.25.11.1.6	该 TCP 连接的远程端口号。
.1.3.6.1.4.1.7564.25.11.1.7	TCP 连接本地 IP 地址的类型。
.1.3.6.1.4.1.7564.25.11.1.8	该 TCP 连接的本地 IP 地址。当一个连接处于 LISTEN 状态且愿意在该节点关联的任何 IP 接口接受连接时，使用 0.0.0.0 或::。
.1.3.6.1.4.1.7564.25.11.1.9	TCP 连接远程 IP 地址的类型。
.1.3.6.1.4.1.7564.25.11.1.10	该 TCP 连接的远程 IP 地址。
.1.3.6.1.4.1.7564.27.1.1	正在被检查的后台服务的数量。
.1.3.6.1.4.1.7564.27.1.2	健康检查统计表。
.1.3.6.1.4.1.7564.27.1.2.1	包含一个后台服务健康检查统计信息的一个健康检查统计表项。
.1.3.6.1.4.1.7564.27.1.2.1.1	每个被检查的后台服务的引用索引。
.1.3.6.1.4.1.7564.27.1.2.1.2	后台服务的名称。
.1.3.6.1.4.1.7564.27.1.2.1.3	健康检查 IP 地址。
.1.3.6.1.4.1.7564.27.1.2.1.4	健康检查端口。
.1.3.6.1.4.1.7564.27.1.2.1.5	健康检查状态（Up 或 Down）。
.1.3.6.1.4.1.7564.27.1.2.1.6	健康检查被标识为 Up 或 Down 的原因。
.1.3.6.1.4.1.7564.27.1.2.1.7	健康检查为 Down 的次数。
.1.3.6.1.4.1.7564.27.1.2.1.8	健康检查为 Up 的次数。
.1.3.6.1.4.1.7564.27.1.2.1.9	连接尝试次数。
.1.3.6.1.4.1.7564.27.1.2.1.10	连接成功次数。
.1.3.6.1.4.1.7564.27.1.2.1.11	连接失败次数。
.1.3.6.1.4.1.7564.27.1.2.1.12	健康检查的 IP 地址的类型。
.1.3.6.1.4.1.7564.27.1.2.1.13	健康检查 IP 地址。

