# 目 录

# 1 SNMP

## 1.1 SNMP配置命令

SNMP 告警信息包括 SNMP Trap 和 Inform 报文，用来告知 NMS 设备上发生了重要事件，比如，用户的登录/退出，接口状态变成 up/down 等。如无特殊说明，本文中的告警信息均指 Trap 和 Inform 两种信息。

### 1.1.1 display snmp-agent community

**display snmp-agent community** 命令用来显示 SNMPv1 或 SNMPv2c 的团体信息。

【命令】

**display snmp-agent community** [ **read** | **write** ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**read**：显示只读访问权限的团体信息。

**write**：显示读写访问权限的团体信息。

【使用指导】

不带参数时，显示所有 SNMP 团体的信息。

用户有两种方式创建团体：

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user** { **v1** | **v2c** }和 **snmp-agent group** { **v1** | **v2c** }命令成功创建 SNMPv1 或 SNMPv2c 用户以及相应的组后，系统会以用户名为团体名自动创建一个团体。

**display snmp-agent community** 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

【举例】

# 显示设备当前所有已配置的团体信息。

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1
```

```
Community name: bb
    Role name: bb
    Storage-type: nonVolatile

Community name: userv1
    Group name: testv1
    Storage-type: nonVolatile

Community name: cc
    Group name: cc
    ACL name: testacl
    Storage-type: nonVolatile
```

表1-1 display snmp-agent community 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Community name | 团体名：<br>• 如果团体名是通过 **snmp-agent community** 命令创建的，则显示的是团体名<br>• 如果团体名是通过 **snmp-agent usm-user { v1 \| v2c }**命令创建的，则显示的是用户名 |
| Group name | 组名：<br>• 如果团体名是通过 **snmp-agent community** 命令的 VACM 方式创建的，则组名和团体名相同<br>• 如果团体名是通过 **snmp-agent usm-user { v1 \| v2c }**命令创建的，则显示用户所在的组名 |
| Role name | SNMP用户所在团体绑定的角色名：<br>通过**snmp-agent community**命令的RBAC方式创建的团体名可绑定用户角色 |
| ACL | 使用的ACL列表的编号（该字段仅在团体名与ACL绑定后显示，不会与ACL name同时存在） |
| ACL name | 使用的ACL列表的名称（该字段仅在团体名与ACL名称绑定后显示，不会与ACL同时存在） |
| Storage-type | 表示存储方式，分为以下几种：<br>• volatile：重启后信息丢失<br>• nonVolatile：重启后信息仍保存<br>• permanent：重启后信息仍保存，允许更改，但不许删除<br>• readOnly：重启后信息仍保存，既不允许更改，也不许删除<br>• other：其他 |
| Context name | SNMP上下文：<br>• 如果此团体名配置了对应的上下文映射，则显示对应的上下文<br>• 如果此团体名未配置对应的上下文映射，该字段显示为空 |

【相关命令】

- **snmp-agent community**
- **snmp-agent usm-user { v1 | v2c }**

### 1.1.2 display snmp-agent context

**display snmp-agent context** 命令用来显示 SNMP 上下文。

【命令】

**display snmp-agent context** [ *context-name* ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

*context-name*：显示指定的 SNMP 上下文，为 1～32 个字符的字符串，区分大小写。不指定该参数时，显示设备上所有已创建的 SNMP 上下文。

【举例】

# 显示设备上所有已创建的 SNMP 上下文。

```
<Sysname> display snmp-agent context
   testcontext
```

【相关命令】

- **snmp-agent context**

### 1.1.3 display snmp-agent group

**display snmp-agent group** 命令用来显示 SNMP 组信息。

【命令】

**display snmp-agent group** [ *group-name* ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

*group-name*：指定要显示信息的 SNMPv1、SNMPv2c 或 SNMPv3 组的名称。取值范围为 1～32 个字符的字符串，区分大小写。不指定该参数时，显示设备上所有已创建的 SNMP 组的信息。

【举例】

# 显示所有 SNMP 组的信息。

```
<Sysname> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
```

```
Notifyview: <no specified>
Storage-type: nonVolatile
ACL name: testacl
```

表1-2 display snmp-agent group 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Group name | SNMP组名 |
| Security model | SNMP组配置的安全模式，包括版本信息和安全模式，以空格分隔：<br>• 对于 SNMPv1 和 SNMPv2c 版本，认证加密级别只能为 noAuthNoPriv（无认证无加密）<br>• 对于 SNMPv3 版本，安全模式分为三种：authPriv（既认证又加密）、authNoPriv（只认证不加密）、noAuthNoPriv（不认证不加密） |
| Readview | SNMP组对应的只读的MIB视图名 |
| Writeview | SNMP组对应的可写的MIB视图名 |
| Notifyview | SNMP组对应的可以发Trap和Inform报文的MIB视图名 |
| Storage-type | 存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体描述请参见表1-1 |
| ACL | 使用的IPv4 ACL列表的编号（该字段仅在SNMP组与IPv4 ACL绑定后显示，不会与ACL name同时存在） |
| IPV6 ACL | 使用的IPv6 ACL列表的编号（该字段仅在SNMP组与IPv6 ACL绑定后显示，不会与ACL name同时存在） |
| ACL name | 使用的ACL列表的名称（该字段仅在SNMP组与ACL名称绑定后显示，不会与ACL同时存在） |

【相关命令】

- **snmp-agent group**

### 1.1.4 display snmp-agent local-engineid

**display snmp-agent local-engineid** 命令用来显示本设备的 SNMP 引擎 ID。

【命令】

**display snmp-agent local-engineid**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

SNMP 引擎 ID 是 SNMP 实体的唯一标识，它在一个 SNMP 管理域内是唯一的。SNMP 引擎是 SNMP 实体的重要组成部分，完成 SNMP 信息的信息调度、信息处理、安全验证、访问控制等功能。

【举例】

# 显示本设备的 SNMP 引擎 ID。

```
<Sysname> display snmp-agent local-engineid
   SNMP local engine ID: 800063A2800084E52BED7900000001
```

【相关命令】

- **snmp-agent local-engineid**

### 1.1.5 display snmp-agent mib-node

**display snmp-agent mib-node** 命令用来显示 SNMP 支持的 MIB 节点信息。

【命令】

**display snmp-agent mib-node** [ **details** | **index-node** | **trap-node** | **verbose** ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**details**：表示显示 SNMP 支持的 MIB 节点细节信息，包括节点名、OID 末位、下一个叶子节点名。

**index-node**：显示 SNMP 支持的 MIB 表、节点名及索引节点 OID。

**trap-node**：显示 SNMP 支持的 MIB 告警节点名及对应的 OID、告警绑定变量节点名及对应的 OID。

**verbose**：显示 SNMP 支持的 MIB 节点详细信息，包括节点名、OID、节点类型、访问权限、数据类型，对应 MOR（Managed Object Repository，管理对象库）定义、父子兄弟节点信息等。

【使用指导】

未指定任何参数时，显示 SNMP 支持的 MIB 节点信息，包括节点名、OID 和节点访问权限。

特性包中可以包含不同的 MIB 插件，设备根据加载特性包的不同，支持的 MIB 不相同。

【举例】

# 显示 SNMP 支持 MIB 节点信息。

```
<Sysname> display snmp-agent mib-node

iso<1>(NA)
  |-std<1.0>(NA)
   |-iso8802<1.0.8802>(NA)
    |-ieee802dot1<1.0.8802.1>(NA)
     |-ieee802dot1mibs<1.0.8802.1.1>(NA)
```

其它显示信息略……

表1-3 display snmp-agent mib-node 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| -std | MIB节点名 |
| <1.0> | MIB节点对应的OID |

| 字段 | 描述 |
| --- | --- |
| (NA) | MIB节点访问权限，取值为：<br>• NA：表示节点不可访问<br>• NF：表示节点支持告警<br>• RO：表示节点支持只读访问<br>• RW：表示节点支持读写访问<br>• RC：表示节点支持读写创建访问<br>• WO：表示节点支持只写访问 |
| * | 表示叶子节点或表节点 |

# 显示 SNMP 支持 MIB 节点细节信息。

```
<Sysname> display snmp-agent mib-node details

 iso(1)(dot1xPaeSystemAuthControl)
  |-std(0)(dot1xPaeSystemAuthControl)
   |-iso8802(8802)(dot1xPaeSystemAuthControl)
    |-ieee802dot1(1)(dot1xPaeSystemAuthControl)
     |-ieee802dot1mibs(1)(dot1xPaeSystemAuthControl)
```

其它显示信息略……

表1-4 display snmp-agent mib-node details 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| -std | MIB节点名 |
| (0) | MIB节点对应OID末位 |
| (lldpMessageTxInterval) | MIB节点下一个叶子节点名 |
| * | 表示叶子节点或表节点 |

# 显示 SNMP 支持的 MIB 表名、索引节点名及对应的 OID。

```
<Sysname> display snmp-agent mib-node index-node

Table           |dot1xPaePortTable
Index           ||dot1xPaePortNumber
OID             |||  1.0.8802.1.1.1.1.1.2.1.1
```

其它显示信息略……

表1-5 display snmp-agent mib-node index-node 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Table | MIB表名 |
| Index | MIB索引节点名 |
| OID | MIB索引节点对应的OID |

# 显示 SNMP 支持的 MIB 告警节点名及对应的 OID、告警绑定变量节点名及对应的 OID。

