Vital Security™ Web Appliances NG-1100/NG-5100/NG-8100

How to Use Simple Network Management Protocol (SNMP) Monitoring

Introduction

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Currently, Vital Security NG supports SNMP Versions 1, and 2c.

NOTE: This SNMP document is relevant for Software version 8.4.0 and above.

SNMP Traps

The SNMP screen allows you to monitor in real time, or near real time, any abnormal behavior of the system. You can also react to these events in a timely manner and potentially resolve the issues.

In the SNMP tab, you can monitor the main modules and components of the system. SNMP Version 2c traps are deployed as the means of notification for specific events.

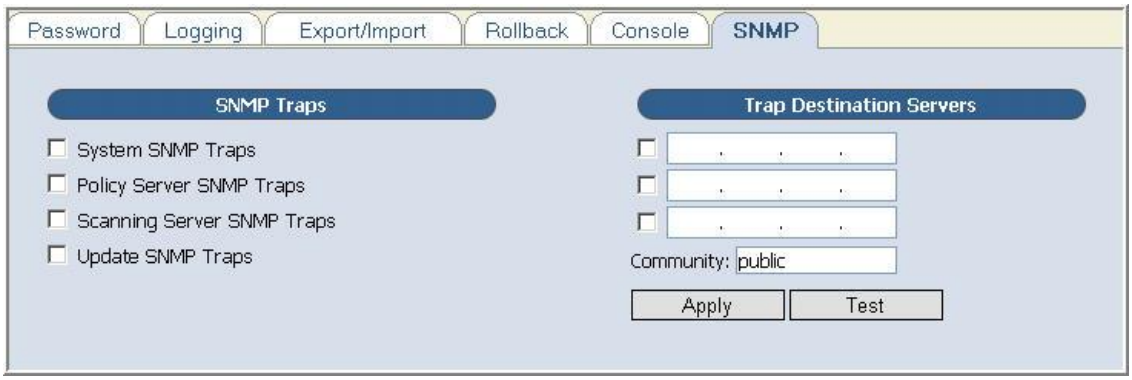

Figure 1: SNMP

SNMP Traps

The following SNMP traps are available:

- **System SNMP Traps**: System load average for last 15 minutes above given threshold, Disk quota limit
- **Policy Server SNMP Traps**: Log Handler down
- **Scanning Server SNMP Traps**: Problems with Scanning Server
- **Update SNMP Traps**: Update issues

NOTE: SNMP is enabled by Default. To disable SNMP traps, navigate to the Setup Console>Advanced Settings >Custom Commands screen and disable for each Scanning Server individually.

Trap Destination Servers

Three destination servers have been provided; you can configure the traps to be sent to any or all of these servers.

An SNMP community is the group that devices and management stations running SNMP belong to. It should be defined as required. The default string is "public".

The Test button allows you to test that the traps are successfully sent to the servers. A test message will be sent to the defined server with the SNMP Name, IP and NG Version. In this screen, clicking Test automatically includes applying the changes.

After making any changes to the SNMP screen, click **Apply** and Commit Changes.

Enabling SNMP for MIB

The SNMP Monitoring feature can be enabled via the Vital Security Setup Console.