.1.3.6.1.4.1.7564.27.1.2.2	包含一个服务组成员的健康检查统计信息的一个健康检查统计表项。
.1.3.6.1.4.1.7564.27.1.2.2.1	每个被检查的服务组的引用索引。
.1.3.6.1.4.1.7564.27.1.2.2.2	服务组健康检查的后台服务名称。
.1.3.6.1.4.1.7564.27.1.2.2.3	服务组健康检查名称。
.1.3.6.1.4.1.7564.27.1.2.2.4	服务组健康检查 IP 地址。
.1.3.6.1.4.1.7564.27.1.2.2.5	服务组健康检查端口。
.1.3.6.1.4.1.7564.27.1.2.2.6	服务组健康检查状态（Up 或 Down）。
.1.3.6.1.4.1.7564.27.1.2.2.7	服务组健康检查被标识为 Up 或 Down 的原因。
.1.3.6.1.4.1.7564.27.1.2.2.8	服务组健康检查为 Down 的次数。
.1.3.6.1.4.1.7564.27.1.2.2.9	服务组健康检查为 Up 的次数。
.1.3.6.1.4.1.7564.27.1.2.2.10	服务组健康检查连接尝试次数。
.1.3.6.1.4.1.7564.27.1.2.2.11	服务组健康检查连接成功次数。
.1.3.6.1.4.1.7564.27.1.2.2.12	服务组健康检查连接失败次数。
.1.3.6.1.4.1.7564.27.1.2.2.13	服务组健康检查 IP 地址的类型。
.1.3.6.1.4.1.7564.27.1.2.2.14	服务组健康检查 IP 地址（十六进制值）。
.1.3.6.1.4.1.7564.27.1.2.3	包含一个 HTTP 被动健康检查统计信息的一个健康检查统计表项
.1.3.6.1.4.1.7564.27.1.2.3.1	每个被检查的后台服务的引用索引
.1.3.6.1.4.1.7564.27.1.2.3.2	HTTP 被动健康检查的后台服务名称
.1.3.6.1.4.1.7564.27.1.2.3.3	HTTP 被动健康检查的名称
.1.3.6.1.4.1.7564.27.1.2.3.4	HTTP 被动健康检查的后台服务 IP 地址
.1.3.6.1.4.1.7564.27.1.2.3.5	HTTP 类型被动健康检查的后台服务端口
.1.3.6.1.4.1.7564.27.1.2.3.6	HTTP 被动健康检查状态（Up 或 Down 或 Nottraffic）
.1.3.6.1.4.1.7564.27.1.2.3.7	HTTP 被动健康检查异常响应码
.1.3.6.1.4.1.7564.27.1.2.3.8	HTTP 被动健康检查响应超时时间
.1.3.6.1.4.1.7564.27.1.2.3.9	HTTP 被动健康检查统计周期
.1.3.6.1.4.1.7564.27.1.2.3.10	HTTP 被动健康检查异常响应阈值
.1.3.6.1.4.1.7564.27.1.2.3.11	HTTP 被动健康检 URL 列表
.1.3.6.1.4.1.7564.27.1.2.3.12	HTTP 被动健康检查 IP 地址类型
.1.3.6.1.4.1.7564.27.1.2.3.13	HTTP 被动健康检查异常响应统计量
.1.3.6.1.4.1.7564.27.1.2.3.14	HTTP 被动健康检查超时响应统计量
.1.3.6.1.4.1.7564.27.1.2.4	包含一个 TCP 被动健康检查统计信息的一个健康检查统计表项
.1.3.6.1.4.1.7564.27.1.2.4.1	每个被检查的后台服务的引用索引
.1.3.6.1.4.1.7564.27.1.2.4.2	TCP 被动健康检查的后台服务名称
.1.3.6.1.4.1.7564.27.1.2.4.3	TCP 被动健康检查的名称
.1.3.6.1.4.1.7564.27.1.2.4.4	TCP 被动健康检查的后台服务 IP 地址
.1.3.6.1.4.1.7564.27.1.2.4.5	TCP 被动健康检查的后台服务端口