```
<Sysname> display snmp-agent mib-node trap-node


Name          |lldpRemTablesChange
OID           ||1.0.8802.1.1.2.0.0.1
Trap Object
Name          |||lldpStatsRemTablesInserts
OID           ||||1.0.8802.1.1.2.1.2.2
Name          |||lldpStatsRemTablesDeletes
OID           ||||1.0.8802.1.1.2.1.2.3
Name          |||lldpStatsRemTablesDrops
OID           ||||1.0.8802.1.1.2.1.2.4
Name          |||lldpStatsRemTablesAgeouts
OID           ||||1.0.8802.1.1.2.1.2.5
```

其它显示信息略……

表1-6 display snmp-agent mib-node trap-node 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Name | MIB告警节点名 |
| OID | MIB告警节点对应的OID |
| Trap Object | MIB告警绑定变量节点相关信息（其中Name表示告警绑定变量节点名，OID表示变量名节点对应的OID） |

# 显示 SNMP 支持的 MIB 节点详细信息，包括节点名、OID、节点类型、访问权限、数据类型，对应 MOR 定义、父子兄弟节点信息等。

```
<Sysname> display snmp-agent mib-node verbose


Name          |iso
OID           ||1
Properties    ||NodeType:   Other
              ||AccessType: NA
              ||DataType:   NA
              ||MOR:        0x00000000
Parent        ||
First child   ||std
Next leaf     ||dot1xPaeSystemAuthControl
Next sibling  ||
```

其它显示信息略……

表1-7 display snmp-agent mib-node verbose 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Name | MIB节点名 |
| OID | MIB节点对应的OID |

| 字段 | 描述 |
| --- | --- |
| Properties | MIB节点的属性 |
| NodeType | MIB节点类型，取值为：<br>• Table：表节点<br>• Row：表中行节点<br>• Column：表中列节点<br>• Leaf：叶子节点<br>• Group：组节点（叶子节点的父节点）<br>• Trapnode：告警节点<br>• Other：其他类型 |
| AccessType | MIB节点访问权限，取值为：<br>• NA：表示节点不可访问<br>• NF：表示节点支持告警<br>• RO：表示节点支持只读访问<br>• RW：表示节点支持读写访问<br>• RC：表示节点支持读写创建访问<br>• WO：表示节点支持只写访问 |
| DataType | MIB节点数据类型，取值为：<br>• Integer：整数<br>• Integer32：32 位整数<br>• Unsigned32：32 位无符号整数<br>• Gauge：可增可减的非负整数<br>• Gauge32：32 位可增可减的非负整数<br>• Counter：可增不可减的非负整数<br>• Counter32：32 位可增不可减的非负整数<br>• Counter64：64 位可增不可减的非负整数<br>• Timeticks：用于计时的非负整数<br>• Octstring：八进制字符串<br>• OID：对象标识符<br>• IPaddress：用于 IP 规范格式的 32 位地址<br>• Networkaddress：网络 IP 地址<br>• Opaque：任意数据<br>• Userdefined：用户类型<br>• BITS：所述位枚举<br>• NA：其他类型节点 |
| MOR | MIB节点对应的MOR定义 |
| Parent | 父节点名 |
| First child | 第一个子节点名 |
| Next leaf | 下一个叶子节点名 |

| 字段 | 描述 |
| --- | --- |
| Next sibling | 右兄弟节点名 |
| Allow | 允许的操作类型，取值包括如下：<br>• get/set/getnext：允许所有操作<br>• get：只允许 Get 操作<br>• set：只允许 Set 操作<br>• getnext：只允许 GetNext 操作 |
| Value range | 节点的取值范围 |
| Index | 表索引，仅表节点显示此字段 |

### 1.1.6 display snmp-agent mib-view

**display snmp-agent mib-view** 命令用来显示 MIB 视图的信息。

【命令】

**display snmp-agent mib-view** [ **exclude** | **include** | **viewname** *view-name* ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**exclude**：显示属性为 exclude 的 MIB 视图的信息。

**include**：显示属性为 include 的 MIB 视图的信息。

**viewname** *view-name*：显示指定名称 MIB 视图的信息，*view-name* 为视图的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

不指定参数时，显示所有 MIB 视图的信息。

【举例】

# 显示设备的所有 MIB 视图。

```
<Sysname> display snmp-agent mib-view
   View name: ViewDefault
       MIB Subtree: iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type: included
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpUsmMIB
```

```
        Subtree mask:
        Storage-type: nonVolatile
        View Type: excluded
        View status: active

    View name: ViewDefault
        MIB Subtree: snmpVacmMIB
        Subtree mask:
        Storage-type: nonVolatile
        View Type: excluded
        View status: active

    View name: ViewDefault
        MIB Subtree: snmpModules.18
        Subtree mask:
        Storage-type: nonVolatile
        View Type: excluded
        View status: active
```

以上信息表明，设备上当前有四个 MIB 视图，名称均为 ViewDefault。使用 ViewDefault 视图名限制 NMS 访问时，除了 snmpUsmMIB、snmpVacmMIB、snmpModules.18 子树下的 MIB 对象，NMS 可以访问 iso 子树下其它所有 MIB 对象。

表1-8 display snmp-agent mib-view 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| View name | 视图名 |
| MIB Subtree | MIB视图对应的MIB子树 |
| Subtree mask | MIB子树的掩码 |
| Storage-type | 存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体请参见表1-1 |
| View Type | MIB视图的类型（即该视图与MIB子树的关系），包括included和excluded两种：<br>• included 表示当前视图包括该子树的所有节点，即可以访问子树内的所有 MIB 对象<br>• excluded 表示当前视图不包括该子树的任意节点，即子树内的所有 MIB 对象都不能被访问 |
| View status | MIB视图的状态，包括：<br>• active 表示 MIB 视图可用<br>• inactive 表示 MIB 视图不可用。用户不能对处于该状态的 MIB 视图中的节点执行读写操作，但允许 MIB 视图中的节点发送 Trap 和 Inform 消息 |

【相关命令】

- **snmp-agent mib-view**

### 1.1.7 display snmp-agent remote

**display snmp-agent remote** 命令用来显示远端 SNMP 实体的引擎 ID。

【命令】

**display snmp-agent remote** [ { *ipv4-address* | **ipv6** *ipv6-address* } ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

*ipv4-address*：显示指定 IPv4 地址的远端 SNMP 实体的引擎 ID。*ipv4-address* 表示远端 SNMP 实体的 IPv4 地址。

**ipv6** *ipv6-address*：显示指定 IPv6 地址的远端 SNMP 实体的引擎 ID。*ipv6-address* 表示远端 SNMP 实体的 IPv6 地址。

【使用指导】

SNMP 实体引擎 ID 是 SNMP 实体的唯一标识，它在一个 SNMP 管理域内是唯一的。SNMP 实体引擎是 SNMP 实体的重要组成部分，完成 SNMP 信息的信息调度、信息处理、安全验证、访问控制等功能。

如果未指定远端 SNMP 实体的 IP 地址，则会显示设备上配置的所有远端 SNMP 实体的引擎 ID。

【举例】

# 显示设备上配置的所有远端 SNMP 实体的引擎 ID。

```
<Sysname> display snmp-agent remote
   Remote engineID: 800063A28000A0FC00580400000001
       IPv4 address: 1.1.1.1
```

表1-9 display snmp-agent remote 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Remote engineID | 远端SNMP实体的引擎，可通过**snmp-agent remote**命令配置 |
| IPv4 address | 远端SNMP实体的IPv4地址 |
| IPv6 address | 远端SNMP实体的IPv6地址。当配置**snmp-agent remote**命令时绑定的是IPv6地址时，显示该信息 |

【相关命令】

- **snmp-agent remote**

## 1.1.8 display snmp-agent statistics

**display snmp-agent statistics** 命令用来显示 SNMP 报文的统计信息。

【命令】

**display snmp-agent statistics**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

# 显示 SNMP 报文的统计信息。

```
<Sysname> display snmp-agent statistics
  1684 messages delivered to the SNMP entity.
  5 messages were for an unsupported version.
  0 messages used an unknown SNMP community name.
  0 messages represented an illegal operation for the community supplied.
  0 ASN.1 or BER errors in the process of decoding.
  1679 messages passed from the SNMP entity.
  0 SNMP PDUs had badValue error-status.
  0 SNMP PDUs had genErr error-status.
  0 SNMP PDUs had noSuchName error-status.
  0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
  16544 MIB objects retrieved successfully.
  2 MIB objects altered successfully.
  7 GetRequest-PDU accepted and processed.
  7 GetNextRequest-PDU accepted and processed.
  1653 GetBulkRequest-PDU accepted and processed.
  1669 GetResponse-PDU accepted and processed.
  2 SetRequest-PDU accepted and processed.
  0 Trap PDUs accepted and processed.
  0 alternate Response Class PDUs dropped silently.
  0 forwarded Confirmed Class PDUs dropped silently.
```

表1-10 display snmp-agent statistics 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| messages delivered to the SNMP entity | Agent收到的数据报文个数 |
| messages were for an unsupported version | 版本不支持的数据报文个数 |
| messages used an unknown SNMP community name | 使用了非法团体名的数据报文个数 |
| messages represented an illegal operation for the community supplied | 包含了超出团体名权限的操作的数据报文个数 |
| ASN.1 or BER errors in the process of decoding | 在解码过程中发生ASN.1（Abstract Syntax Notation dot one，抽象记法1）或BER（Basic Encoding Rules，基本编码规则）错误的数据报文个数 |
| messages passed from the SNMP entity | Agent发送给别的SNMP实体的数据报文个数 |
| SNMP PDUs had badValue error-status | 错误类型为BadValues的数据报文个数 |
| SNMP PDUs had genErr error-status | genErr错误的数据报文个数 |
| SNMP PDUs had noSuchName error-status | NoSuchName错误的数据报文个数 |

| 字段 | 描述 |
| --- | --- |
| SNMP PDUs had tooBig error-status | TooBig错误的数据报文个数（设备允许通过的最大SNMP PDU为1500字节） |
| MIB objects retrieved successfully | 已成功获取的MIB对象个数 |
| MIB objects altered successfully | 已成功修改的MIB对象个数 |
| GetRequest-PDU accepted and processed | 已接收并处理的Get请求的个数 |
| GetNextRequest-PDU accepted and processed | 已接收并处理的GetNext请求的个数 |
| GetBulkRequest-PDU accepted and processed | 已接收并处理的GetBulk请求的个数 |
| GetResponse-PDU accepted and processed | 已接收并处理的Get响应的个数 |
| SetRequest-PDU accepted and processed | 已接收并处理的Set请求的个数 |
| Trap PDUs accepted and processed | 已接收并处理的Trap和Inform报文的个数 |
| alternate Response Class PDUs dropped silently | 被丢弃的响应数据报文个数 |
| forwarded Confirmed Class PDUs dropped silently | 被丢弃的转发数据报文个数 |

### 1.1.9 display snmp-agent sys-info

**display snmp-agent sys-info** 命令用来显示 SNMP 设备的系统信息。

【命令】

**display snmp-agent sys-info** [ **contact** | **location** | **version** ] *

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**contact**：显示当前设备维护者的联系信息。

**location**：显示当前设备的物理位置信息。

**version**：显示当前设备中运行的 SNMP 版本号。

【使用指导】

不指定参数时，显示设备的全部系统信息。

【举例】

# 显示设备系统信息。