⇨ **To enable the SNMP feature:**

1. Log in to the Setup Console.
2. Navigate to Advanced Settings →Custom Commands. The following screen appears:

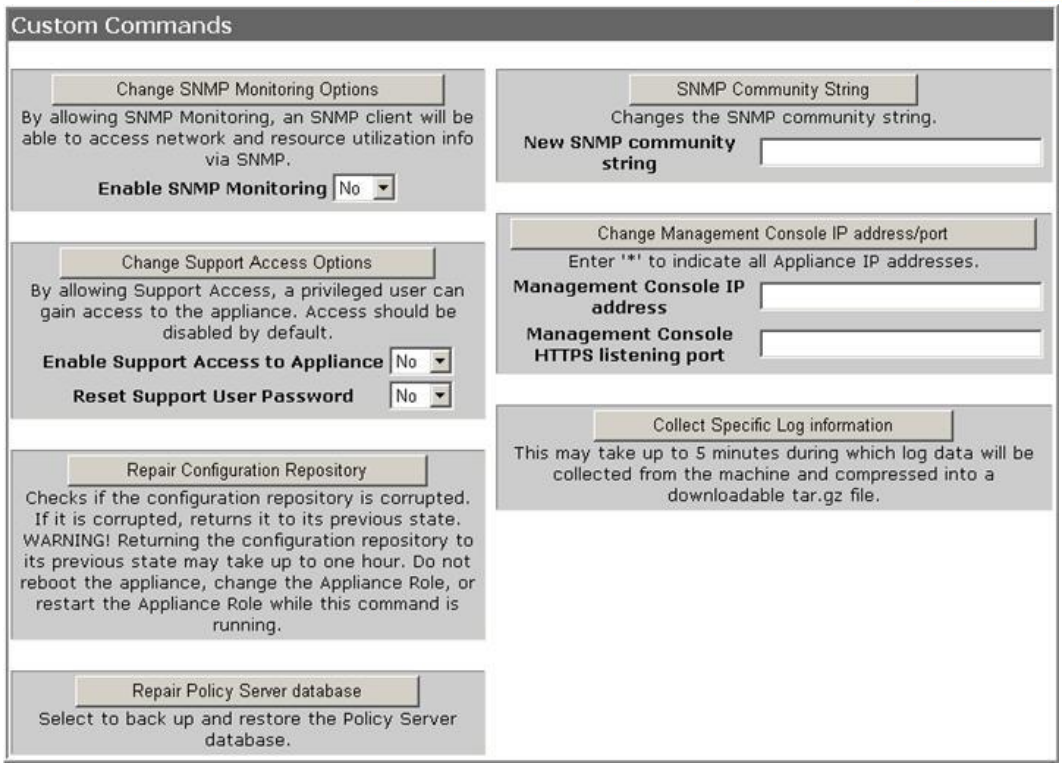

Figure 2: Custom Commands

3. In the **Enable SNMP Monitoring** option at the top of the screen, select the radio button **Yes**.
4. Click on **Change SNMP Monitoring Options** for the change to take effect.

The password or SNMP Community String can also be changed if required. The default value is “public”.

⇨ **To change the SNMP Community String:**

1. Enter the required text in the **New SNMP Community String** field.
2. Click on SNMP Community String for the changes to take effect.

NOTE: Currently, Vital Security NG supports SNMP read-only values.

Management Information Base (MIB) Support

A Management Information Base (MIB) is a database of objects that can be monitored by the SNMP. An MIB-II is a Network Management for TCP/IP based devices.

The **Vital Security NG Web Appliances** support the following SNMP MIBs:

- Interfaces: MIBII - 2
- IP MIBII - 4
- TCP MIBII - 6

Example Using Standard MIB support

Use **`1.3.6.1.2.1.6.8.`** to get "The number of times that TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state."

Any software which is able to work in conjunction with SNMP MIBs can be used. This includes the following:

- HPOV
- TEMIP
- MRTG/PRTG

Object Identifier (OID)

An object identifier (OID), also known as a MIB variable, is a number assigned to devices in a network for identification purposes. In addition to standard MIBs, Vital Security NG Web Appliances also use non-standard object IDs (OIDs).

The CPU, MEM and SCANNER OIDs contain the following values:

Application	Values
CpuUser	**.1.3.6.1.4.1.2021.11.50.0**
CpuNice	**.1.3.6.1.4.1.2021.11.51.0**
CpuSystem	**.1.3.6.1.4.1.2021.11.52.0**
CpuIdle	**.1.3.6.1.4.1.2021.11.53.0**
CpuKernel	**.1.3.6.1.4.1.2021.11.55.0**
MemTotalReal	**.1.3.6.1.4.1.2021.4.5.0**
MemAvailReal	**.1.3.6.1.4.1.2021.4.6.0**
Scanner Status	**.1.3.6.1.4.1.2021.8.1.100.1** Supported Values: 0: Scanner Up 1: Scanner Down
Scanner Status String	**.1.3.6.1.4.1.2021.8.1.101.1** Supported Values: Scanner Up Scanner Down

Example Using a Non-Standard OID

The following example enables the administrator to calculate the CPU usage using the application and values listed in the above table.

⇨ **To calculate the CPU usage:**

1. Calculate delta values for all CPU counters (deltaIdle, deltaUser, deltaNice, deltaSystem, deltaKernel) by taking a sample for each CPU counter every n amount of time.
2. Then, minus the value taken at an earlier stage of time from the value calculated at a later stage of time in order to calculate the delta value. For example, if at 10.00am, the value for CpuUser was 15, and at 10.02, the value for CpuUser was 20, then 20-15=5.
3. Add up each of these delta values for each CPU counter (delta CpuIdle + delta CpuUser + delta CpuNice + delta CpuSystem + delta CpuKernel) to obtain the deltaTotal.
4. The CPU Usage in percentage is **100 - 100 * deltaIdle / deltaTotal**. This represents the CPU Usage between the sampled time intervals.