.1.3.6.1.4.1.7564.27.1.2.4.6	TCP 被动健康检查状态（Up 或 Down 或 Nottraffic）
.1.3.6.1.4.1.7564.27.1.2.4.7	TCP 被动健康检查统计周期
.1.3.6.1.4.1.7564.27.1.2.4.8	TCP 被动健康检查 RST 包阈值
.1.3.6.1.4.1.7564.27.1.2.4.9	TCP 被动健康检查零窗口阈值
.1.3.6.1.4.1.7564.27.1.2.4.10	TCP 被动健康检查 IP 地址类型
.1.3.6.1.4.1.7564.27.1.2.4.11	TCP 被动健康检查 RST 包统计量
.1.3.6.1.4.1.7564.27.1.2.4.12	TCP 被动健康检查 ACK 包统计量
.1.3.6.1.4.1.7564.27.1.2.4.13	TCP 被动健康检查零窗口统计量
.1.3.6.1.4.1.7564.28.1	收到的字节总数。
.1.3.6.1.4.1.7564.28.2	发送的字节总数。
.1.3.6.1.4.1.7564.28.3	每秒收到的字节数。
.1.3.6.1.4.1.7564.28.4	每秒发送的字节数。
.1.3.6.1.4.1.7564.28.5	每秒收到的字节数峰值。
.1.3.6.1.4.1.7564.28.6	每秒发送的字节数峰值。
.1.3.6.1.4.1.7564.28.7	当前活动事务数。
.1.3.6.1.4.1.7564.30.1	当前 CPU 使用率百分比。
.1.3.6.1.4.1.7564.30.2	每秒连接数。
.1.3.6.1.4.1.7564.30.3	每秒请求数。
.1.3.6.1.4.1.7564.30.4	SSL 内核的当前使用率百分比。
.1.3.6.1.4.1.7564.30.5	压缩内核的当前使用率百分比。
.1.3.6.1.4.1.7564.30.6	已建立的 TCP 连接数。
.1.3.6.1.4.1.7564.30.7	所有 VIP 的出向吞吐率。
.1.3.6.1.4.1.7564.30.8	所有 VIP 的入向吞吐率。
.1.3.6.1.4.1.7564.30.9	H 系列 SSL 硬件的 SSL AE 内核的当前使用率百分比。
.1.3.6.1.4.1.7564.30.10	H 系列 SSL 硬件的 SSL SE 内核的当前使用率百分比。
.1.3.6.1.4.1.7564.30.11	每 5 分钟的 CPU 平均使用率百分比。
.1.3.6.1.4.1.7564.31.1	DNS 请求总数。
.1.3.6.1.4.1.7564.31.2	成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.3	失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.4	上一秒内 DNS 请求总数。
.1.3.6.1.4.1.7564.31.5	上一秒内成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.6	上一秒内失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.7	一秒内的 DNS 请求峰值。
.1.3.6.1.4.1.7564.31.8	一秒内成功的 DNS 解析峰值。
.1.3.6.1.4.1.7564.31.9	上一分钟内的 DNS 请求总数。
.1.3.6.1.4.1.7564.31.10	上一分钟内成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.11	上一分钟内失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.12	一分钟内的 DNS 请求峰值。

.1.3.6.1.4.1.7564.31.13	一分钟内成功的 DNS 解析峰值。
.1.3.6.1.4.1.7564.31.14	上一小时内的 DNS 请求总数。
.1.3.6.1.4.1.7564.31.15	上一小时内成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.16	上一小时内失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.17	一小时内的 DNS 请求峰值。
.1.3.6.1.4.1.7564.31.18	一小时内成功的 DNS 解析峰值。
.1.3.6.1.4.1.7564.31.19	前一天的 DNS 请求总数。
.1.3.6.1.4.1.7564.31.20	前一天成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.21	前一天失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.22	一天内的 DNS 请求峰值。
.1.3.6.1.4.1.7564.31.23	一天内成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.24	前 5 秒内的 DNS 请求总数。
.1.3.6.1.4.1.7564.31.25	前 5 秒内成功的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.26	前 5 秒内失败的 DNS 解析总数。
.1.3.6.1.4.1.7564.31.27	5 秒内 DNS 请求峰值。
.1.3.6.1.4.1.7564.31.28	5 秒内成功的 DNS 解析峰值。
.1.3.6.1.4.1.7564.32.1	CPU 和系统的当前温度。
.1.3.6.1.4.1.7564.32.2	当前风扇转速。
.1.3.6.1.4.1.7564.32.3	双电源当前状态，0 代表正常，1 代表有问题。
.1.3.6.1.4.1.7564.32.4	CPU1 风扇当前状态。
.1.3.6.1.4.1.7564.32.5	CPU2 风扇当前状态。
.1.3.6.1.4.1.7564.32.6	系统风扇 1 当前状态。
.1.3.6.1.4.1.7564.32.7	系统风扇 2 当前状态。
.1.3.6.1.4.1.7564.32.8	系统风扇 3 当前状态。
.1.3.6.1.4.1.7564.32.9	系统风扇 4 当前状态。
.1.3.6.1.4.1.7564.32.11	电源 1 当前状态，0 代表正常，1 代表有故障。
.1.3.6.1.4.1.7564.32.12	电源 2 当前状态，0 代表正常，1 代表有故障。
.1.3.6.1.4.1.7564.34.2.1	链路路由的数量。
.1.3.6.1.4.1.7564.34.2.2	链路路由状态表
.1.3.6.1.4.1.7564.34.2.2.1	包含一个链路状态信息的链路路由状态表项。
.1.3.6.1.4.1.7564.34.2.2.1.1	每个被检查的链路的引用索引。
.1.3.6.1.4.1.7564.34.2.2.1.2	链路路由名称。
.1.3.6.1.4.1.7564.34.2.2.1.3	链路路由网关。
.1.3.6.1.4.1.7564.34.2.2.1.4	链路路由状态。
.1.3.6.1.4.1.7564.34.2.2.1.5	链路路由响应时间。
.1.3.6.1.4.1.7564.34.2.2.1.6	链路路由 Up 的时间。
.1.3.6.1.4.1.7564.34.2.2.1.7	链路路由 Down 的时间。