```
<Sysname> display snmp-agent sys-info
   The contact information of the agent:
       New H3C Technologies Co., Ltd.

   The location information of the agent:
```

```
    Hangzhou, China

  The SNMP version of the agent:
    SNMPv3
```

【相关命令】

- **snmp-agent sys-info**

## 1.1.10 display snmp-agent trap queue

**display snmp-agent trap queue** 命令用来显示告警信息队列的基本信息。

【命令】

**display snmp-agent trap queue**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

# 显示当前告警信息队列的配置及使用情况。

```
<Sysname> display snmp-agent trap queue
  Queue size: 100
  Message number: 6
```

表1-11 display snmp-agent trap queue 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Queue size | 告警信息队列长度 |
| Message number | 告警信息队列中当前告警信息的个数 |

【相关命令】

- **snmp-agent trap life**
- **snmp-agent trap queue-size**

## 1.1.11 display snmp-agent trap-list

**display snmp-agent trap-list** 命令用来显示 SNMP 告警功能的开启状态。

【命令】

**display snmp-agent trap-list**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

如果一个模块包含多个子模块，只要有任何一个子模块的告警信息是使能的，就显示整个模块是使能的。

业务模块是否支持 SNMP 告警功能请通过执行 **snmp-agent trap enable ?**命令来获知。本命令的显示信息和 **snmp-agent trap enable** 命令以及业务模块的配置相关。

【举例】

# 显示 SNMP 告警功能的开启状态。

```
<Sysname> display snmp-agent trap-list
   arp notification is disabled.
   configuration notification is enabled.
   mac-address notification is enabled.
   radius notification is disabled.
   standard notification is enabled.
   syslog notification is disabled.
   system notification is enabled.

   Enabled notifications: 4; Disabled notifications: 3
```

【相关命令】

- **snmp-agent trap enable**

### 1.1.12 display snmp-agent usm-user

**display snmp-agent usm-user** 命令用来显示 SNMPv3 用户信息。

【命令】

**display snmp-agent usm-user** [ **engineid** *engineid* | **group** *group-name* | **username** *user-name* ] *

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**engineid** *engineid*：显示指定引擎 ID 的 SNMPv3 用户信息，*engineid* 表示 SNMP 引擎 ID，不区分大小写。SNMPv3 用户创建的时候，系统会记录当时设备的 SNMP 实体引擎 ID，如果设备的引擎 ID 被修改，则被创建的 SNMPv3 用户将暂时无效，只有引擎 ID 恢复后，才能继续生效。

**group** *group-name*：显示属于指定 SNMP 组的 SNMPv3 用户信息，区分大小写。

**username** *user-name*：显示指定名称的 SNMPv3 用户信息，区分大小写。

【使用指导】

使用 **snmp-agent usm-user** 命令可以创建 SNMPv1/v2c/v3 用户，如果创建是的 SNMPv1/v2c 用户，系统自动添加一个新的同名的团体名，并将这个用户当成 SNMPv1/v2c 团体来处理。所以，

不能通过 **display snmp-agent usm-user** 命令来查看 SNMPv1/v2c 用户的信息，能通过 **display snmp-agent community** 查看 SNMPv1/v2c 用户对应的团体的信息。

【举例】

# 显示设备上已创建的所有 SNMPv3 用户的信息。

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000

   Username: userv3
   Group name: mygroupv3
       Engine ID: 8000259503000BB3100A508
       Storage-type: nonVolatile
       UserStatus: active
       ACL name: testacl

   Username: userv3code
   Role name: groupv3code
              network-operator
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active

   Username: userv3code
   Role name: snmprole
              network-operator
       Engine ID: 800063A280000002BB0001
       Storage-type: nonVolatile
       UserStatus: active
```

表1-12 display snmp-agent usm-user 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Username | SNMP用户的用户名 |
| Group name | SNMP用户所在组的组名 |
| Role name | SNMP用户的角色名称 |
| Engine ID | SNMP用户创建时使用的SNMP实体引擎ID |
| Storage-type | 存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体请参见表1-1 |

| 字段 | 描述 |
| --- | --- |
| UserStatus | SNMP用户的状态，分为以下几种：<br>• active：有效<br>• notInService：当前不可用<br>• notReady：未配置完成<br>• other：其他 |
| ACL | 使用的ACL列表的编号（该字段仅在用户与ACL绑定后显示，不会与ACL name同时存在） |
| ACL name | 使用的ACL列表的名称（该字段仅在用户与ACL名称绑定后显示，不会与ACL同时存在） |

【相关命令】

- **snmp-agent usm-user v3**

## 1.1.13 enable snmp trap updown

**enable snmp trap updown** 命令用来开启接口状态变化的告警功能。

**undo enable snmp trap updown** 命令用来关闭接口状态变化的告警功能。

【命令】

**enable snmp trap updown**

**undo enable snmp trap updown**

【缺省情况】

接口状态变化的告警功能处于开启状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

需要注意的是，如果要求接口在状态发生改变时生成接口状态变化的告警信息，需要开启全局告警功能并在接口开启接口状态变化的告警功能。接口下开启请使用命令 **enable snmp trap updown**，全局下开启请使用命令 **snmp-agent trap enable standard [ linkdown | linkup ] ***。

【举例】

# 允许发送端口 GigabitEthernet1/0/1 的 linkUp/linkDown 的 SNMP 告警，使用团体名 public，向 IP 地址为 10.1.1.1 的目的主机发送 Trap 报文。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

【相关命令】

- **snmp-agent target-host**
- **snmp-agent trap enable**

### 1.1.14 snmp-agent

**snmp-agent** 命令用来开启 SNMP Agent 功能。

**undo snmp-agent** 命令用来关闭 SNMP Agent 功能。

【命令】

**snmp-agent**

**undo snmp-agent**

【缺省情况】

SNMP Agent 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

执行除 **snmp-agent calculate-password** 外任何以 **snmp-agent** 开头的命令都可以开启 SNMP Agent 功能。

当 SNMP 侦听端口被设备上的其他服务占用时，会导致 SNMP 功能启动失败。SNMP 侦听端口可通过 **snmp-agent port** 命令配置，用户可使用 **display udp verbose** 命令查看设备上 UDP 端口的使用情况。

用户修改 SNMP 模块的相关配置后，如果关闭 SNMP Agent 功能，这些配置将暂时不生效。执行 **display current-configuration** 命令不会显示这些命令，执行 **save** 命令，这些配置也不会保存到配置文件。开启 SNMP Agent 功能后，这些配置会自动立即生效，不需要重复配置。

【举例】

# 开启设备的 SNMP Agent 功能。

```
<Sysname> system-view
[Sysname] snmp-agent
```

【相关命令】

- **display udp verbose**（网络互通/IP 性能优化）
- **snmp-agent port**

### 1.1.15 snmp-agent { inform | trap } source

**snmp-agent** { **inform** | **trap** } **source** 命令用来配置发送的告警信息的源 IP 地址。

**undo snmp-agent** { **inform** | **trap** } **source** 命令用来恢复缺省情况。

【命令】

**snmp-agent** { **inform** | **trap** } **source** *interface-type* { *interface-number* | *interface-number.subnumber* }

**undo snmp-agent** { **inform** | **trap** } **source**

【缺省情况】

使用出接口的 IP 地址作为告警信息的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**inform**：用来指定 Inform 报文中的源 IP 地址。

**trap**：用来指定 Trap 报文中的源 IP 地址。

*interface-type* { *interface-number* | *interface-number.subnumber* }：指定三层接口类型与接口编号。其中 *interface-number* 为主接口编号；*subnumber* 为子接口编号，取值范围为 1～4094。

【使用指导】

执行该命令后，系统会使用指定接口的主 IP 地址作为发送出去的告警信息的源 IP 地址。这样，在 NMS 上就可以使用该 IP 地址唯一标志 Agent。即便 Agent 使用不同的出接口发送告警信息，NMS 都可以使用该 IP 地址来过滤 Agent 发送的所有告警信息。

