Collection Templates

Overview

The Collection Templates tab lists all of the current collection templates that currently exist in the system. Selecting a template from the template listing displays all of the properties for that selected template. This is the same information that you would see in the Collection tab of the Library.

In this article, learn how to:

- Add Collection Templates
- Modify Collection Templates
- Delete Collection Templates
- Use the OID Selector
- Add a Collection Template with a Custom Rule

Add Collection Templates

Now that you have created a detection template, you can create a collection template to collect data pertaining to the device. Using the example Cisco 3620 router, lets create a collection template to collect data on lost IP packets and total bytes lost (based on data in the Conduct an SNMP walk example).

To add a new collection template, follow the steps listed below:

1. Prior to adding a collection template, look at the list of collection templates to see if there is already a template to avoid making duplicates.
2. Click on the **Add** icon. The **Template Configuration** values are cleared of data to allow you to enter the new information.

3. Enter the **Name** you want to give the template (e.g., Cisco 3620 Information).
4. Select **Template is sub-procedure**, if applicable. This allows them to be called from other templates, minimizing the need for duplication collections. Templates can only be sub-procedures or top-level templates (nesting templates is not allowed).
5. Select **Stop collection after this device** if you want this template to stop collecting data when it is finished with this device. This feature is typically only used when collecting data from antiquated devices to limit information stored.
6. Select the device from the **Apply to Device** drop-down that this template applies to. Please note that when

---

you are creating collection templates based on information received from a walk, that the data may be available to all units for a specific make of device (e.g., all Cisco units) and thus should be applied to the base object and not a specific model. However, for our example, we only select the Cisco 3620 Router option.

7. Select the **Network Devices** and/or **Computers** checkboxes, if applicable. Selecting Network Devices and not **Computers** tells the template to run against only networked devices, not on computers with agents trying to self-collect.
8. Select the **Custom Storage Table** checkbox if you want to store data to a custom table. Select the table from the database. The table must already exist in the database and the table name must begin with ProbeCustom. **This is not recommended unless you are an advanced user**. This table requires the following conditions:
   - The table name must start with *probecustom_*.
   - The table must have a DeviceID as the primary key (in addition to any other keys).
   - The table needs to have at least one column for the index (this column is used if the **Custom Table Walk** rule is selected later).
   - The table needs to have a column for each piece of data you wish to gather.
   - The table needs a LastUpdate column.
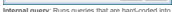9. Click on the **Add New Rule** icon.

10. Enter the **Rule Name** (e.g., Get actLostPkts).
11. Select the **Rule Type** from the drop-down. Your choices are: Call Sub-procedure, Custom Table Walk, Internal Query, Perform Walk and Retrieve OID. For our example, we select Retrieve OID. Your remaining fields depend on what was chosen for the **Rule Type**.
   - **Call Sub-procedure**: Only available from top-level templates. Allows for specifying any collection

---

template marked as a sub-procedure.
- **Custom Table Walk**: Only available if custom storage table was selected in Step 8. Allows for walking a certain OID and storing all retrieved values in a custom table. Refer to the Adding a Collection Template with a Custom Table Walk Rule for more information.
  - **OID**: The addresses of the SNMP table that you wish to retrieve information from.
  - **Index(es)**: The column in your custom database table that holds the values for the indexes of the SNMP table entered in the OID field.
  - **Data**: The specific information that is retrieved from the targeted SNMP table. This information must be in the format of <ColumnName>:<Index>;<ColumnName>:<Index>; etc. <ColumnName> is the name of a column in the specific custom table and <Index> is the field or property value from the SNMP table you wish to retrieve.
  - Example: Once the rule is set up, the expected results include the data from the fields (e.g., defined in the **Data** field) of the SNMP table (e.g., defined in the **OID** field). These results are stored in the custom table that was created earlier. All of the data that was collected and stored can be viewed by accessing the custom table in your database. The data in the rule should look similar to the following:

- **Internal query**: Runs queries into the probe system, which allows for optimization and standardization of data.
  - Host Resources Table: What resources (e.g., ink, ram, hard drives, etc.) are attached to the device.
  - Interface Sample Table: Sample the V1 interface table for bandwidth usage. Sampling occurs by querying the counters for each interface, waiting a few seconds, and querying the tables again. This is meant for networks where bandwidth is restricted and constant network monitoring is not feasible.
  - Interface Sample Tables II: Samples the V2 (64-bit counters) tables.
  - Interface Table: Queries the V1 interface table counters. Subtraction of subsequent counters is used to calculate bandwidth information. Collection period should be sufficient

