Configuring SNMP

This article describes how to enable SNMP on a Viptela device.

Enabling SNMP

By default, SNMP is disabled on Viptela devices. To enable it and provide support for SNMP Versions 1, 2, and 3:

```
Viptela(config)# snmp
Viptela(config-snmp)# no shutdown
```

Enabling SNMP allows the device to use MIBs, generate traps, and respond to requests from an SNMP walk application.

Configuring an SNMP View

To create an SNMP view, along with an OID, so that SNMP information is available to the SNMP server, configure an SNMP view and its corresponding OID subtree:

```
Viptela(config-snmp)# view string
Viptela(config-snmp)# oid oid-subtree
```

In the OID subtree, you can use the wildcard * (asterisk) in any position to match any value at that position.

The following example creates a view of the Internet portion of the SNMP MIB:

```
Viptela(config)# snmp view v2 oid 1.3.6.1
```

The following example creates a view of the private portion of the Viptela MIB:

```
Viptela(config)# snmp view viptela-private oid 1.3.6.1.4.1.41916
```

Configuring Access to an SNMP View

To require authentication privileges to access an SNMP view, configure SNMPv3. To do this, you configure authentication credentials for SNMPv3 users, and you configure groups of SNMP views and the authentication credentials required to access the views.

To configure authentication credentials for an SNMPv3 user, create a user and assign them an authentication level and a privacy level, depending on the authentication type you configure for the SNMP group (with the `snmp group` command, described below):

```
Viptela(config)# snmp user username
Viptela(config-user)# auth authentication
Viptela(config-user)# auth-password password
Viptela(config-user)# priv privacy
Viptela(config-user)# priv-password password
```

The username can be a string from 1 to 32 characters.
The authentication commands enable authentication privileges for the user. authentication can be either message digest 5 (md5) or SHA-2 message digest (sha). You can enter the password as a cleartext string or as an AES-encrypted key.

The privacy commands enable a privacy mechanism for the user. privacy can be either the Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key (aes-cfb-128). You can enter the password as a cleartext string or as an AES-encrypted key.

Then associate the SNMPv3 user with an SNMP group:

```
Viptela(config-user)# group group-name
```

group-name is the name of a group of views that you configure with the snmp group command.

To configure a group of views:

```
Viptela(config)# snmp group group-name authentication
Viptela(config-group)# view view-name
```

The group name can be a string from 1 to 32 characters.

The authentication to use to for the group can be one of the following:

- **auth-no-priv**—Authenticate using the HMAC-MD5 or HMAC-SHA algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password (with the snmp user auth and auth-password commands).

- **auth-priv**—Authenticate using the HMAC-MD5 or HMAC-SHA algorithm, and provide CBC DES 56-bit encryption. When you configure this authentication, users in this group must be configured with an authentication and an authentication password (with the snmp user auth and auth-password commands) and a privacy and privacy password (with the snmp user priv and priv-password commands).

- **no-auth-no-priv**—Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials.

The view name is the name of a SNMP view that you configure with the snmp view command.

Here is an example configuration for SNMP users and groups:

```
vEdge(config-snmp)# show full-configuration
snmp
    no shutdown
    view v2
        oid 1.3.6.1
    !
    community private
        view v2
        authorization read-only
    !
    group private-community auth-priv
        view v2
    !
    user noc-staff
        auth md5
        auth-password $4$aCGzJjtS3/czj48gLEFXKw==
        group private-community
    !
```
Configuring Contact Parameters

For each Viptela device, you can configure its SNMP node name, physical location, and contact information for the person or entity responsible for the device:

```
Viptela(config)# snmp
Viptela(config-snmp)# name string
Viptela(config-snmp)# location string
Viptela(config-snmp)# contact string
```

If any of the strings include spaces, enclose the entire string in quotation marks (" ").

Configuring an SNMP Community

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string, use the `community` command:

```
Viptela(config-snmp)# community name
Viptela(config-community-name)# authorization read-only
Viptela(config-community-name)# view string
```

The community name can be 1 through 32 characters long. It can include angle brackets (< and >). If the name includes spaces, enclose the entire name in quotation marks (" ").