在将某个接口配置为获取告警信息的源地址接口之前需要注意的是：

- 如果配置的接口已存在，并且配置了合法的 IP 地址，则该 IP 地址将作为告警信息的源地址；
- 如果配置的接口不存在，则该命令会配置失败；
- 如果配置的接口已存在，但未配置合法的 IP 地址，则该命令不生效，在接口配置了合法 IP 地址后，该命令会自动生效。

【举例】

# 配置 Trap 报文的源地址为虚拟模板接口 1 上的接口主 IP 地址。

```
<Sysname> system-view
[Sysname] snmp-agent trap source Virtual-Template 1
```

# 配置 Inform 报文的源地址为虚拟模板接口 1 上的接口主 IP 地址。

```
<Sysname> system-view
[Sysname] snmp-agent inform source Virtual-Template 1
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**

## 1.1.16 snmp-agent calculate-password

**snmp-agent calculate-password** 命令用来为明文密码计算对应的密文密码。

【命令】

**snmp-agent calculate-password** *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*plain-password*：表示明文密码，为 1～64 个字符的字符串，区分大小写。

**mode**：指定认证算法和加密算法。设备支持的认证算法有 HMAC-MD5 和 HMAC-SHA1，其中 HMAC-MD5 的计算速度比 HMAC-SHA1 快，而 HMAC-SHA1 的安全强度比 HMAC-MD5 高；设备支持的加密算法安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

- **3desmd5**：用于计算密文加密密码，此时对应的认证算法必须为 HMAC-MD5，加密算法必须为 3DES。
- **3dessha**：用于计算密文加密密码，此时对应的认证算法必须为 HMAC-SHA1，加密算法必须为 3DES。
- **md5**：用于计算密文认证密码和密文加密密码。用于计算密文认证密码时，认证算法必须为 HMAC-MD5；用于计算密文加密密码时，认证算法必须为 HMAC-MD5，加密算法可以为 AES 或者 DES。因为当认证算法为 HMAC-MD5 时，相同的明文密码，各自计算出来的密文认证密码和密文加密密码均相同。
- **sha**：用于计算密文认证密码和密文加密密码。用于计算密文认证密码时，认证算法必须为 HMAC-SHA1；用于计算密文加密密码时，认证算法必须为 HMAC-SHA1，加密算法可以为 AES 或者 DES。因为当认证算法为 HMAC-SHA1 时，相同的明文密码，各自计算出来的密文认证密码和密文加密密码均相同。

**local-engineid**：使用本地引擎 ID 计算密文密码，引擎 ID 的相关描述与配置可参考命令 **snmp-agent local-engineid**。

**specified-engineid**：使用用户指定的引擎 ID 计算密文密码。

*engineid*：引擎 ID，必须为偶数个十六进制数，偶数的取值范围为 10～64，不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

执行本命令前，必须先开启设备的 SNMP Agent 功能。

在创建 SNMPv3 用户时，如果指明认证或者加密密码采用密文配置方式，则可以输入该命令生成的密文密码来代替明文密码，从而避免在非安全环境直接输入明文密码造成的安全隐患。

生成的密码是和引擎 ID 相关联的，在某一引擎 ID 下生成的密码，也只在此引擎 ID 下生效。

【举例】

# 使用本地引擎 ID 和 HMAC-SHA1 算法计算明文认证密码 authkey 的密文密码。

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

【相关命令】

- **snmp-agent local-engineid**
- **snmp-agent usm-user v3**

### 1.1.17 snmp-agent community

**snmp-agent community** 命令用来创建 SNMP 团体。

**undo snmp-agent community** 命令用来删除 SNMP 团体。

【命令】

VACM 方式：

**snmp-agent community** { **read** | **write** } [ **simple** | **cipher** ] *community-name* [ **mib-view** *view-name* ] [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

**undo snmp-agent community** [ **cipher** ] *community-name*

RBAC 方式：

**snmp-agent community** [ **simple** | **cipher** ] *community-name* **user-role** *role-name* [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

**undo snmp-agent community** [ **cipher** ] *community-name*

【缺省情况】

不存在 SNMP 团体。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**read**：表示对 MIB 对象的访问权限为只读。NMS 使用该团体名访问 Agent 时只能执行读操作。

**write**：表示对 MIB 对象的访问权限为读写。NMS 使用该团体名访问 Agent 时可以执行读、写操作。

**simple**：表示以明文方式配置团体名并以密文方式保存到配置文件中。

**cipher**：表示以密文方式配置团体名并以密文方式保存到配置文件中。

*community-name*：配置明文团体名或密文团体名，是限制 NMS 访问 Agent 时所使用的团体名。区分大小写，需要转义的字符请加 “\” 后输入。当以明文方式配置时，团体名为 1～32 个字符的字符串；当以密文方式配置时，团体名为 33～73 个字符的字符串。

**mib-view** *view-name*：用来指定 NMS 可以访问的 MIB 对象的范围，*view-name* 表示 MIB 视图名，为 1～32 个字符的字符串，区分大小写。不指定参数时，缺省视图为 ViewDefault。

**user-role** *role-name*：该团体对应的角色名称，*role-name* 为 1～63 个字符的字符串，区分大小写。

**acl**：将团体名与基本/高级 IPv4 ACL 绑定。

*ipv4-acl-number*：表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 的取值范围为 2000～2999，高级 IPv4 ACL 的取值范围为 3000～3999。

**name** *ipv4-acl-name*：表示基本或高级 IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

**acl ipv6**：将团体名与基本/高级 IPv6 ACL 绑定。

*ipv6-acl-number*：表示基本或高级 IPv6 ACL 的编号，其中基本 IPv6 ACL 的取值范围为 2000～2999，高级 IPv6 ACL 的取值范围为 3000～3999。

**name** *ipv6-acl-name*：表示基本或高级 IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

为了安全起见，只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 SNMP 特性或本命令的操作权限，也不能执行本命令。

该命令用于 SNMPv1 和 SNMPv2c 组网环境。

团体是 NMS 和 Agent 的集合，用团体名来标志。团体名相当于密码，团体内的设备通信使用团体名来进行认证。只有 NMS 和 Agent 上配置的团体名相同时，才能互相访问。通常情况下，“public”被用来作为读权限团体名、“private”被用来作为写权限团体名。为了增强安全性，网络管理员也可以配置其它团体名。

用户有两种方式创建团体：

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user** { **v1** | **v2c** }和 **snmp-agent group** { **v1** | **v2c** }命令成功创建 SNMPv1 或 SNMPv2c 用户以及相应的组后，系统会以用户名为团体名自动创建一个团体。

**display snmp-agent community** 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

使用 **snmp-agent community** 命令创建团体时，可以通过两种配置方式来控制团体的访问：

- VACM（View-based Access Control Model，基于视图的访问控制模型）的配置方式：该方式通过指定 MIB 视图来限定 NMS 可以访问的 MIB 节点，访问的动作包括只读和读写两种。
- RBAC（Role Based Access Control，基于角色的访问控制）的配置方式：该方式使用用户角色来限定 NMS 的访问权限。缺省情况下，用户角色 network-admin 和 level-15 可以读写所有的 MIB 节点，network-operator 可以只读所有的 MIB 节点。有关用户角色的详细信息，请参见“基础配置指导”中的“RBAC”。

推荐使用 RBAC 配置方式，安全性更高。

多次执行本命令最多可创建 10 个团体名。

多次执行该命令，指定的团体名相同，其它参数不同时，新配置生效。

不指定 **simple** 和 **cipher** 参数时，表示以明文方式配置团体名，并以明文方式保存到配置文件。

使用 **acl** 参数可以限制非法 NMS 访问设备：

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时，则只有规则中 permit 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

关于 ACL 的详细描述和介绍请参见“安全配置指导”中的“ACL”。

【举例】

# 以明文方式创建 SNMP 团体 readaccess，并且允许 NMS 使用该团体名对设备上缺省视图内的 MIB 对象进行只读访问。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read simple readaccess
```

# 以明文方式配置团体名 writeaccess，并且只允许 IP 地址为 1.1.1.1 的 NMS 使用该团体名对设备上缺省视图内的 MIB 对象进行读写操作，禁止其它 NMS 使用该团体名执行写操作。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl 2001
```

# 以明文方式配置团体名 writeaccess，并且只允许 IP 地址为 1.1.1.2 的 NMS 使用该团体名对设备上缺省视图内的 MIB 对象进行读写操作，禁止其它 NMS 使用该团体名执行写操作。

```
<Sysname> system-view
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl name testacl
```

# 以明文方式创建团体名 wr-sys-acc，使用该团体名访问设备时只能对 system（OID 为 1.3.6.1.2.1.1）子树下的 MIB 对象执行写操作。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write simple wr-sys-acc mib-view test
```

【相关命令】

- **display snmp-agent community**
- **snmp-agent mib-view**

## 1.1.18 snmp-agent community-map

**snmp-agent community-map** 命令用来创建团体名到 SNMP 上下文的映射。

**undo snmp-agent community-map** 命令用来删除团体名到 SNMP 上下文的映射。

【命令】

**snmp-agent community-map** *community-name* **context** *context-name*

**undo snmp-agent community-map** *community-name* **context** *context-name*

【缺省情况】

不存在团体名到 SNMP 上下文的映射。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*community-name*：团体名，为 1～32 个字符的字符串，区分大小写。

*context-name*：SNMP 上下文。为 1～32 个字符的字符串，区分大小写。

【使用指导】

用户配置成功后，使用 SNMP v1/v2 版本连接 SNMP Agent 时，SNMP 插件端所获取的上下文，是此时 NMS 访问 Agent，使用的团体名映射的上下文。如团体名未配置上下文映射，则获取不到。