---

to ensure the counters don't overflow and yield incorrect data.
- Interface Table II: Queries the V2 interface table counters.
- Printer Errors Table: Collects from the PRINTER-MIB errors OID to get standard errors (Low Toner, Paper Jam, etc.)
- Printer Marker Supply Table: Gets levels for the consumables (typically ink).
- Printer Markers Table: Gets the consumables for the printer.
- SNMP Information: Get basic information (name, description, uptime, etc.) common to all SNMP devices.
- Storage Areas Table: Gets usage information (total space, free space) for storage devices.
- **Perform Walk**: Walks a certain OID and store all retrieved values. Refer to the below warning before choosing this option.
  Important: The **Perform Walk** option should only be used by more advanced users. Using this setting without full understanding of the amount of data retrieved can have a serious impact on your bandwidth usage and system performance. Refer to Walking SNMP Devices for more information on doing an SNMP Walk.
- **Retrieve OID**: Pulls a specific OID. The name is used for reference information when storing in the central database.
  - The Parse As: indicates how Automate should handle the SNMP response. This should almost always be an integer or readable text.

12. If Retrieve OID was selected as the **Rule Type**, then a monitor can be created. A monitor may be useful for some information retrieved. In our example, lost packets may indicate failing network devices or an overloaded network. You may want a monitor to alert when packets are lost so you may check on network devices and traffic in a timely manner. If you are creating a monitor, select a frequency from the **Monitor Interval** drop-down. This determines the frequency that the monitor runs. If a monitor interval is selected, the **Monitor** tab appears in the **Collection Rule** window and allow you to create the collection monitor.
13. Select the **Collection Interval** from the drop-down. This is the frequency that the collection takes place to retrieve real-time information.
14. Select the desired **Historical Interval**. This is the amount of time the collection data is saved (e.g., how much printer ink was used over the past 24 hours).
   Note: If collection is set to every hour and historical is set to every 12 hours, data is sent every hour and at the 12th hour, this data is then stored in the history tables. To store historical data for a custom table, refer to Store Custom Data.
15. Enter the **OID** or click on the **Ellipsis** icon to select the OID using the **OID Selector**. If using the **OID Selector**, select the appropriate OID and click **OK**.

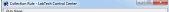16. Enter the **Name** associated with the OID. If you selected the OID using the **OID Selector**, the **Name** field

---

automatically populates.

17. Select the appropriate **Parse As:** response from the drop-down. The available options are: Integer, Readable Text, Standard Time (Ticks), MAC Address, Bit Value and Byte Encoded Time (y,m,d...). For our example, we choose Integer.
18. Additional fields are accessible if you chose **Bit Value** as the **Parse As:** response. If applicable, enter the zero-based index of the bit value to be captured.
   - **Bit Index**: Enter the zero-based index of the bit value to be captured.
   - **Text if ON**: Enter the text to appear when the value in the Bit Index is detected.
   - **Text if OFF**: Enter the text to appear if the value in the **Bit Index** is detected.
     Note: For example, if the collection template is setup for a printer, the value in the **Bit Index** field could be used for an operational failure (e.g., a paper jam). If the **Bit Index** value is detected by the collection template, the value in the **Text if ON** field is displayed (e.g., The printer has experienced a paper jam). However, if the collection template does not detect the **Bit Index** value, the **Text if OFF** is displayed (e.g., The printer is operating normally).
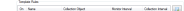19. If you selected a monitor interval, select the monitor tab to create a monitor.

