**Configure SNMP Trap Monitoring**

This article will walk through the process of adding a device to inventory, importing the MIBs to Goliath and then configuring SNMP Trap definitions for generating alerts.

**Prerequisites**

Before getting started, please makes sure the following has been completed.

1. Enable SNMP on the device(s) you will be adding to Goliath Performance Monitor
2. Identify/assign a community string for your devices
   1. (this will be needed later during configuration)
3. Gather the MIB file(s) necessary for monitoring

**Prepare Goliath for SNMP MIB Monitoring**

1. Connect to the Goliath Server via RDP or a console session
2. Open **Server Manager** and go to **Manage>Add Roles & Features**
3. Proceed through the Add Roles & Features Wizard, on the **Features** pane, ensure the **SNMP Service** is installed
   1. If not, please check the box and install the feature
4. Once the SNMP Service is installed, open Windows Services and go to the properties of the SNMP Service
5. Navigate to the **Traps** tab of the SNMP Service properties
6. Add the community string(s) you would like the technology to accept and click **apply**
7. Navigate to the "Security" tab of the SNMP Service properties
8. In the bottom section of the Security tab, ensure the radio button for **accept SNMP packets from any host** is selected
9. Click **Apply** and restart the SNMP Service
10. Close Windows Services
11. Gather the MIB file(s) necessary for monitoring and add them to the MIBs folder of the Goliath installation
    1. C:\Program Files (x86)\MonitorIT\Mibs
    2. C:\Program Files\MonitorIT\Mibs

**Configure SNMP MIB Monitoring**

1. Open the Goliath web console and navigate to Configure > Inventory
2. Next, you’ll want to add in the device(s) you are looking to monitoring. If they are not in the technology already. please see the below instructions for adding them in, as appropriate.
   1. Auto-Discovery
      1. Click the **menu** button at the top of the page and select the sub menu option for **Discovery**
      2. Check off the box for **Find Servers/Devices in IP Address Range**
      3. Specify the IP Address range of the device(s) you wish to monitor
      4. Select **OK** at the bottom to begin discovery
      5. A new pane will appear and will start to load and list out the discovered machines/devices
      6. After discovery completes select the check box next to the appropriate device and select **Add** at the bottom
   2. Manual Addition
      1. Select **New** at the top of the page
      2. Specify the name of the device
      3. Next to the ‘Primary IP Address’ field click the **Add** link
      4. Specify the IP address of the device and click **OK** when finished
      5. Click **save**
      6. Repeat process to add additional devices
3. Once the devices have been added, go to **Settings>SNMP Mib Import**
4. Press the Process MIBs button to analyze all the '.mib' files stored in the "...\MonitorIT\Mibs" folder.
   1. The '.mib' files found here will have the Trap OIDs automatically discovered and added to the technology for monitoring.
   2. The '.mib' files can be processed any number of times as duplicate Trap OIDs are looked for and prevented.
   3. An error in any one '.mib' file will prevent the processing of any them. Refer to the error message in the pop-up message box. Usual errors are 'unknown identifiers'.Look for a case sensitive mismatch on the definition of the Object Type, and the later use of it in the Mib. If the Object name is used but not identified in the Mib, you may be missing the base Mib from the vendor where the Object Type identifiers are defined.
   4. If unable to correct the problem with the Mib, remove it from the "...\MonitorIT\Mibs" folder (or rename it to something other than '.mib', for example, '.mi\_') and run **Process MIBs**again to process the other Mibs in the folder.  After you correct the problem with the Mib, place it back in the "...\MonitorIT\Mibs" folder and rerun **Process MIBs.**
5. Once the MIBs have been processed, go to **Configure>Monitoring Rules**
6. Click the **New** button at the top of the page and then select the option for **SNMPTrapWatch**
7. Name the Monitoring Rule in the **Rule Name** field, as well as define the description and the severity.
8. The **Trap OID(s)** field, defines the Trap OID(s) for this Monitoring Rule. Click the **Add/Remove** button immediately to the right to modify the drop-down list.
   1. Clicking the *Add/Remove*button displays a pop-up box with all available Trap OIDs.
   2. Check or uncheck the associated checkbox to include or exclude the OID from this Monitoring Rule.
   3. Click the *Custom* button to define a new SNMP Trap OID, and optionally add it to the SNMP Trap OID Definitions
9. In the Selections tree, select the devices that you want to monitor the specified OID(s) on.
10. Click **Save** to complete the configuration

**Post Configuration - What's Next?**

Now that Goliath has been configured to receive SNMP traps, the data and information can be:

1. Viewed on our real-time dashboard via the **Views>SNMP Trap** page
2. Configured for scheduled or demand historical reports via the Reports page
   1. **Reports>New Report**
   2. Select the Report Type for **Alert & Log Analysis**, the report template **Alert Analysis** and click next
   3. Select the option for **SNMPWatch Alerts** and click next
   4. Select the objects/devices you'd like included in the report and click **next**
   5. Define the report details and click **next**
   6. Configure email/export options if applicable and click **next**
   7. Configure the reporting schedule and click done to **save**