系统中可配置的映射最多为 10 个。

【举例】

# 配置一个团体名到 SNMP 上下文的映射。

```
<Sysname> system-view
[Sysname] snmp-agent community-map private context testcontext
```

【相关命令】

- **display snmp-agent community**

### 1.1.19 snmp-agent context

**snmp-agent context** 命令用来创建 SNMP 上下文。

**undo snmp-agent context** 命令用来删除 SNMP 上下文。

【命令】

**snmp-agent context** *context-name*

**undo snmp-agent context** *context-name*

【缺省情况】

不存在 SNMP 上下文。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*context-name*：SNMP 上下文，为 1～32 个字符的字符串，区分大小写。

【使用指导】

NMS 未配置上下文，或 NMS 与 Agent 配置为相同的上下文时，两者可以连接成功，否则返回超时。

系统中可配置的 SNMP 上下文最多为 20 个。

【举例】

# 创建一个新的 context。

```
<Sysname> system-view
[Sysname] snmp-agent context testcontext
```

【相关命令】

- **display snmp-agent context**

### 1.1.20 snmp-agent group

**snmp-agent group** 命令用来创建 SNMP 组。

**undo snmp-agent group** 命令用来删除 SNMP 组。

【命令】

- SNMPv1 和 SNMPv2c 版本下的命令格式是：

  **snmp-agent group** { **v1** | **v2c** } *group-name* [ **read-view** *view-name* ] [ **write-view** *view-name* ] [ **notify-view** *view-name* ] [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

  **undo snmp-agent group** { **v1** | **v2c** } *group-name*

- SNMPv3 版本下的命令格式是：

  **snmp-agent group v3** *group-name* [ **authentication** | **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

  **undo snmp-agent group v3** *group-name* [ **authentication** | **privacy** ]

【缺省情况】

不存在 SNMP 组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**v1**：SNMPv1 版本。

**v2c**：SNMPv2c 版本。

**v3**：SNMPv3 版本。

*group-name*：SNMP 组的名称，取值范围为 1～32 个字符的字符串，区分大小写。

**authentication**：表示对报文进行认证但不加密。

**privacy**：表示对报文进行认证和加密。

**read-view** *view-name*：只读视图名，为 1～32 个字符的字符串，区分大小写。缺省值为 ViewDefault。

**write-view** *view-name*：读写视图名，为 1～32 个字符的字符串，区分大小写。缺省情况下，未配置读写视图，即 NMS 不能对设备的所有 MIB 对象进行写操作。

**notify-view** *view-name*：可以发告警信息的视图名，为 1～32 个字符的字符串，区分大小写。缺省情况下，未配置告警信息视图。

**acl**：将组与基本/高级 IPv4 ACL 绑定。

*ipv4-acl-number*：表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 编号的取值范围为 2000～2999，高级 IPv4 ACL 编号的取值范围为 3000～3999。

**name** *ipv4-acl-name*：表示基本或高级 IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

**acl ipv6**：将组与基本/高级 IPv6 ACL 绑定。

*ipv6-acl-number*：表示基本或高级 IPv6 ACL 的编号，其中基本 IPv4 ACL 编号的取值范围为 2000～2999，高级 IPv6 ACL 编号的取值范围为 3000～3999。

**name** *ipv6-acl-name*：表示基本或高级 IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

为了安全起见，只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 SNMP 特性或本命令的操作权限，也不能执行本命令。

SNMP 组可以定义安全模式、视图权限等信息，配置在此组内的用户都具有这些公共属性。

系统中可配置的 SNMP 组最多为 20 个。

是否指定 **authentication** 和 **privacy** 参数存在如下情况：

- 当不指定 **authentication** 和 **privacy** 时，表示不认证不加密。此时，使用和该组绑定的用户名建立 SNMP 连接时，均不认证不加密。即便用户配置了认证密码/加密密码，认证密码/加密密码也不生效。
- 当指定 **authentication** 时，表示认证不加密。此时，使用和该组绑定的用户名建立 SNMP 连接时，均认证不加密。即便用户配置了加密密码，加密密码也不生效。
- 当指定 **privacy** 时，表示认证加密。此时，使用和该组绑定的用户名建立 SNMP 连接时，均认证加密。该组内的用户必须配置认证密码和加密密码，否则，不能建立 SNMP 连接。

创建 SNMP 组和用户的时候都可以使用 **acl** 参数限制非法 NMS 访问设备，只有两个 ACL 均允许的 NMS 才能访问设备。在创建组或用户时，ACL 均遵循以下规则：

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时，则只有规则中 permit 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

关于 ACL 的详细描述和介绍请参见“安全配置指导”中的“ACL”。

【举例】

# 在运行 SNMPv3 版本的设备上创建一个 SNMP 组 group1。

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

【相关命令】

- **display snmp-agent group**
- **snmp-agent mib-view**
- **snmp-agent usm-user**

### 1.1.21 snmp-agent local-engineid

**snmp-agent local-engineid** 命令用来配置本设备的 SNMP 引擎 ID。

**undo snmp-agent local-engineid** 命令用来恢复缺省情况。

【命令】

**snmp-agent local-engineid** *engineid*

**undo snmp-agent local-engineid**

【缺省情况】

设备引擎 ID 为“公司的企业号+设备信息”。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*engineid*：SNMP 引擎 ID，必须为偶数个十六进制数，偶数的取值范围为 10～64，不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

SNMP 引擎 ID 有两个作用：

- 在 NMS 管理的所有设备中，每一台设备都需要用一个唯一的引擎 ID 来标识 Agent，缺省情况下每个设备有一个缺省的引擎 ID，网络管理员需要确保管理域内不能有重复的引擎 ID。
- SNMPv3 版本的用户名、密文密码等都和引擎 ID 相关联，如果更改了引擎 ID，则原引擎 ID 下配置的用户名、密码失效。

通常情况下，使用设备的缺省引擎 ID 即可，用户也可以根据网络整体规划给设备配置方便记忆的引擎 ID，比如 A 栋一楼的一号设备可以将它的引擎 ID 设置为 000Af0010001，二号设备可以配置为 000Af0010002。

【举例】

# 配置本设备的 SNMP 引擎 ID 为 123456789A。

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

【相关命令】

- **display snmp-agent local-engineid**
- **snmp-agent usm-user**

### 1.1.22 snmp-agent log

**snmp-agent log** 命令用来开启 SNMP 日志功能。

**undo snmp-agent log** 命令用来关闭 SNMP 日志功能。

【命令】

**snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }

**undo snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }

【缺省情况】

SNMP 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**all**：表示 SNMP Get 操作、Set 操作和 SNMP 认证失败的日志开关。

**authfail**：表示 SNMP 认证失败的日志开关。

**get-operation**：表示 SNMP Get 操作的日志开关。

**set-operation**：表示 SNMP Set 操作的日志开关。

【使用指导】

当打开 SNMP Get 或者 Set 操作的日志开关，NMS 对 Agent 执行指定的操作时，Agent 会记录与该操作相关信息并保存到设备的信息中心。当打开 SNMP 认证失败的日志开关时，如果 Agent 收到来自 NMS 的 SNMP 请求但是没有通过认证，Agent 会记录相关信息并保存到设备的信息中心。保存的相关信息将通过信息中心的参数配置，最终决定 SNMP 日志的输出规则（即是否允许输出以及输出方向）。

【举例】

# 打开 SNMP Get 操作的日志开关。

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

# 打开 SNMP Set 操作的日志开关。

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

# 打开 SNMP 认证失败的日志开关。

```
<Sysname> system-view
[Sysname] snmp-agent log authfail
```

### 1.1.23 snmp-agent mib-view

**snmp-agent mib-view** 命令用来创建或者更新 MIB 视图。

**undo snmp-agent mib-view** 命令用来删除 MIB 视图。

【命令】

**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [ **mask** *mask-value* ]

**undo snmp-agent mib-view** *view-name*

【缺省情况】

存在四个 MIB 视图，名称均为 ViewDefault：

- 视图一包含 MIB 子树 iso；
- 视图二不包含子树 snmpUsmMIB；

- 视图三不包含子树 snmpVacmMIB；
- 视图四不包含子树 snmpModules.18。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**excluded**：表示当前视图不包括该 MIB 子树的任何节点（即禁止访问 MIB 子树的所有节点）。

**included**：表示当前视图包括该 MIB 子树的所有节点（即允许访问 MIB 子树的所有节点）。

*view-name*：视图名，为 1～32 个字符的字符串，区分大小写。

*oid-tree*：MIB 子树，用子树根节点的 OID（如“1.3.6.1.2.1.1”）或名称（如“system”）表示，为 1～255 个字符的字符串，区分大小写。OID 是由一系列的整数组成，标明节点在 MIB 树中的位置，它能唯一地标识一个 MIB 库中的对象。

**mask** *mask-value*：对象子树的掩码，必须为偶数个十六进制数，偶数的取值范围为 1～32，不区分大小写。

【使用指导】

MIB 视图是 MIB 的子集，由视图名和 MIB 子树来唯一确定一个 MIB 视图。视图名相同但包含的子树不同，则认为是不同的视图。

缺省视图可以通过 **display snmp-agent mib-view** 命令来查看。如果使用缺省视图限制 NMS 的访问权限时，除了 snmpUsmMIB、snmpVacmMIB、snmpModules.18 子树下的 MIB 对象，NMS 可以访问 iso 子树下其它所有 MIB 对象。缺省视图可以通过 **undo snmp-agent mib-view** 命令删除，但是删除以后，可能导致不能对 Agent 的所有 MIB 节点执行读写操作，除非另外手工配置视图。

【举例】

# 创建并更新 MIB 视图信息，视图名称为 mibtest，先创建一个包含 mib-2 子树（OID 为“1.3.6.1.2.1”）所有对象的 MIB 视图，再更新为不包含“system”子树(OID 为“1.3.6.1.2.1.1”)所有对象的 MIB 视图。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Sysname] snmp-agent mib-view excluded mibtest system
[Sysname] snmp-agent community read public mib-view mibtest
```

以上配置成功后，当 NMS 使用 SNMPv1 版本，public 团体名访问设备时，不能查询 system 子树的所有对象（比如 sysDescr 和 sysObjectID 等节点），可以查询 mib-2 子树下的其它所有对象。

【相关命令】

- **display snmp-agent mib-view**
- **snmp-agent group**

## 1.1.24 snmp-agent packet max-size

**snmp-agent packet max-size** 命令用来配置 Agent 能接收或发送的 SNMP 报文的最大长度。

**undo snmp-agent packet max-size** 命令用来恢复缺省情况。

【命令】

**snmp-agent packet max-size** *byte-count*

**undo snmp-agent packet max-size**

【缺省情况】

Agent 能处理的 SNMP 报文的最大长度为 1500。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*byte-count*：Agent 能接收/发送的 SNMP 报文的最大长度，取值范围为 484～17940，单位为字节。

【使用指导】

配置报文的最大长度是为了防止网络中存在不支持分片的主机，而导致超长数据被丢弃。通常情况下，使用缺省值即可。

【举例】

# 配置 Agent 能接收/发送的 SNMP 报文的最大长度为 1024 字节。

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1024
```

### 1.1.25 snmp-agent port

**snmp-agent port** 命令用来配置 SNMP 服务的侦听端口号。

**undo snmp-agent port** 命令用来恢复缺省情况。

【命令】

**snmp-agent port** *port-number*

**undo snmp-agent port**

【缺省情况】

SNMP 服务的侦听端口号是 161。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*port-number*：SNMP 服务的侦听端口号，取值范围为 1～65535。

【使用指导】

当开启 SNMP Agent 功能时，如果 SNMP 侦听端口正被设备上的其它服务占用，会导致 SNMP 功能启动失败。此时，可使用本命令修改 SNMP 侦听端口。如果指定的新端口仍被其它服务占用，则

新端口配置失败。建议修改前使用 **display udp verbose** 命令查看设备上 UDP 端口的使用情况。

本命令配置成功后，NMS 需要使用新端口重新连接设备后，才能进行 Get/Set 等操作。

【举例】

# 配置 SNMP 服务的侦听端口号为 5555。

```
<Sysname> system-view
[Sysname] snmp-agent port 5555
```

【相关命令】

- **display udp verbose**（网络互通/IP 性能优化）

### 1.1.26 snmp-agent remote

**snmp-agent remote** 命令用来配置远端 SNMP 实体的引擎 ID。

**undo snmp-agent remote** 命令用来取消已配置的远端 SNMP 实体的引擎 ID。

【命令】

**snmp-agent remote** { *ipv4-address* | **ipv6** *ipv6-address* } **engineid** *engineid*

**undo snmp-agent remote** *ip-address*

【缺省情况】

未配置远端 SNMP 实体的引擎 ID。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*ipv4-address*：远端 SNMP 实体的 IP 地址。

**ipv6** *ipv6-address*：远端 SNMP 实体的 IPv6 地址。

*engineid*：引擎 ID，必须为偶数个十六进制数，偶数的取值范围为 10～64，不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

当设备需要向 NMS 发送 SNMPv3 Inform 报文时，必须配置该命令，并将 *ip-address* 配置为 NMS 的 IP 地址，*engineid* 配置为 NMS 的引擎 ID。因为协议要求 SNMPv3 Inform 报文中必须携带一个权威引擎 ID，NMS 收到该报文后，会用自己的引擎 ID 和这个权威引擎 ID 比较，如果相同，才能接收。

用户最多可以配置 20 个远端 SNMP 实体引擎 ID。

【举例】

# 配置 IP 地址为 10.1.1.1 的 SNMP 实体的引擎 ID 为 123456789A。

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

【相关命令】

- **display snmp-agent remote**

### 1.1.27 snmp-agent sys-info contact

**snmp-agent sys-info contact** 命令用来配置设备的维护联系信息。

**undo snmp-agent sys-info contact** 命令用来恢复缺省情况。

【命令】

**snmp-agent sys-info contact** *sys-contact*

**undo snmp-agent sys-info contact**

【缺省情况】

设备的维护联系信息为 New H3C Technologies Co., Ltd.

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*sys-contact*：描述系统维护联系信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

如果设备发生故障，设备维护人员可以利用系统维护联系信息，及时与设备生产厂商取得联系。

【举例】

# 配置设备的维护联系信息为 Dial System Operator # 27345。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator # 27345
```

【相关命令】

- **display snmp-agent sys-info**

### 1.1.28 snmp-agent sys-info location

**snmp-agent sys-info location** 命令用来配置设备的物理位置信息。

**undo snmp-agent sys-info location** 命令用来恢复缺省情况。

【命令】

**snmp-agent sys-info location** *sys-location*

**undo snmp-agent sys-info location**

【缺省情况】

物理位置信息为 Hangzhou, China。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*sys-location*：设备的物理位置信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

为便于识别和管理设备，请使用该命令将设备所处的物理位置记录在设备中。

【举例】

# 配置设备的物理位置信息为 Room524-row1-3。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info location Room524-row1-3
```

【相关命令】

- **display snmp-agent sys-info**

### 1.1.29 snmp-agent sys-info version

**snmp-agent sys-info version** 命令用来配置设备支持的 SNMP 版本。

**undo snmp-agent sys-info version** 命令用来取消对指定 SNMP 版本的支持。

【命令】

**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }

**undo snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }

【缺省情况】

启用 SNMPv3 版本。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**all**：支持 SNMPv1、SNMPv2c 和 SNMPv3 版本。

**v1**：支持 SNMPv1 版本。

**v2c**：支持 SNMPv2c 版本。

**v3**：支持 SNMPv3 版本。

【使用指导】

支持指定的 SNMP 版本后，设备才能收发该版本的 SNMP 报文。只有 NMS 和 Agent 使用的 SNMP 版本相同，NMS 才能和 Agent 建立连接。

【举例】

# 配置设备支持 SNMPv3 版本。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v3
```

【相关命令】

- **display snmp-agent sys-info**

### 1.1.30 snmp-agent target-host

**snmp-agent target-host** 命令用来配置接收 SNMP 告警信息的目的主机（能够解析 Trap 和 Inform 报文的设备，通常为 NMS）的属性。

**undo snmp-agent target-host** 命令用来取消目的主机配置。

【命令】

**snmp-agent target-host inform address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [ **udp-port** *port-number* ] **params securityname** *security-string* { **v2c** | **v3** [ **authentication** | **privacy** ] }

**snmp-agent target-host trap address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [ **udp-port** *port-number* ] **params securityname** *security-string* [ **v1** | **v2c** | **v3** [ **authentication** | **privacy** ] ]

**undo snmp-agent target-host** { **trap** | **inform** } **address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

【缺省情况】

未配置告警主机。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**inform**：配置接收 Inform 报文的目的主机的参数。

**trap**：配置接收 Trap 报文的目的主机的参数。

**address**：指定接收告警信息的目的主机的地址。

**udp-domain**：指定使用 UDP 协议来传输 SNMP 告警信息。

*ipv4-address*：接收告警信息的目的主机的 IPv4 地址或主机名，主机名为 1～253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_” 或 “.”。若使用主机名配置，发送时将获取主机名对应的 IPv4 地址，向对应的主机发送告警信息。

**ipv6** *ipv6-address*：接收告警信息的目的主机的 IPv6 地址或主机名，主机名为 1～253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_” 或 “.”。若使用主机名配置，发送时将获取主机名对应的 IPv6 地址，向对应的主机发送告警信息。若使用 IPv6 地址配置，则不能为链路本地地址。

**udp-port** *port-number*：指定目的主机上用来接收告警信息的端口号，缺省值为 162。

**params securityname** *security-string*：指定认证的参数，*security-string* 为 SNMPv1、SNMPv2c 的团体名或 SNMPv3 的用户名，为 1～32 个字符的字符串，区分大小写。

**v1**：SNMPv1 版本。

**v2c**：SNMPv2c 版本。

**v3**：SNMPv3 版本。

**authentication**：指明对报文进行认证但不加密。认证功能用来验证报文的完整性或报文是否被篡改等，认证密码在创建 SNMPv3 用户时配置。

**privacy**：指明对报文进行认证和加密。加密是对报文的数据部分进行加密处理以防信息被窃取，认证密码和加密密码在创建 SNMPv3 用户时配置。

【使用指导】

根据实际组网需要，用户可以多次使用该命令配置不同的目的主机的属性，使得设备可以向多个 NMS 发送告警信息。

不指定 **udp-port** *port-number* 参数时，使用的端口号为 162。162 是 SNMP 协议规定的 NMS 接收告警信息的端口，通常情况下（比如使用 iMC 或者 MIB Browser 作为 NMS 时），使用该缺省值即可。如果要将该参数修改为其它值，则必须和 NMS 上的配置保持一致。

不指定 **v1**、**v2c**、**v3** 版本参数时，使用的版本是 v1。设备配置的 SNMP 版本必须和 NMS 上运行的 SNMP 版本一致，否则，NMS 将收不到告警信息。

不指定 **authentication** 和 **privacy** 参数时，使用的是不认证不加密的安全级别。

【举例】

# 允许向 10.1.1.1 发送 SNMPv3 Trap 报文，用户名为 public。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
v3
```

【相关命令】

- **snmp-agent** { **inform** | **trap** } **source**
- **snmp-agent trap enable**
- **snmp-agent trap life**

## 1.1.31 snmp-agent trap enable

**snmp-agent trap enable** 命令用来开启 SNMP 告警功能。

**undo snmp-agent trap enable** 命令用来关闭 SNMP 告警功能。

【命令】

**snmp-agent trap enable** [ **configuration** | *protocol* | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ] * | **system** ]

**undo snmp-agent trap enable** [ **configuration** | *protocol* | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ] * | **system** ]

【缺省情况】

SNMP 配置告警、标准告警和系统告警功能处于开启状态，其他各模块告警功能是否开启请参见各模块手册。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**configuration**：SNMP 配置告警信息。配置该参数后，系统会以 10 分钟为周期，查看周期内当前运行配置或者启动配置是否被修改，以及是否有用户对启动配置文件进行修改，并将最后一次修改形成一条告警输出。

*protocol*：开启指定协议模块的 SNMP 告警功能。用户可通过执行 **snmp-agent trap enable ?** 命令来获取该参数的取值，有关此参数的详细介绍，请参见各模块的命令手册。

**standard**：SNMP 标准告警信息。包括以下五种：

- **authentication**：NMS 访问设备时认证失败，输出 SNMP 认证失败的告警信息。
- **coldstart**：当设备重新启动时，输出设备冷启动告警信息。
- **linkdown**：当接口的链路 down 时，输出 linkDown 告警信息。
- **linkup**：当接口的链路 up 时，输出 linkUp 告警信息。
- **warmstart**：当 SNMP 模块重新启动时，输出热启动告警信息。

**system**：SNMP 系统告警信息。配置该参数后，如果系统时间被修改、系统重启或系统主用启动软件包不可用，均会生成告警信息。

【使用指导】

对于协议模块的 SNMP 告警功能，需要先使能相关协议，本命令才能配置成功。

开启指定协议模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

不指定可选参数时，表示在全局下开启/关闭所有可选模块的告警功能。

【举例】

# 开启 SNMP 认证失败的告警功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard authentication
```

【相关命令】

- **snmp-agent target-host**

## 1.1.32 snmp-agent trap if-mib link extended

**snmp-agent trap if-mib link extended** 命令用来对标准格式的 linkUp 或 linkDown 告警信息进行私有扩展。

**undo snmp-agent trap if-mib link extended** 命令用来恢复缺省情况。

【命令】

**snmp-agent trap if-mib link extended**

**undo snmp-agent trap if-mib link extended**

【缺省情况】

系统发送的 linkUp/linkDown 告警信息的格式为标准格式，不对其进行私有扩展。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

扩展格式的 linkUp/linkDown 告警信息由标准格式的 linkUp/linkDown 告警信息后增加接口描述和接口类型信息构成，使用扩展格式的告警信息有助于网络管理员快速定位问题。

需要注意的是，配置该命令后，设备发送的 linkUp/linkDown 告警信息为扩展格式的信息。如果 NMS 不支持扩展格式，可能会无法解析信息。

【举例】

# 对标准格式的 linkUp/linkDown 告警信息进行私有扩展。

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

## 1.1.33 snmp-agent trap life

**snmp-agent trap life** 命令用来配置告警信息的保存时间。

**undo snmp-agent trap life** 命令用来恢复缺省情况。

【命令】

**snmp-agent trap life** *seconds*

**undo snmp-agent trap life**

【缺省情况】

SNMP 告警信息的保存时间为 120 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*seconds*：超时时间，取值范围为 1～2592000，单位为秒。

【使用指导】

SNMP 模块使用队列来发送告警信息，告警信息进入消息发送队列时会启动一个存活定时器。如果直到定时器超时（即达到 **snmp-agent trap life** 命令配置的时间），告警信息还没有被发送出去，系统就会将该告警信息从发送队列中删除。

【举例】

# 配置告警信息的保存时间为 60 秒。

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**
- **snmp-agent trap queue-size**

### 1.1.34 snmp-agent trap log

**snmp-agent trap log** 命令用来开启 SNMP 告警日志功能。

**undo snmp-agent trap log** 命令用来关闭 SNMP 告警日志功能。

【命令】

**snmp-agent trap log**

**undo snmp-agent trap log**

【缺省情况】

SNMP 告警日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

打开 SNMP 告警日志开关，Agent 向 NMS 发送告警时，Agent 会向信息中心模块发送一条日志来记录该告警相关的信息。通过配置信息中心的参数，最终决定 SNMP 告警日志的输出规则（即是否允许输出以及输出方向）。

【举例】

# 开启 SNMP 告警日志功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap log
```

### 1.1.35 snmp-agent trap queue-size

**snmp-agent trap queue-size** 命令用来配置告警信息发送队列的长度。

**undo snmp-agent trap queue-size** 命令用来恢复缺省情况。

【命令】

**snmp-agent trap queue-size** *size*

**undo snmp-agent trap queue-size**

【缺省情况】

告警信息的发送队列最多可以存储 100 条告警信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*size*：消息队列中可以存储的告警信息的数目，取值范围 1～1000。

【使用指导】

告警信息产生后，会进入告警信息消息队列进行发送，告警信息消息队列的长度决定了队列最多可以存储的告警信息的数目。当告警信息队列达到设定长度后，最新生成的告警信息会进入消息队列，最早产生的告警信息被丢弃。

【举例】

# 配置发送告警信息的消息队列最多可以存储 200 条告警信息。

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**
- **snmp-agent trap life**

## 1.1.36 snmp-agent usm-user { v1 | v2c }

**snmp-agent usm-user** { **v1** | **v2c** }命令用来创建 SNMPv1 或 SNMPv2c 用户。

**undo snmp-agent usm-user** { **v1** | **v2c** }命令用来删除 SNMPv1 或 SNMPv2c 用户。

【命令】

**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

**undo snmp-agent usm-user** { **v1** | **v2c** } *user-name*

【缺省情况】

不存在 SNMP 用户。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**v1**：表示配置的用户名适用于 SNMPv1 组网环境。

**v2c**：表示配置的用户名适用于 SNMPv2c 组网环境。

*user-name*：用户名，为 1～32 个字符的字符串，区分大小写。

*group-name*：该用户对应组的名称，取值范围为 1～32 个字符的字符串，区分大小写。创建用户时，组可以不存在。但要使创建的用户生效，必须先创建组。

**acl**：将用户名与基本/高级 IPv4 ACL 绑定。

*ipv4-acl-number*：表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 的取值范围为 2000～2999，高级 IPv4 ACL 的取值范围为 3000～3999。

**name** *ipv4-acl-name*：表示基本或高级 IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

**acl ipv6**：将用户名与基本/高级 IPv6 ACL 绑定。

*ipv6-acl-number*：表示基本或高级 IPv6 ACL 的编号，其中基本 IPv6 ACL 的取值范围为 2000～2999，高级 IPv6 ACL 的取值范围为 3000～3999。

**name** *ipv6-acl-name*：表示基本或高级 IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

为了安全起见，只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 SNMP 特性或本命令的操作权限，也不能执行本命令。

SNMPv1 和 SNMPv2c 组网应用中 NMS 和 Agent 之间使用团体名来认证，SNMPv3 组网应用中使用用户名来认证。

用户有两种方式创建团体：

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user { v1 | v2c }**和 **snmp-agent group { v1 | v2c }**命令成功创建 SNMPv1 或 SNMPv2c 用户以及相应的组后，系统会以用户名为团体名自动创建一个团体。该团体的访问权限可通过 **snmp-agent community** 或 **snmp-agent group { v1 | v2c }**命令来修改，最后一次执行的命令生效。

**display snmp-agent community** 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

创建 SNMP 组和用户的时候都可以使用 **acl** 参数限制非法 NMS 访问设备，只有两个 ACL 均允许的 NMS 才能访问设备。在创建组或用户时，ACL 均遵循以下规则：

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时，则只有规则中 permit 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

关于 ACL 的详细描述和介绍请参见“安全配置指导”中的“ACL”。

【举例】

# 在 SNMP 组 readCom 里创建 SNMPv2c 用户 userv2c。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

如果 NMS 需要访问 Agent，则应将 NMS 的版本号指定为 SNMPv2c，Read community 选项填写为 userv2c。

# 在 SNMP 组 readCom 里创建 SNMPv2c 用户 userv2c，并且只允许 IP 地址为 1.1.1.1 的 NMS 使用该用户名访问 Agent，禁止其它 NMS 使用该用户名访问。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