.1.3.6.1.4.1.7564.34.2.2.1.8	链路路由 Down 的次数。
.1.3.6.1.4.1.7564.34.2.2.1.9	链路路由 Down 事件。
.1.3.6.1.4.1.7564.35.1.1.1	当前已配置的流量监听器的数量。
.1.3.6.1.4.1.7564.35.1.1.2	包含流量监听器配置的表。
.1.3.6.1.4.1.7564.35.1.1.2.1	包含一个流量监听器配置的表项。
.1.3.6.1.4.1.7564.35.1.1.2.1.1	流量监听器的引用索引。
.1.3.6.1.4.1.7564.35.1.1.2.1.2	流量监听器的名称。
.1.3.6.1.4.1.7564.35.1.1.2.1.3	流量监听器的部署模式。
.1.3.6.1.4.1.7564.35.1.1.2.1.4	流量监听器的 uplink 接口。
.1.3.6.1.4.1.7564.35.1.1.2.1.5	流量监听器的 downlink 接口。
.1.3.6.1.4.1.7564.35.1.2.1	当前已配置的 L2 安全设备的数量。
.1.3.6.1.4.1.7564.35.1.2.2	包含 L2 安全设备配置的表。
.1.3.6.1.4.1.7564.35.1.2.2.1	包含一个 L2 安全设备配置的表项。
.1.3.6.1.4.1.7564.35.1.2.2.1.1	L2 安全设备的引用索引。
.1.3.6.1.4.1.7564.35.1.2.2.1.2	L2 安全设备的名称。
.1.3.6.1.4.1.7564.35.1.2.2.1.3	L2 安全设备的 to_interface 接口名称。
.1.3.6.1.4.1.7564.35.1.2.2.1.4	L2 安全设备的 from_interface 接口名称。
.1.3.6.1.4.1.7564.35.1.3.1	当前已配置的 L3 安全设备的数量。
.1.3.6.1.4.1.7564.35.1.3.2	包含 L3 安全设备配置的表。
.1.3.6.1.4.1.7564.35.1.3.2.1	包含一个 L3 安全设备配置的表项。
.1.3.6.1.4.1.7564.35.1.3.2.1.1	L3 安全设备的引用索引。
.1.3.6.1.4.1.7564.35.1.3.2.1.2	L3 安全设备的名称。
.1.3.6.1.4.1.7564.35.1.3.2.1.3	L3 安全设备的 to_ip 地址。
.1.3.6.1.4.1.7564.35.1.3.2.1.4	L3 安全设备的 from_ip 地址。
.1.3.6.1.4.1.7564.35.1.4.1	当前已配置的 L4 安全设备的数量。
.1.3.6.1.4.1.7564.35.1.4.2	包含 L4 安全设备配置的表。
.1.3.6.1.4.1.7564.35.1.4.2.1	包含一个 L4 安全设备配置的表项。
.1.3.6.1.4.1.7564.35.1.4.2.1.1	L4 安全设备的引用索引。
.1.3.6.1.4.1.7564.35.1.4.2.1.2	L4 安全设备关联的 SLB 后台服务名称。
.1.3.6.1.4.1.7564.35.1.4.2.1.3	L4 安全设备的 from_ip 地址。
.1.3.6.1.4.1.7564.35.1.5.1	当前已配置的 L2 安全服务的数量。
.1.3.6.1.4.1.7564.35.1.5.2	包含 L2 安全服务配置的表。
.1.3.6.1.4.1.7564.35.1.5.2.1	包含一个 L2 安全服务配置的表项。
.1.3.6.1.4.1.7564.35.1.5.2.1.1	L2 安全服务的引用索引。
.1.3.6.1.4.1.7564.35.1.5.2.1.2	L2 安全服务的名称。
.1.3.6.1.4.1.7564.35.1.5.2.1.3	L2 安全服务不可用时所采取的行为。
.1.3.6.1.4.1.7564.35.1.5.2.1.4	L2 安全服务的负载均衡算法。
.1.3.6.1.4.1.7564.35.1.5.2.1.5	L2 安全服务中安全设备的个数。
.1.3.6.1.4.1.7564.35.1.5.2.1.6	L2 安全设备的名称。
.1.3.6.1.4.1.7564.35.1.6.1	当前已配置的 L3 安全服务的数量。
.1.3.6.1.4.1.7564.35.1.6.2	包含 L3 安全服务配置的表。