20. From here, a monitor can be set up to monitor any devices found by the collection template. This essentially be a universal monitor that enables you to monitor any devices of the type that are found by the collection template (e.g., a collection template for a specific printer will monitor all of these attached printers). Refer to the **Creating Remote Monitors** section of Create Remote Monitors for more information on setting up remote monitors.
   1. Select a monitor condition from the **Condition** drop-down (e.g., Exists, Not Equals, etc.)
   2. Enter a **Comparison Value** in the blank field. If **State Based** was selected for the **Condition**, you need to enter further **State Conditions**. Refer to Using State Based Monitoring for more information.
   3. Select an **Alert Template** from the drop-down. Refer to Configuring Alert Templates for more information on the available alert templates or for information on creating an alert template for this monitor.
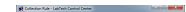
---

4. Select the **Alert Style** from the drop-down. Alert styles determine the frequency in which you are notified when the monitor fails.
   - **Continuous**: The alert action occurs every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket will be created and will not get another ticket until the first one is resolved or deleted.
   - **Once**: The alert action occurs one time until the monitor checks and returns a success message.
   - **Second through Tenth**: The alert action occurs on the selected fail count until the monitor checks and returns a success message. For example, if Second is chosen, the monitor must have two consecutive failures before performing the alert action.
5. Statistics can be recorded for this monitor and combined with other monitors with the same report category and reported in the status gauges. To record the statistics from this monitor, select a gauges. To record the statistics from this monitor, select a **Report Category** from the drop-down. Refer to Using Status Gauges for more information.
6. The **Ticket Category** is used to classify tickets and is leveraged by your PSA software (if supported) to route common types of tickets to different service boards in the PSA. New monitors need to be assigned to the proper ticket category. Refer to Using Ticket Categories for more information.
7. Scripts can be run to automatically correct problems reported by a monitor (e.g, restarting stopped services). If applicable, select the appropriate **Script to Run** from the drop-down.
21. Click **OK**. The new rule now displays in the **Template Rules** section.

22. Repeat the above steps for any additional rules you need to apply to this template. For this particular example, we need two rules for this collection template. So, we would follow the above steps for ackLostBytes.

---

23. Click **Apply** when you have completed the template configuration and template rules.
24. Close the Probe Template Manager.
25. Right-click on your probe-enabled computer from the **Control Center** navigation tree and select **Commands > Probe > Refresh Configuration**. If you do not refresh the configuration, it automatically refreshes every four hours.
26. Wait for the collection to take place. This may take some time. Re-open your device window (e.g., Cisco 3620 Router) and click on the **SNMP Collected** tab.

Modify Collection Templates

To modify collection templates, follow the steps listed below:

1. From the **Collection Templates** tab, highlight the template to modify.
2. Make the necessary adjustments to the **Template Configuration** section.
3. If any changes need to be made to the rules, select the rule and click the **Edit Selected Rule** icon. Make the necessary adjustments and click **OK**.
4. Click **Apply** to save the changes to the template.
5. Open the probe-enabled computer from the **Control Center** navigation tree and select **Begin > Commands > Probe > Refresh Configuration** to update the probe.

Delete Collection Templates

If you decide to delete any collection templates, it also deletes any rules associated with the template.

To delete collection templates, follow the steps listed below:

---

1. From the **Collection Templates** tab, highlight the template to delete.
2. Click the **Delete** icon.
3. You are prompted to confirm removal. Click **Yes** to remove the template and any associated rules or **No** to cancel.
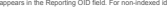
Use the OID Selector

The OID Selector lists all the object identifiers retrieved from the MIB files located in the %windir%\LTShare\ MIBs directory. Object identifiers are presented in a tree-like structure, which displays their logical associations. Selecting a node in the tree reveals information about the selected OID.

Field	Description
Name	The name of the object (e.g, sysObjectID).
Syntax	Displays how the data that the object identifier references, is formatted (integer, octet string, etc.).
Access Type	Displays the read/write access of the value.
Module(s)	The MIB file(s) that the OID information was retrieved from.
Augments	Displays the values that belong to a table, this displays the indexes that are required to access the data.
Descriptions	Displays the description of the object identifier.
Reporting Name	Name used when storing the values in the central database.
Reporting OID	OID used by the template.
MIB Files	To help narrow down the search process, select the Specific radio button in the MIB Files section and select the specific file from the drop-down menu. This shows you the OIDS from the selected file and any dependent OIDs. To load a custom MIB, select the Custom radio button and when prompted select the appropriate MIB file. Otherwise, if All Loaded is selected all current MIB files are loaded.

To use the OID Selector, navigate to the desired OID. If the OID is not part of the table (not indexed), then it appears in the Reporting OID field. For non-indexed identifiers, press the **OK** button to use the selected OID.

Indexed objects require specifying the value of the desired index. In the example below, the value was changed from 1 to 3 because port 3 was connected to a critical system component where monitoring was desired. Once the index has been changed, it appends to the value in the Reporting Name field and to the end of the Reporting OID.

