[APPLICATION NOTE #195]

Setting up SNMP Monitoring Policies for APC UPS Devices

MANAGED SERVICES

Location
Single- or multi-location, network and tool dependent.

Applications
Networking Applications, Remote Monitoring and Management (RMM) tools, Custom Policies

Equipment
APC Smart-UPS

CUSTOMER BENEFITS

- **Build your own SNMP policies to address the needs of your installation.**
- **Use the APC PowerNet MIB and the inherent capabilities of your RMM tool to create policies, rules and actions.**
- **SNMP Custom policies are interoperable, flexible and can be refined and adapted over time.**
- **Use of existing network resources, no additional licensing cost.**
- **Build additional policies and rules to enhance monitor policies provided by APC for popular RMM tools.**

The purpose of this document is to assist APC by Schneider UPS users to define, build and deploy SNMP monitoring of their battery backup devices. This approach may also be applied to SNMP based monitoring of related Schneider-Electric products such as PDUs and other SNMP-enabled devices.

APC assists customers with SNMP based monitoring of health and performance of its UPS devices through two distinct mechanisms:

- SNMP Integration Kits for selected RMM or NMS tools
- Best practices documentation for SNMP based UPS monitoring (this application note)

The RMM Monitoring Sets are purpose-built monitoring integration kits for a select number of RMM tools and are available free of charge on apc.com. The monitoring kits deliver out of the box SNMP integration with the selected RMM tool to provide UPS monitoring based upon a fixed number of metrics. In those instances when an integration kit or manufacturer-built policies are not provided, this application note may be used by an IT administrator to build and deploy their own SNMP based monitoring policies or expand existing ones.

APC by Schneider Electric

Pre-requisites

In order to successfully monitor the UPS, the following pre-requisites exist:

- The UPS device must include a Network Management Card (NMC). The NMC enables SNMP communication between the UPS and the RMM application.
- A Monitoring tool with SNMP support must be in place to receive SNMP Traps and/or initiate SNMP commands to collect data from the UPS (SNMP polling). These tools may be referred to as Remote Monitoring and Management (RMM) platforms, Network Monitoring Systems (NMS) or simply as a SNMP Manager.
- The monitoring tool must be authorized to access the UPS device. Issues may arise, if the SNMP protocol is blocked from accessing the network by a router or a firewall.
- An RMM or NMS tool administrator needs to be familiar with configuring SNMP based monitoring and data collection (reporting). This includes experience with selecting metrics and defining thresholds for alerts.
- The administrator should have a basic understanding of SNMP based monitoring, MIBs and OID structure. Most network technicians or engineers would qualify or be able to work through the process.

SNMP Monitoring Highlights

SNMP is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. RMM or NSM tools can utilize SNMP to receive alerts about the status of a UPS, collect data to report on the performance of a UPS over time and to initiate specific changes to the UPS configuration remotely. Three versions of SNMP have been developed and are currently deployed and used globally. SNMPv1 is the original version of the protocol and more recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security. SNMP v1 remains the predominant version in production today and continues to be deployed in new implementations of remote monitoring.

The primary functions that can be executed from the monitoring tool are:

- SNMP Get: A “Get” command issued to a specific device will return a specific data item from the UPS (i.e. input voltage). Monitoring Set kits provided by APC support SNMP ‘Get’ queries.
- SNMP Set: The “Set” command is used to modify a UPS configuration item, if supported by the monitoring tool.
- SNMP Trap: While Gets and Sets are explicit commands issued from the RMM or NMS tools, the “Trap” is an alert initiated from the monitored device when a configured condition occurs (i.e. UPS goes on battery). The “Trap” is a message from the UPS that is directed at a specified “Trap Receiver” address which is generally part of the RMM or NMS.

Reporting capabilities are usually built into RMM platforms, and a system administrator is responsible for scheduling, generating and reviewing the report output. This is required for budgeting, maintenance and trend analysis. Reporting capabilities should be taken into consideration when selecting a RMM tool.

Actual data used within the UPS reports is comprised of the status alerts, traps and any SNMP data collections that were configured. The data collections are typically set to run periodically, (minutes, hours or days) to capture interesting data elements (i.e. battery life) to enable trend reporting.

MIB Hierarchy and OID structure

SNMP is the protocol and mechanism used to move the data the UPS presents. The management data is organized in hierarchies and defined and described in a structure called a Management Information Base (MIB). The actual data items made available through the MIB are defined by the UPS Vendor (in this case APC by Schneider) and not by SNMP. The management data items available are

referred to as variables and they are stored in hierarchical namespaces called Object Identifiers (OIDs). If a user wants to be alerted on a specific event (i.e. the UPS is on battery), then the specific OID for that management data item on the UPS must be known and configured within the RMM or NMS monitoring platform.

Reviewing the MIB and selecting the appropriate OIDs and variables is probably one of the more time consuming steps due to the complexity of SNMP formats and structure. To help accelerate this process, APC has provided a breakdown of the steps that are typically required to set up SNMP based monitoring (see *Table 1: Steps to Set Up SNMP Monitoring*).

Additionally, SNMP MIBS provide vast amounts of OIDs and data variables which can result in data overload, so it is critical to select the most appropriate OIDs for a given environment. The selection process may have to be iterative to suit a particular installation and to refine the operational procedures to manage the collected data. To accelerate this activity, APC has provided a list of suggested MIB OIDs and variables to consider as part of the monitoring implementation based upon our experience and best practices. This list is available on apc.com as a Manual under the section for Managed Services Integration Kits: (SNMP Monitoring, OID and Metrics Catalogue) http://www.apc.com/shop/us/en/categories/power/uninterruptible-power-supply-ups-/ups-management/managed-services-integration-kits/_/N-44hdb7

Once the RMM or NMS is configured to receive and recognize the selected alerts, the native configuration capabilities of the tool are used to:

1. Set appropriate thresholds so that the state change on the UPS is identified or received in the tool only when the condition is met

2. Configure the workflow or the RMM application to reflect how the tool will process the received data (alarm, ticket, notification).

Table 1 *– Steps to set up SNMP Monitoring*

Using the PowerNet MIB for APC UPS devices to set up custom SNMP Monitoring:
1. Identify the management data items that matter to your operations team for monitoring and reporting. For reference, a shortlist of monitoring data items, 'SNMP Monitoring, OID and Metrics Catalogue' is provided on apc.com under the Managed Services Integration Kits – product pages.
2. Enable the NMC on the UPS for SNMP, typically the read- only community string is 'public'.
3. Ensure you have a tool, often referred to as a MIB browser that will allow you to read the APC UPS MIB (APC PowerNet MIB). Most RMM or NMS tools include a MIB browser that can be used. Additionally, a number of free open source MIB browsers are available.
4. Within the RMM or NSM tool, there should be a mechanism to add SNMP Objects (the UPS device would be considered an SNMP Object). Within this area of the tool, you should be able to "browse" or view the MIB tree to see if the objects (UPS devices) you wish to monitor exist. If they exist, skip the next step.
5. If the UPS object is not in the tool's existing MIB tree, then download the current PowerNet MIB from the APC website and import it into the RMM or NSM tool.
6. Once imported (or "loaded"), the PowerNet MIB definitions should be available within the tree and the specific OIDs to be monitored can be selected. The browser should display the APC OID's MIB organized by product and management data element type. The actual steps (commands or menu selections) executed will most likely vary between RMM and NSM tools, therefore it is recommended to review the vendor's documentation prior to beginning this process.
7. Configure the RMM or NSM Tool to manage the SNMP traps sent by the monitored UPS devices. Often this is referred to as an "SNMP Trap Handler" or "Trap Receiver". Again, depending upon the RMM or NSM used, the vendor's documentation and/or support communities should be reviewed.
8. Several basic SNMP configuration items must be set to enable the RMM or NSM tool to communicate with the UPS. For example, when using Kaseya, ensure the SNMP option is enabled in your LAN Watch discovery job and that it is allowed to leverage an existing agent on a managed machine to periodically scan the local area network for any new devices. Again, each tool may define the process a little differently, however at a minimum the community string will need to be set for the devices (this will vary depending upon which version of SNMP is used)
9. Once the OID's have been identified, the RMM or NMS tool must be configured to "poll" (or get) the UPS status and to receive the traps from the UPS (presuming the Trap Receiver has been configured on the NMC). Within the RMM or NMS tool, the user can configure the frequency of the polling to collect the status and then, based upon the data returned, determine whether an alert should be generated or to simply store the status information for reporting purposes. The action or alerting capabilities are highly dependent on the capabilities of the RMM tool in use.
10. Test the polling and trap monitoring by creating specific events (e.g. disconnecting the battery on a test instance)
11. Refine over time: Periodically review the frequency and type of alerts generated to determine if the monitoring configuration needs to change: a. Ensure the events or alarms generated are in fact worth receiving b. Evaluate whether or not additional management data items should be monitored c. Ensure the frequency of polling ("Gets") are appropriate (i.e. is polling too frequent and creating unnecessary "noise" within the RMM or NMS and operations processes d. Are alarm thresholds set properly ensuring efficiency of operations

Things to be aware of:

- SNMP is an IP based protocol and will identify devices by, among other things, their IP address. Most UPS's with an NMC will probably have a private IP address which must be considered if the monitoring tool is on the public side of a router
- Be clear on which version of SNMP will be used to validate it is supported by the RMM or NMS as well as the target UPS
- Understand the differences between SNMP v1, v2 and v3 as it relates to security and flexibility. For example, SNMP v1 is the least secure of the three versions, however it is the most widely deployed