.1.3.6.1.4.1.7564.35.1.6.2.1	包含一个 L3 安全服务配置的表项。
.1.3.6.1.4.1.7564.35.1.6.2.1.1	L3 安全服务的引用索引。
.1.3.6.1.4.1.7564.35.1.6.2.1.2	L3 安全服务的名称。
.1.3.6.1.4.1.7564.35.1.6.2.1.3	L3 安全服务不可用时所采取的行为。
.1.3.6.1.4.1.7564.35.1.6.2.1.4	L3 安全服务的负载均衡算法。
.1.3.6.1.4.1.7564.35.1.6.2.1.5	L3 安全服务中安全设备的个数。
.1.3.6.1.4.1.7564.35.1.6.2.1.6	L3 安全设备的名称。
.1.3.6.1.4.1.7564.35.1.7.1	当前已配置的 L4 安全服务的数量。
.1.3.6.1.4.1.7564.35.1.7.2	包含 L4 安全服务配置的表。
.1.3.6.1.4.1.7564.35.1.7.2.1	包含一个 L4 安全服务配置的表项。
.1.3.6.1.4.1.7564.35.1.7.2.1.1	L4 安全服务的引用索引。
.1.3.6.1.4.1.7564.35.1.7.2.1.2	L4 安全服务关联的 SLB 虚拟服务名称。
.1.3.6.1.4.1.7564.35.1.8.1	当前已配置的 TAP 安全服务的数量。
.1.3.6.1.4.1.7564.35.1.8.2	包含 TAP 安全服务配置的表。
.1.3.6.1.4.1.7564.35.1.8.2.1	包含一个 TAP 安全服务配置的表项。
.1.3.6.1.4.1.7564.35.1.8.2.1.1	TAP 安全服务的引用索引。
.1.3.6.1.4.1.7564.35.1.8.2.1.2	TAP 安全服务的名称。
.1.3.6.1.4.1.7564.35.1.8.2.1.3	TAP 安全服务转发报文时使用的接口名称。
.1.3.6.1.4.1.7564.35.1.8.2.1.4	TAP 安全服务转发报文时的目的 MAC 地址。
.1.3.6.1.4.1.7564.35.1.9.1	当前已配置的安全服务链的数量。
.1.3.6.1.4.1.7564.35.1.9.2	包含安全服务链配置的表。
.1.3.6.1.4.1.7564.35.1.9.2.1	包含一个安全服务链配置的表项。
.1.3.6.1.4.1.7564.35.1.9.2.1.1	安全服务链的引用索引。
.1.3.6.1.4.1.7564.35.1.9.2.1.2	安全服务链的名称。
.1.3.6.1.4.1.7564.35.1.9.2.1.3	安全服务链的节点数。
.1.3.6.1.4.1.7564.35.1.9.2.1.4	安全服务链的节点名称。
.1.3.6.1.4.1.7564.35.2.1.1	L2/L3/L4 安全设备的统计表。
.1.3.6.1.4.1.7564.35.2.1.1.1	包含一个 L2/L3/L4 安全设备统计的表项。
.1.3.6.1.4.1.7564.35.2.1.1.1.1	安全设备的引用索引。
.1.3.6.1.4.1.7564.35.2.1.1.1.2	安全设备的类型（L2、L3 或 L4）。
.1.3.6.1.4.1.7564.35.2.1.1.1.3	安全设备的名称。
.1.3.6.1.4.1.7564.35.2.1.1.1.4	安全设备的健康状态（Up 或 Down）。
.1.3.6.1.4.1.7564.35.2.1.1.1.5	安全设备 to_device 接口 inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.1.1.1.6	安全设备 to_device 接口 inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.1.1.1.7	安全设备 to_device 接口 inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.1.1.1.8	安全设备 to_device 接口 inbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.1.1.1.9	安全设备 to_device 接口 outbound 方向总