To search for a specific OID, enter the string in the **Find:** field, and press the **Find Next** button.

Use the **Labels** menu to make the OIDs in the tree give more or less information. Label options include:

- Module: File the object was retrieved from.
- Name: Name of the object.
- OID: Object Identifier.
- Sub-ID: Object identification code for just the object (as opposed to the entire OID)

To help narrow down the search process, select the Specific radio button in the MIB Files section and select the specific file from the drop-down menu. This shows you the OIDS from the selected file and any dependent OIDs. To load a custom MIB, select the Custom radio button and when prompted select the appropriate MIB file.

Add a Collection Template with a Custom Table Walk Rule

Collection templates can have a variety of rules applied to them in order to determine the type of information they collect from detected devices. The Custom Table Walk option can be used to collect and store information to a custom table. This configuration is not recommended unless you are an advanced user.
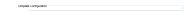
Create the New Collection Rule

To add a collection template with the custom table walk rule:

1. From the **Control Center**, select **Automation > Template > Probe Templates** and then click on the **Collection Templates** tab.
2. Prior to adding a collection template, look at the list of collection templates to see if there is already a template to avoid making duplicates.
3. Click on the **Add** icon. The **Template Configuration** values are cleared of data to allow you to enter the new information.
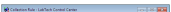
---

4. Enter the **Name** you want to give the template (e.g., Cisco 3620 Information).
5. Select **Template is sub-procedure**, if applicable. This allows them to be called from other templates, minimizing the need for duplication collections. Templates can only be sub-procedures or top-level templates (nesting templates is not allowed).
6. Select **Stop collection after this device** if you want this template to stop collecting data when it is finished with this device. This feature is typically only used when collecting data from antiquated devices to limit information stored.
7. Select the device from the **Apply to Device** drop-down that this template applies to. Please note that when you are creating collection templates based on information received from a walk, that the data may be available to all units for a specific make of device (e.g., all Cisco units) and thus should be applied to the base object and not a specific model. However, for our example, we only select the Cisco 3620 Router option.
8. Select the **Network Devices** and/or **Computers** checkboxes, if applicable. Selecting Network Devices and not **Computers** tells the template to run against only networked devices, not on computers with agents trying to self-collect.
9. Select the **Custom Storage Table** checkbox to store data to a custom table. Select the table from the database. The table must already exist in the database and the table name must begin with *probecustom_*. This table requires the following conditions:
   - The table name must start with *probecustom_*.
   - The table must have a DeviceID as the primary key (in addition to any other keys).
   - The table needs to have at least one column for the index (this column is used if the **Custom Table Walk** rule is selected later).
   - The table needs to have a column for each piece of data you wish to gather.
   - The table needs a LastUpdate column.
10. Click on the **Add New Rule** icon.

---

11. Enter the **Rule Name** (e.g., Custom Table OID Storage).
12. Select **Custom Table Walk** from the **Rule Type** drop-down.
13. Select a **Monitor Interval**, **Collection Interval** and **Historical Interval** for this rule, if necessary. Refer to the Adding Collection Templates section for detailed instruction on these fields.
14. Enter the addresses of the SNMP table that you wish to retrieve information from in the **OID** field.
15. In the **Index(es)** field, enter the indexes of the column(s) in your custom database table that holds the values for the indexes of the SNMP table that was defined in the **OID** field.
16. Enter the specified information that is retrieved from the targeted SNMP table in the **Data** field. This information must be in the format of <ColumnName>:<Index>;<ColumnName>:<Index>; etc. <ColumnName> is the name of a column in the specific custom table and <Index> is the field or property value from the SNMP table you wish to retrieve.
17. Click **OK** to save and apply this rule to the template.

Example Rule and Expected Results

Once the rule is set up, the expected results include the data from the fields (e.g., defined in the Data field) of the SNMP table (e.g., defined in the Data field). These results are stored in the custom table that was created earlier. All of the data that was collected and stored can be viewed by accessing the custom table in your database. The data in the rule should appear similar to the following:

The results that from the **Data** and **OID** fields are stored in the custom table that was created. In this example, there is a section for a network device that shows the data that we wish to collect:

This data above are collected via the new rule and stored in the custom database table that was created and defined earlier, as the example below shows: