Using SNMP with Devio

This article provides an overview of the Simple Network Management Protocol (SNMP), as well as information on how it is used within Biamp's Devio platform.

What is SNMP?

Simple Network Management Protocol, or SNMP, is a set of standards defined by the IETF for the management of network devices. It allows network administrators to gather information about managed network devices, often with the ability to modify a device's settings, on devices that support it. It is often part of a broader Network Management System (NMS), and may require the assistance of your local Network Administrator for configuration.

There are several versions of SNMP currently, with the most common versions being SNMPv2c and SNMPv3. Most Network Management Systems support the latest version, SNMPv3, and should also provide the necessary SNMP services for any other SNMP clients that might be using an older version of SNMP. SNMP implementations are commonly comprised of a NMS that requires supporting devices across several versions of SNMP. Devio uses SNMPv2c, and is therefore widely supported across many different Network Management Systems that provide an SNMP tool.

Note: SNMPv2c indicates the simple community-based security scheme, similar to SNMPv1, which became the de facto SNMPv2 standard due to controversy surrounding the initial SNMPv2 security model. More on v2c below.

Devio SNMP basics

There are three major components in a SNMP network:

- **Managed Device** - commonly, network endpoints that will be monitored. (e.g. Devio CR-1, Devio SCR-20, Devio SCR-25)

- **Agent** - software that runs on the managed device and is responsible for translating device information to SNMP-specific format. This often has to be enabled and configured to communicate with the Network Management System. (i.e. This is software created by the manufacturer for relaying information of pertinent device attributes such as device states, connections, firmware versions, etc.)

- **Network Management System** - management station that runs the software required for monitoring the network devices. This contains the Management Information Base, or MIB. (e.g. Computer running Network Management Tool capable of SNMP)

Simply put, the SNMP agent will receive queries from the NMS for information pertaining to the Object Identifiers (OIDs) of the managed device. An object identifier can be thought of as the attribute that you are looking to monitor and/or modify. Each OID is unique and denotes specific characteristics of a managed device. The collection of these OIDs into
a hierarchical list is what makes up the MIB, or Management Information Base - essentially a master list of attributes available for monitoring/modifying. The OIDs will be noted in the MIB as a dotted list of integers. For example, the OID in RFC1213 for "sysDescr" is 1.3.6.1.2.1.1.1. Structure of Management Information Version 2.0 defines the notation used by MIB. The Devio MIB can be found on the Cornerstone Devio Documents page.

Protocol operations

The abilities of SNMP are, perhaps, most easily understood when the Protocol Data Units (PDU) are explained. You can think of the PDUs as being the available functions. SNMPv1 introduced five core protocol data units -- GetRequest, SetRequest, GetNextRequest, Response, and Trap -- with SNMPv2 adding two additional protocol data units -- GetBulkRequest and InformRequest.

- GetRequest/GetNextRequest/GetBulkRequest - The Get operation is a request sent by the Manager to the Agent. It is performed to retrieve one or more values from the managed device, and the Agent returns a Response with current values.
- SetRequest - This operation is used by the Managers to modify or assign a value to the managed device. The Agent returns a Response with the updated values.
- Response - an agent to manager acknowledgment for the Get and Set requests.
- Trap - Unlike the above commands which are initiated from the SNMP Manager, Trap(s) are initiated by the Agent. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
- Inform - started as a Manager to Manager PDU, but is now utilized as an Agent to Manager communication when an acknowledgement is required.

Security mechanism

Community-based security creates SNMP communities for establishing trust between SNMP Agent and manager. This means that the Agent and Manager have to be configured with the same SNMP community names in order to be able to successfully pass requests and notifications. An Agent, such as Devio, is capable of supporting three communities for read-only, read-write, and trap. Each community is capable of supporting a particular activity; read-only applies to GET requests, read-write applies to SET requests, and trap applies to Trap/Inform. Essentially, if a device isn't configured with the correct SNMP community name then it won't be allowed to perform that level of process.

Transport

SNMP utilizes the User Datagram Protocol (UDP) transport protocol. The SNMP Manager will send requests from an available source port to port 161 on the Agent, at which point the Agent will solely reply to the source port. When the Agent sends unsolicited notifications to the Manager (known as Traps) the Agent will use any available source port, and will send the response to port 162 of the Manager.
Configuring an NMS for Devio SNMP

Any Network Management System that provides an SNMP manager tool capable of SNMPv2c should be fully capable of monitoring the Object IDs (OIDs) available in Devio. You may want to speak with your organization's network administrator or IT department to see if they have a program in place that is capable of SNMPv2c already. Additionally, some networks may have more than one Network Management station per system, or several different systems for monitoring different network segments. Simply import the Devio Management Information Base (MIB) into the network management tool of your choosing, and then select the OIDs you would like to monitor for each device.

An example of configuring the ManageEngine MIB Browser can be found in the Devio SNMP Browser section of the Devio Help-file.

Troubleshooting SNMP in Devio

- Ensure SNMP is enabled within the Devio SAU - This should be enabled by default, however, many administrators will disable this when not in use to negate an security concerns.
- Determine if the SNMP Trap destination IP address and port have been correctly entered in the System Administration Utility.
- Confirm that the correct SNMP version is selected within your Network Management software - remember there are several different versions, and the NMS's SNMP tool has to know what version to be speaking with the device.
- Verify that the community string naming convention matches between the Agent and Manager.
- Check that you have a valid network path between the SNMP agent and SNMP manager. Ports 161 & 162 are utilized for requests and traps, so any necessary port forwarding will need to be configured as such.
- Confirm the correct OID is being specified by checking the MIB file for description.