	字节数。
.1.3.6.1.4.1.7564.35.2.1.1.1.10	安全设备 to_device 接口 outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.1.1.1.11	安全设备 to_device 接口 outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.1.1.1.12	安全设备 to_device 接口 outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.1.1.1.13	安全设备 from_device 接口 inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.1.1.1.14	安全设备 from_device 接口 inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.1.1.1.15	安全设备 from_device 接口 inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.1.1.1.16	安全设备 from_device 接口 inbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.1.1.1.17	安全设备 from_device 接口 outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.1.1.1.18	安全设备 from_device 接口 outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.1.1.1.19	安全设备 from_device 接口 outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.1.1.1.20	安全设备 from_device 接口 outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.2.1	L2/L3/L4 安全服务的统计表。
.1.3.6.1.4.1.7564.35.2.2.1.1	包含一个 L2/L3/L4 安全服务统计的表项。
.1.3.6.1.4.1.7564.35.2.2.1.1.1	安全服务的引用索引。
.1.3.6.1.4.1.7564.35.2.2.1.1.2	安全服务的类型（L2、L3 或 L4）。
.1.3.6.1.4.1.7564.35.2.2.1.1.3	安全服务的名称。
.1.3.6.1.4.1.7564.35.2.2.1.1.4	安全服务的健康状态。
.1.3.6.1.4.1.7564.35.2.2.1.1.5	安全服务 to_device 接口 inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.2.1.1.6	安全服务 to_device 接口 inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.2.1.1.7	安全服务 to_device 接口 inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.2.1.1.8	安全服务 to_device 接口 inbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.2.1.1.9	安全服务 to_device 接口 outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.2.1.1.10	安全服务 to_device 接口 outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.2.1.1.11	安全服务 to_device 接口 outbound 方向总包数。