Use the `view` command to specify the portion of the MIB tree to view. `string` is the name of a view record configured with the `snmp view` command, as described below.

The Viptela software supports the standard interfaces MIB, IF-MIB, and the system MIB (SNMPv2-MIB), which are automatically loaded onto the Viptela device when you install the Viptela software. For a list of enterprise MIBs, see the System and SNMP Overview. The MIBs supported by the Viptela software do not allow write operations, so you can configure only read-only authorization (which is the default authorization).

Configuring View Records

To configure a portion of an SNMP MIB to view, use the `view` command:

```
Viptela(config-snmp)# view string
Viptela(config-view)# oid oid-subtree [exclude]
```

For example, to view the Internet portion of the SNMP MIB configure the OID 1.3.6.1:

```
Viptela(config-snmp)# view v2 oid 1.3.6.1
```

To view the private portion of the Viptela MIB, configure the OID 1.3.6.1.4.1.41916.

Configuring SNMP Traps

SNMP traps are asynchronous notifications that a Viptela device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the Viptela device. By default, SNMP
traps are not sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

To configure SNMP traps, you define the traps themselves and you configure the SNMP server that is to receive the traps.

To configure groups of traps to be collected on a Viptela device, use the trap group command:

```
Viptela(config-snmp)# trap group group-name
Viptela(config-group)# trap-type level severity
```

The group-name is a name of your choosing.

The trap-type can be one of those listed in the table below.

The severity level can be one or more of critical, major, and minor.

<table>
<thead>
<tr>
<th>Trap Type</th>
<th>Critical</th>
<th>Major</th>
<th>Minor</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All critical traps listed below.</td>
<td>All major traps listed below.</td>
<td>All minor traps listed below.</td>
</tr>
<tr>
<td>app-route</td>
<td>SLA_Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bfd</td>
<td>BFD_State_Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge</td>
<td>Bridge_Creation Bridge_Deletion Max_MAC_Reach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>control</td>
<td>No_Active_vBond No_Active_vSmart Connection_Auth_Fail Connection_State_Change Connection_TLOC_IP_Change vBond_State_Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dhcp</td>
<td>Server_State_Change Address_Assigned Address_Released Address_Renewed Request_Rejected Server_State_Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hardware</td>
<td>EMMC_Fault Fan_Fault FanTray_Fault Flash_Fault PEM_Fault PEM_State_Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Events</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| PIM      | Fault  
          | State_Change |
| SDCard   | Fault  |
| SFP      | State_Change |
| TempSensor | Fault  
             | State  |
| USB      | State_Change |
| Data_Policy |  |
| Number_of_vSmarts | Change |
| Peer_State | Change  |
| State | Change  |
| TLOC_State | Change  |
| Access_List_Association_Status |  |
| Data_Policy_Association_Status |  |
| SLA_Violation_Pkt_Drop |  |
| SLA_Violation |  |
| BGP_Peer_State | Change  |
| OSPF_Interface_State | Change  
                  |       |
| OSPF_Neighbor_State | Change  |
| PIM_Interface_State | Change  
                     |       |
| PIM_Neighbor_State | Change  |
| PIM_Tunnel_State | Change  |
| Clear_Installed_Certificate |  |
| Root_Cert_Chain_Uninstalled |  |
| vEdge_Entry_Added |  |
| vEdge_Entry_Removed |  |
| vEdge_Serial_File_Uploaded |  |
| vSmart_Entry_Added |  |
| vSmart_Entry_Removed |  |
| vSmart_Serial_File_Uploaded |  |
| Certificate_Installed |  |
| New_CSR_Generated |  |
| Root_Cert_Chain_Installed |  |
| Tunnel_IPSec_Manual_Rekey |  |
| Tunnel_IPSec_Rekey |  |
| AAA_Admin_Pwd | Change  |
| Disk_Usage |  |
| Memory_Usage |  |
| Process_Restart |  |
| System_AAA_Login_Fail |  |
| System_Pseudo_Commit_Status |  |
| System_Reboot_Complete |  |
| Domain_ID | Change  |
| Org_Name | Change  |
| Reboot_Issued |  |
| Site_ID | Change  |
| Software_Install_Status |  |
| System_Commit |  |
| System_IP | Change  |
A single trap group can contain multiple trap types. In the configuration, specify one trap type per line, and each trap type can have one, two, or three severity levels. See the configuration example below for an illustration of the configuration process.