# 在 SNMP 组 readCom 里创建 SNMPv2c 用户 userv2c，并且只允许 IP 地址为 1.1.1.2 的 NMS 使用该用户名访问 Agent，禁止其它 NMS 使用该用户名访问。

```
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

【相关命令】

- **snmp-agent group**
- **snmp-agent community**
- **display snmp-agent community**

## 1.1.37 snmp-agent usm-user v3

**snmp-agent usm-user v3** 命令用来创建 SNMPv3 用户。

**undo snmp-agent usm-user v3** 命令用来删除 SNMPv3 用户。

【命令】

- VACM 方式：

  **snmp-agent usm-user v3** *user-name group-name* [ **remote** { *ipv4-address* | **ipv6** *ipv6-address* } ] [ { **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [ **privacy-mode** { **3des** | **aes128** | **des56** } *priv-password* ] ] [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

  **undo snmp-agent usm-user v3** *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

- RBAC 方式：

  **snmp-agent usm-user v3** *user-name* **user-role** *role-name* [ **remote** { *ipv4-address* | **ipv6** *ipv6-address* } ] [ { **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [ **privacy-mode** { **3des** | **aes128** | **des56** } *priv-password* ] ] [ **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* } ] *

  **undo snmp-agent usm-user v3** *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

【缺省情况】

不存在 SNMPv3 用户。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*user-name*：用户名，为 1～32 个字符的字符串，区分大小写。

*group-name*：该用户对应组的名称，取值范围为 1～32 个字符的字符串，区分大小写。创建用户时，组可以不存在。但要使创建的用户生效，必须先创建组。

**user-role** *role-name*：该用户对应的角色名称，*role-name* 为 1～63 个字符的字符串，区分大小写。

**remote** { *ipv4-address* | **ipv6** *ipv6-address* }：接收 Inform 报文的目的主机的 IP 地址或者 IPv6 地址，通常为 NMS 的 IP 地址或者 IPv6 地址。当设备需要向目的主机发送 SNMPv3 Inform 报文时，该参数必须配置，还需要使用 **snmp-agent remote** 命令将目的主机的 IP 地址或者 IPv6 地址和引擎 ID 绑定。

**cipher**：以密文方式配置认证密码和加密密码。该密码将转换成对应的密文摘要存储在设备中。

**simple**：以明文方式配置认证密码和加密密码。该密码将转换成对应的密文摘要存储在设备中。

**authentication-mode**：指定认证算法。不指定该参数时，表示不认证。取值为：

- **md5**：采用 HMAC-MD5 算法。HMAC-MD5 的相关内容请参见“安全配置指导”中的“IPsec”。
- **sha**：采用 HMAC-SHA1 算法。HMAC-SHA1 的相关内容请参见“安全配置指导”中的“IPsec”。

*auth-password*：表示认证密码，区分大小写，具体要求如下：

- 以明文方式配置时，*auth-password* 表示明文认证密码。认证密码的长度范围是 1～64 个字符。
- 以密文方式配置时，*auth-password* 表示密文认证密码，该密码可通过 **snmp-agent calculate-password** 命令计算获得。

**privacy-mode**：指定加密算法。不指定该参数时，表示不加密。取值为：

- **3des**：采用 3DES（Triple Data Encryption Standard，三重数据加密标准）算法，密钥长度为 168 比特。
- **aes128**：采用 AES（Advanced Encryption Standard，高级加密标准）算法，密钥长度为 128 比特。
- **des56**：采用 DES（Data Encryption Standard，数据加密标准）算法，密钥长度为 56 比特。

*priv-password*：表示加密密码，区分大小写，具体要求如下：

- 以明文方式配置时，*auth-password* 表示明文加密密码。密码的长度范围是 1～64 个字符。
- 以密文方式配置时，*auth-password* 表示密文加密密码，该密码可通过 **snmp-agent calculate-password** 命令计算获得。

**acl**：将用户名与基本/高级 IPv4 ACL 绑定。

*ipv4-acl-number*：表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 的取值范围为 2000～2999，高级 IPv4 ACL 的取值范围为 3000～3999。

**name** *ipv4-acl-name*：表示基本或高级 IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

**acl ipv6**：将用户名与基本/高级 IPv6 ACL 绑定。

*ipv6-acl-number*：表示基本或高级 IPv6 ACL 的编号，其中基本 IPv6 ACL 的取值范围为 2000～2999，高级 IPv6 ACL 的取值范围为 3000～3999。

**name** *ipv6-acl-name*：表示基本或高级 IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

**local**：表示本地实体引擎 ID。缺省情况下，创建的 SNMPv3 用户与本地 SNMP 实体引擎相关联。

**engineid** *engineid-string*：指定与该用户相关联的引擎 ID 字符串，必须为偶数个十六进制数，偶数的取值范围为 10～64，不区分大小写。全 0 和全 F 均被认为是无效参数。由于 SNMPv3 版本的用户名、密文密码等都和引擎 ID 相关联，如果更改了引擎 ID，则原引擎 ID 下配置的用户名、密码失效，更改后可以使用该参数将 *engineid-string* 指定为创建该用户时的本地引擎 ID 来删除失效用户名。

【使用指导】

为了安全起见，只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 SNMP 特性或本命令的操作权限，也不能执行本命令。

创建 SNMPv3 用户时，可以通过两种配置方式来控制用户访问的权限：

- 通过 VACM 方式配置的 SNMP 用户依附于 SNMP 组，创建用户时，请先创建组。否则，用户能够创建成功但是不生效。一个组可以包含多个用户。组定义了用户能够访问的 SNMP 对象（通过 MIB 视图来限定）以及是否进行认证和加密等，而认证和加密的具体算法和密码则是在创建用户时定义。
- 通过 RBAC 方式配置的 SNMP 用户依附于用户角色，创建用户时，通过 **user-role** *role-name* 参数配置用户的角色。用户角色定义了 SNMP 用户能够访问的 SNMP 对象以及操作类型（通过 **rule** 规则来限定）。使用 RBAC 方式创建 SNMP v3 用户后，还可以使用 **snmp-agent usm-user v3 user-role** 命令为该用户绑定更多的用户角色，最多可绑定 64 个用户角色。

推荐使用 RBAC 配置方式，安全性更高。

通过 VACM 和 RBAC 方式配置 SNMP 用户时，需要注意：

- 通过 VACM 方式配置 SNMP 用户时，当用户名相同，多次执行本命令，最后一次执行的命令生效。
- 通过 RBAC 方式配置 SNMP 用户时，可以多次使用本命令为已创建的 SNMPv3 用户添加角色，若未配置其他参数，则其他配置不变，只添加角色；若同时配置其他参数（如认证方式），则为用户添加角色，同时修改其他配置。

创建 SNMP 组和用户的时候都可以使用 **acl** 参数限制非法 NMS 访问设备，只有两个 ACL 均允许的 NMS 才能访问设备。在创建组或用户时，ACL 均遵循以下规则：

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时，则只有规则中 permit 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

关于 ACL 的详细描述和介绍请参见“安全配置指导”中的“ACL”。

【举例】

# VACM 方式：为 v3 组 testGroup 加入一个用户 testUser，安全级别为只认证不加密，认证算法为 HMAC-SHA1，认证密码为明文 123456TESTplat&!。

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTplat&!
```

在 NMS 上配置：版本号为 SNMPv3，用户名为 testUser，认证算法为 HMAC-SHA1，认证密码为 123456TESTplat&!，建立连接，就可以对设备上缺省视图内的 MIB 对象进行访问了。

# VACM 方式：为 v3 组 testGroup 加入一个用户 testUser，安全级别为认证和加密，认证算法为 HMAC-SHA1、加密算法为 AES，认证密码为明文 123456TESTauth&!，加密密码为明文 123456TESTencr&!。

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

在 NMS 上配置：版本号为 SNMPv3，用户名为 testUser，认证算法为 HMAC-SHA1，认证密码为 123456TESTauth&!，加密算法为 AES，加密密码为 123456TESTencr&!，建立连接，就可以对设备上缺省视图内的 MIB 对象进行访问了。

# VACM 方式：为 v3 组 testGroup 加入一个与 IP 为 10.1.1.1 的远端 SNMP 实体引擎相关联的 SNMPv3 用户 remoteUser，安全级别为认证和加密，认证算法为 HMAC-SHA1、加密算法为 AES，认证密码为明文 123456TESTauth&!，加密密码为明文 123456TESTencr&!。

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 remoteUser testGroup remote 10.1.1.1 simple
authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

# RBAC 方式：创建一个新的 SNMPv3 用户 testUser，角色为 network-operator，安全级别为只认证不加密，认证算法为 HMAC-SHA1，认证密码为明文 123456TESTplat&!。

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple
authentication-mode sha 123456TESTplat&!
```

在 NMS 上配置：版本号为 SNMPv3，用户名为 testUser，认证算法为 HMAC-SHA1，认证密码为 123456TESTplat&!，建立连接，就可以对设备上所有 MIB 对象进行只读操作。

【相关命令】

- **display snmp-agent usm-user**
- **snmp-agent group**
- **snmp-agent calculate-password**
- **snmp-agent remote**
- **snmp-agent usm-user v3 user-role**

## 1.1.38 snmp-agent usm-user v3 user-role

**snmp-agent usm-user v3 user-role** 命令用来为通过 RBAC 方式创建的 SNMPv3 用户添加角色。

**undo snmp-agent usm-user user-role** 命令用来为 SNMPv3 用户删除角色。

【命令】

**snmp-agent usm-user v3** *user-name* **user-role** *role-name*

**undo snmp-agent usm-user v3** *user-name* **user-role** *role-name*

【缺省情况】

使用创建 SNMPv3 用户时指定的角色。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*user-name*：用户名，为 1～32 个字符的字符串，区分大小写。

**user-role** *role-name*：该用户对应的角色名称，*role-name* 为 1～63 个字符的字符串，区分大小写。

【使用指导】

一个 RBAC 方式配置的 SNMPv3 用户可配置多个用户角色。用户可以通过本命令来为通过 RBAC 方式创建的 SNMPv3 用户添加与删除角色，最多可以配置 64 个有效的用户角色且至少保留一个用户角色。

【举例】

# 已创建 SNMPv3 用户 testUser 拥有 network-operato 用户角色，现为用户 testUser 添加 network-admin 用户角色。

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-admin
```

【相关命令】

- **snmp-agent usm-user v3**