.1.3.6.1.4.1.7564.35.2.2.1.1.12	安全服务 to_device 接口 outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.2.1.1.13	安全服务 from_device 接口 inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.2.1.1.14	安全服务 from_device 接口 inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.2.1.1.15	安全服务 from_device 接口 inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.2.1.1.16	安全服务 from_device 接口 inbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.2.1.1.17	安全服务 from_device 接口 outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.2.1.1.18	安全服务 from_device 接口 outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.2.1.1.19	安全服务 from_device 接口 outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.2.1.1.20	安全服务 from_device 接口 outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.2.1.1.21	安全服务 to_device 接口的 deny 包数。
.1.3.6.1.4.1.7564.35.2.2.1.1.22	安全服务 from_device 接口的 deny 包数。
.1.3.6.1.4.1.7564.35.2.3.1	TAP 安全服务的统计表。
.1.3.6.1.4.1.7564.35.2.3.1.1	包含一个 TAP 安全服务统计的表项。
.1.3.6.1.4.1.7564.35.2.3.1.1.1	TAP 安全服务的引用索引。
.1.3.6.1.4.1.7564.35.2.3.1.1.2	TAP 安全服务的名称。
.1.3.6.1.4.1.7564.35.2.3.1.1.3	TAP 安全服务 to_device 接口 outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.3.1.1.4	TAP 安全服务 to_device 接口 outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.3.1.1.5	TAP 安全服务 to_device 接口 outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.3.1.1.6	TAP 安全服务 to_device 接口 outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.4.1	安全服务链的统计表。
.1.3.6.1.4.1.7564.35.2.4.1.1	包含一个安全服务链统计的表项。
.1.3.6.1.4.1.7564.35.2.4.1.1.1	安全服务链的引用索引。
.1.3.6.1.4.1.7564.35.2.4.1.1.2	安全服务链的名称。
.1.3.6.1.4.1.7564.35.2.4.1.1.3	安全服务链的健康状态。
.1.3.6.1.4.1.7564.35.2.4.1.1.4	安全服务链 uplink inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.5	安全服务链 uplink inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.4.1.1.6	安全服务链 uplink inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.4.1.1.7	安全服务链 uplink inbound 方向 pps。

.1.3.6.1.4.1.7564.35.2.4.1.1.8	安全服务链 uplink outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.9	安全服务链 uplink outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.4.1.1.10	安全服务链 uplink outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.4.1.1.11	安全服务链 uplink outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.4.1.1.12	安全服务链 uplink 方向的 deny 总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.13	安全服务链 uplink 方向的 deny 总包数。
.1.3.6.1.4.1.7564.35.2.4.1.1.14	安全服务链 downlink inbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.15	安全服务链 downlink inbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.4.1.1.16	安全服务链 downlink inbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.4.1.1.17	安全服务链 downlink inbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.4.1.1.18	安全服务链 downlink outbound 方向总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.19	安全服务链 downlink outbound 方向 bps。
.1.3.6.1.4.1.7564.35.2.4.1.1.20	安全服务链 downlink outbound 方向总包数。
.1.3.6.1.4.1.7564.35.2.4.1.1.21	安全服务链 downlink outbound 方向 pps。
.1.3.6.1.4.1.7564.35.2.4.1.1.22	安全服务链 downlink 方向的 deny 总字节数。
.1.3.6.1.4.1.7564.35.2.4.1.1.23	安全服务链 downlink 方向的 deny 总包数。
.1.3.6.1.4.1.7564.35.2.5.1	deny 类型安全策略的统计表。
.1.3.6.1.4.1.7564.35.2.5.1.1	包含一个 deny 类型安全策略统计的表项。
.1.3.6.1.4.1.7564.35.2.5.1.1.1	deny 类型安全策略的引用索引。
.1.3.6.1.4.1.7564.35.2.5.1.1.2	deny 类型安全策略的名称。
.1.3.6.1.4.1.7564.35.2.5.1.1.3	安全策略 to 方向的 deny 总字节数。
.1.3.6.1.4.1.7564.35.2.5.1.1.4	安全策略 to 方向的 deny 总包数。
.1.3.6.1.4.1.7564.35.2.5.1.1.5	安全策略 from 方向的 deny 总字节数。
.1.3.6.1.4.1.7564.35.2.5.1.1.6	安全策略 from 方向的 deny 总包数。
.1.3.6.1.4.1.7564.36.2.1.1	当前已创建的分区数量。
.1.3.6.1.4.1.7564.36.2.1.2	包含分区成员配置的表。
.1.3.6.1.4.1.7564.36.2.1.2.1	包含一个分区信息的表项。
.1.3.6.1.4.1.7564.36.2.1.2.1.1	每个分区的引用索引。
.1.3.6.1.4.1.7564.36.2.1.2.1.2	分区名称。
.1.3.6.1.4.1.7564.36.2.1.2.1.3	分区每秒新建连接数。
.1.3.6.1.4.1.7564.36.2.1.2.1.4	分区当前连接数。
.1.3.6.1.4.1.7564.36.2.1.2.1.5	按照一定时间间隔统计的分区出向吞吐率（KB/s）。
.1.3.6.1.4.1.7564.36.2.1.2.1.6	按照一定时间间隔统计的分区入向吞吐率（KB/s）。

