目 录

1 Flow 日志

1.1 Flow日志配置命令

1.1.1 display userlog export

display userlog export 命令用来查看输出到日志主机的 Flow 日志的配置和统计信息。

【命令】

display userlog export

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

查看输出到日志主机的 Flow 日志的配置和统计信息。

```
<Sysname> display userlog export
Flow:
  Export flow log as UDP Packet.
  Version: 3.0
  Source ipv4 address: 2.2.2.2
  Source ipv6 address:
  Log load balance function: Disabled
  Local time stamp: Disabled
  Number of log hosts: 2

  Log host 1:
    Host/Port: 1.2.3.6/2000
    Total logs/UDP packets exported: 112/87

  Log host 2:
    VPN instance:abc
    Host/Port:1.1.1.1/2000
    Total logs/UDP packets exported: 6553665536/409597846
```

表1-1 display userlog export 命令显示信息描述表

字段	描述
Flow	表示该段显示的是Flow日志的相关配置和统计信息
Export flow log as UDP Packet	表示Flow日志按照封装成UDP报文的方式发送
Version	Flow日志的版本号

字段	描述
Source ipv4/ipv6 address	Flow日志UDP报文的源IP地址
Log load balancing function	Flow日志UDP报文负载分担功能是否使能： • Enabled：使能 • Disabled：未使能
Local time stamp	Flow日志的时间戳是否使用本地时间： • Enabled：使能 • Disabled：未使能
Number of log hosts	已配置的Flow日志主机数量
Log host 1	日志主机1的相关信息
VPN instance	（暂不支持）Flow日志主机所属的VPN
Host/port	Flow日志主机的IP地址和端口号
Total logs	Flow日志的总数
UDP packets exported	Flow日志的UDP报文总数，一条UDP报文中可能含有多条Flow日志

【相关命令】

- **userlog flow export**

1.1.2 display userlog host-group

display userlog host-group 命令用来显示 Flow 日志主机组的信息。

【命令】

display userlog host-group [**ipv6**] [*host-group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ipv6：显示 IPv6 日志主机组信息。如果不指定该参数，则显示 IPv4 日志主机组信息。

host-group-name：日志主机组的名称，为 1～63 个字符的字符串，区分大小写。如果不指定 *host-group-name* 参数，则显示所有 IP 类型的日志主机组。

【举例】

显示 IPv4 Flow 日志主机组 test 的信息。

```
<Sysname> display userlog host-group test
Userlog host-group test:
  ACL number: 2000
```

```
  Flow log host numbers: 1

    Log host 1:
      VPN-instance: test
      Host/port: 1.1.1.2/2000
```

显示所有 IPv4 日志主机组的信息。

```
<Sysname> display userlog host-group
There are 2 IPv4 host groups.

Userlog host-group test:
  ACL number: 2000

  Flow log host numbers: 1

    Log host 1:
      VPN-instance: test
      Host/Port: 1.2.3.6/0

Userlog host-group test2:
  ACL name: test

  Flow log host numbers: 1

    Log host 1:
      Host/Port: 1.1.1.1/0
```

表1-2 **display userlog host-group** 命令显示信息描述表

字段	描述
Userlog host-group test	日志主机组的信息
ACL number/ACL name	日志主机组匹配的ACL的信息
Flow log host numbers	Flow日志主机的数量
Log host	Flow日志主机的信息
VPN-instance	（暂不支持）Flow日志主机所属的VPN，如果没有配置，则不显示该字段
Host/Port	Flow日志主机的IP地址和端口号

【相关命令】

- **userlog host-group**
- **userlog host-group host flow**

1.1.3 reset userlog flow export

reset userlog flow export 命令用来清除 Flow 日志的统计信息。

【命令】

reset userlog flow export

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 Flow 日志的统计信息。

```
<Sysname> reset userlog flow export
```

【相关命令】

- **userlog flow export**

1.1.4 userlog flow export host

userlog flow export host 命令用来配置 Flow 日志主机地址和 UDP 端口号。

undo userlog flow export host 命令用来删除 Flow 日志主机配置。

【命令】

userlog flow export host { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } **port** *udp-port*

undo userlog flow export host { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

【缺省情况】

未配置 Flow 日志主机的 IP 地址和 UDP 端口号。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

hostname：指定 Flow 日志主机名，为 1～253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv4-address：指定 Flow 日志主机的 IPv4 地址，取值范围是合法的单播 IPv4 地址，且不能是环回地址。

ipv6 *ipv6-address*：指定 Flow 日志主机的 IPv6 地址。

port *udp-port*：指定 Flow 日志主机的 UDP 端口号，*udp-port* 取值范围为 1～65535，为了避免与通用的 UDP 端口号冲突，建议使用 1025～65535 的 UDP 端口号。