To configure the SNMP server to receive the traps, use the `trap target` command:

```
Viptela(config-snmp)# trap target vpn vpn-id ipv4-address udp-port
```

For each SNMP server, specify the identifier of VPN where the server is located, the server's IPv4 address, and the UDP port on the server to connect to. When configuring the trap server's address, you must use an IPv4 address. You cannot use an IPv6 address.

In the `group-name` command, associate a previously configured trap group with the server. The traps in that group are sent to the SNMP server.

In the `community-name` command, associate a previously configured SNMP community with the SNMP server.

In the `source-interface` command, configure the interface to use to send traps to the SNMP server that is receiving the trap information. This interface cannot be a subinterface.

The following configuration example sends all traps to one SNMP server and only critical traps to another SNMP server.

We configure two SNMP trap groups and the two target SNMP servers:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# snmp
vEdge(config-snmp)# view community-view
vEdge(config-snmp)# community public
vEdge(config-community-public)# authorization read-only
vEdge(config-community-public)# view community-view
vEdge(config-community-public)# exit
vEdge(config-snmp)# trap group all-traps
vEdge(config-group-all-traps)# all level critical major minor
vEdge(config-group-all-traps)# exit
vEdge(config-snmp)# trap group critical-traps
vEdge(config-group-critical-traps)# control level critical
vEdge(config-group-critical-traps)# exit
vEdge(config-group-critical-traps)# trap target vpn 0 10.0.0.1 162
vEdge(config-target-0/10.0.0.1/162)# group-name all-traps
vEdge(config-target-0/10.0.0.1/162)# community-name public
vEdge(config-target-0/10.0.0.1/162)# exit
vEdge(config-snmp)# trap target vpn 0 10.0.0.2 162
vEdge(config-target-0/10.0.0.2/162)# group-name critical-traps
vEdge(config-target-0/10.0.0.2/162)# community-name public
vEdge(config-target-0/10.0.0.2/162)# exit
```
vEdge(config-snmp)# show full-configuration
snmp
view community-view
!
community public
view community-view
authorization read-only
!
trap target vpn 0 10.0.0.1 162
  group-name    all-traps
  community-name public
!
trap target vpn 0 10.0.0.2 162
  group-name    critical-traps
  community-name public
!
trap group all-traps
  all
  level critical major minor
!
trap group critical-traps
  bfd
  level critical
  !
  control
  level critical
  !
  hardware
  level critical
  !
  omp
  level critical
  !
!
vEdge(config-snmp)#

For each trap generated by a Viptela device, the device also generates a notification message. Use the show notification stream viptela command to display these messages. Here is an example of the command output. The first line of the output shows the time when the message was generated (the SNMP eventTime). The time is shown in UTC format, not in the device's local time. The second line of the notification contains a description of the event, and the third line indicates the severity level.

vEdge# show notification stream viptela
notification eventTime 2015-04-17T14:39:41.687272+00:00 bfd-state-change severity-level major
  host-name vEdge
  system-ip 1.1.4.2
dst-ip 108.200.52.250
  proto ipsec
  src-port 12346
dst-port 12406
  local-system-ip 1.1.4.2
  local-color default
  remote-system-ip 1.1.9.1
  remote-color default
  new-state down
!

notification eventTime 2015-04-17T15:12:20.435831+00:00 tunnel-ipsec-rekey severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
color default
!

notification eventTime 2015-04-17T16:56:50.314986+00:00 system-login-change severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  user-name admin
Additional Information

OID Repository

System, Interface, and SNMP CLI Reference

System and SNMP Overview

For Viptela enterprise MIBs, see the YANG Files for Netconf and Enterprise MIB Files section in the release notes for your software release.