.1.3.6.1.4.1.7564.251.1	代理启动时，该 Trap 会被发送。
.1.3.6.1.4.1.7564.251.2	代理终止时，该 Trap 会被发送。
.1.3.6.1.4.1.7564.251.3	许可剩余天数。
.1.3.6.1.4.1.7564.251.4	当一个电源发生故障时，该 Trap 会被发送。
.1.3.6.1.4.1.7564.251.5	当故障电源恢复时，该 Trap 会被发送。
.1.3.6.1.4.1.7564.251.6	Webroot 许可剩余天数。
Float	单精度浮点数。语义和编码与 IEEE 标准 ANSI/IEEE Std 754-1985 中对 Single 类型的二进制浮点的定义相同。取值仅限于以下 ASN.1 类型的 BER 序列格式： FLOATTYPE ::= [120] IMPLICIT FloatType（注意：取值 120 是'30'h 和'48'h 的总和）。此类型取值的 BER 序列的 Length 必须为定长、短型编码。例如，取值为 123 类型为 FLOATTYPE 的 BER 序列为'9f780442f60000'h（Tag 是'9f78'h；Length 是'04'h；Value 是'42f60000'h。）。 取值为'9f780442f60000'h 数据类型为 Opaque 的 BER 序列为'44079f780442f60000'h。（Tag 是'44'h；Length 是'07'h；Value 是'9f780442f60000'h。）。
Syslogseverity	系统日志消息的严重性级别。枚举值等于系统日志的级别+1。例如，emergency 级别的系统日志的值是 0。

附录二 功能规格

流量编排功能规格

规格	内存			
	<4G	≥4G	≥32G	≥128G
流量监听器数量	0	4	4	4
安全设备数量	0	64	128	256
安全服务数量	0	16	32	64
安全服务链数量	0	32	64	128
安全服务链成员总数量	0	128	256	512
网络流量编排规则数量	0	128	256	512
编排策略数量	0	64	128	256
网络流量编排规则关联到编排策略的总数量	0	512	1024	2048

相关保持算法的动态会话条目规格

相关保持算法可创建的动态会话条目规格取决于系统内存的大小，如下表所示（实际数值可能因为内存的使用情况而有变动）：

• 系统内存	• 相关保持算法的动态会话条目规格
1 GB	512
2 GB	75*1024
4 GB	300*1024
8 GB	1024*1024
16 GB	4*1024*1024
24 GB	4*1024*1024
32 GB	20*1024*1024
64 GB	20*1024*1024
96 GB	30*1024*1024
≥128 GB	40*1024*1024



注意：

- 相关保持算法包括 sipcidps、sipuidps、radpsun、persistence 和 diametersid。
- 当动态会话条目数量达到记录上限后，系统将无法建立新的动态会话条目进行会话保持。

全局服务器负载均衡功能规格

规格	内存				
	<8G	≥8G	≥16G	≥32G	≥64G
SDNS 数据中心数量	64	64	64	64	64
SDNS 服务 IP 数量	10,000	50,000	100,000	200,000	500,000
SDNS 服务池数量	10,000	50,000	100,000	200,000	500,000
SDNS 链路数量	1,024	1,024	1,024	1,024	1,024
SDNS 域名数量	2,500	5,000	10,000	20,000	40,000
SDNS 区域数量	1,000	2,000	4,000	8,000	16,000
SDNS 就近性规则数量	100,000	500,000	1,000,000	2,000,000	4,000,000
SDNS 健康检查模版数量	500	1,000	2,000	4,000	8,000
SDNS 健康检查实例数量	10,000	20,000	40,000	80,000	160,000