【举例】

将 Flow 日志信息发送给 Flow 日志主机，Flow 日志主机的地址为 1.2.3.6，对应 UDP 端口号为 2000。

```
<Sysname> system-view
```

```
[Sysname] userlog flow export host 1.2.3.6 port 2000
```

【相关命令】

- **display userlog export**

1.1.5 userlog flow export load-balancing

userlog flow export load-balancing 命令用来配置 Flow 日志按照负载分担方式输出到日志主机。

undo userlog flow export load-balancing 命令用来恢复缺省情况。

【命令】

userlog flow export load-balancing

undo userlog flow export load-balancing

【缺省情况】

每一条 Flow 日志复制发送给所有已配置的 Flow 日志主机。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

配置了 Flow 日志负载分担功能以后，一条 Flow 日志仅仅会发送到用户配置的所有日志主机中的某一台特定的日志主机。

Flow 日志按照会话源 IP 进行负载分担。在不改变配置的前提下，源 IP 固定的会话对应的 Flow 日志始终发送到固定的一台日志主机。

如果配置的日志主机不可达时，日志主机仍会参与 Flow 日志的负载分担，但负载分担到不可达的日志主机的 Flow 日志会直接被丢弃。

【举例】

设置 Flow 日志负载分担发送。

```
<Sysname> system-view
[Sysname] userlog flow export load-balancing
```

【相关命令】

- **userlog flow export host**

1.1.6 userlog flow export source-ip

userlog flow export source-ip 命令用来配置 Flow 日志报文的源地址。

undo userlog flow export source-ip 命令用来恢复缺省情况。

【命令】

userlog flow export source-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo userlog flow export source-ip [**ipv6**]

【缺省情况】

Flow 日志报文的源地址为发送该报文的接口的 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：Flow 日志报文的源 IPv4 地址。

ipv6 *ipv6-address*：Flow 日志报文的源 IPv6 地址。

【举例】

将 1.2.1.2 配置为 Flow 日志报文的源地址。

```
<Sysname> system-view
[Sysname] userlog flow export source-ip 1.2.1.2
```

【相关命令】

- **userlog flow export host**

1.1.7 userlog flow export timestamp localtime

userlog flow export timestamp localtime 命令用来配置 Flow 日志的时间戳使用本地时间。

undo userlog flow export timestamp localtime 命令用来恢复缺省情况。

【命令】

userlog flow export timestamp localtime

undo userlog flow export timestamp localtime

【缺省情况】

Flow 日志的时间戳使用 UTC 时间。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

Flow 日志的时间戳可以使用 UTC 时间和本地时间，其中：

- UTC 时间指的是标准的格林威治时间。
- 本地时间指的是格林威治时间加上时区偏移的时间。用户可以使用命令 **clock timezone** 来配置需要偏移的时间。关于命令 **clock timezone** 的详细介绍，请参见“设备管理命令参考”中的“设备管理”。

【举例】

配置 Flow 日志的时间戳使用本地时间。

```
<Sysname> system-view
[Sysname] userlog flow export timestamp localtime
```

1.1.8 userlog flow export version

userlog flow export version 命令用来配置 Flow 日志报文的版本号。

undo userlog flow export version 命令用来恢复缺省情况。

【命令】

userlog flow export version *version-number*

undo userlog flow export version

【缺省情况】

Flow 日志报文的版本号为 1.0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

version-number：Flow 日志报文的版本号，取值为 1、3 或 5，分别对应 Flow1.0、Flow3.0 和 Flow5.0。

【使用指导】

同一时刻只能使用一个版本，如果多次执行本命令，最后一次执行的命令生效。

【举例】

将 Flow 日志报文版本号设为 3.0。

```
<Sysname> system-view
[Sysname] userlog flow export version 3
```

【相关命令】

- **userlog flow export host**

1.1.9 userlog flow syslog

userlog flow syslog 命令用来配置 Flow 日志输出到信息中心。

undo userlog flow syslog 命令用来恢复缺省情况。

【命令】

userlog flow syslog

undo userlog flow syslog

【缺省情况】

Flow 日志不输出。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

日志主机和信息中心两种输出方向互斥，默认输出方向为日志主机。如果配置了信息中心方向，则会忽略日志主机方向。

通常情况下，用户访问网络会在短时间内产生大量 NAT 会话日志。系统日志传输格式为 ASCII 码，相比 Flow 日志的二进制格式传输效率低。所以，建议在日志量较小的情况下，使用输出到信心中心的方式。

日志输出至信息中心时，日志信息的优先级为 informational，即作为设备的一般提示信息。

【举例】

设置 Flow 日志输出到信息中心。

```
<Sysname> system-view
[Sysname] userlog flow syslog
```

【相关命令】

- **userlog flow export host**

1.1.10 userlog host-group

userlog host-group 命令用来创建 Flow 日志主机组，并进入 Flow 日志主机组视图。如果指定的主机组已存在，则直接进入该主机组视图。

undo userlog host-group 命令用来删除指定的 Flow 日志主机组。

【命令】

userlog host-group [**ipv6**] *host-group-name* **acl** { **name** *acl-name* | **number** *acl-number* }

undo userlog host-group [**ipv6**] *host-group-name*

【缺省情况】

不存在 Flow 日志主机组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6：配置 IPv6 日志主机组。如果不指定该参数，则表示配置的是 IPv4 日志主机组。

host-group-name：日志主机组的名称，为 1～63 个字符的字符串，区分大小写。

acl：指定用来匹配 Flow 日志信息的 IPv4 ACL 或 IPv6 ACL。如果日志信息匹配该 ACL，则 Flow 日志发送到该日志主机组中的日志主机。

name *acl-name*：指定 ACL 的名称，*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头，为避免混淆，ACL 的名称不允许使用英文单词 all。

number *acl-number*：指定 ACL 的编号，*acl-number* 表示 ACL 的编号，取值范围为 2000～3999。

【使用指导】

为了方便用户从大量日志中获取特定日志信息，同时降低设备发送和处理日志的压力，可以通过配置 Flow 日志主机组对发往日志主机的日志进行过滤。

请合理规划 ACL 的规则，使 Flow 日志能够按照需求发送到指定的日志主机组。如果 Flow 日志匹配了多个日志主机组，则按照日志主机组的名称字母序选择最先匹配上的日志主机组。

如果 Flow 日志主机组配置中引用的 ACL 不存在或者没有规则，则该日志主机组不生效。

【举例】

创建 IPv4 Flow 日志主机组，名称为 test，匹配 Flow 日志信息的 ACL 编号为 2000。

```
<Sysname> system-view
[Sysname] userlog host-group test acl number 2000
[Sysname-userlog-host-group-test]
```

【相关命令】

- **display userlog host-group**
- **userlog host-group host flow**

1.1.11 userlog host-group host flow

userlog host-group host flow 命令用来向 Flow 日志主机组中添加日志主机。

undo userlog host-group host flow 命令用来删除 Flow 日志主机组中的日志主机。

【命令】

IPv4 Flow 日志主机组视图：

userlog host-group host flow { *hostname* | *ipv4-address* }

undo userlog host-group host flow { *hostname* | *ipv4-address* }

IPv6 Flow 日志主机组视图：

userlog host-group host flow ipv6 { *hostname* | *ipv6-address* }

undo userlog host-group host flow ipv6 { *hostname* | *ipv6-address* }

【缺省情况】

Flow 日志主机组中不存在日志主机。

【视图】

IPv4 Flow 日志主机组视图

IPv6 Flow 日志主机组视图

【缺省用户角色】

network-admin

【参数】

hostname：指定 Flow 日志主机名，为 1～253 个字符的字符串，不区分大小写，字符串中只能包含字母、数字、“-”、“_”和“.”。

ipv4-address：指定 Flow 日志主机的 IPv4 地址，取值范围是合法的单播 IPv4 地址，且不能是环回地址。

ipv6 *ipv6-address*：指定 Flow 日志主机的 IPv6 地址，取值范围是合法的单播 IPv6 地址，且不能是环回地址或全 0 地址。

【使用指导】

一个 Flow 日志主机组中可以添加多台日志主机，一个日志主机也可以同时添加到多个 Flow 日志主机组中。

向 Flow 日志主机组添加的日志主机必须是通过 **userlog flow export host** 命令配置的日志主机，否则该日志主机不生效。

【举例】

创建名称为 test 的 IPv4 Flow 日志主机组，并将 IP 地址为 1.2.3.6 的 Flow 日志主机添加到该日志主机组中。

```
<Sysname> system-view
[Sysname] userlog host-group test acl number 2000
[Sysname-userlog-host-group-test] userlog host-group host flow 1.2.3.6
```

【相关命令】

- **display userlog host-group**
- **userlog flow export host**
- **userlog host-group**