OpenService, Inc. White Paper

NerveCenter™ 3.8: Node Classification

PublicationDate

Open Service, Inc | 110 Turnpike Road, Suite 308 | Westborough, MA 01581
www.open.com | 508.599.2000 | info@open.com

Contents

About Open Service, Inc.

Open (OpenService, Inc.) is the premier provider of network security management solutions that enable enterprises and service providers to continuously protect and manage mission-critical business information. More than 450 customers are using Open's SystemWatch and/or NerveCenter™ for network security management. Open's products are available globally through a network of VARs and direct sales. A privately held company based in Westborough, MA, Open is backed by venture capital and an equity stake taken by Veritas. For more information, please call 800-892-3646, or visit the Open web site at http://www.open.com.

Node Classification

NerveCenter™ 3.8 can communicate with devices that support any of the available versions of SNMP: v1, v2c, v3. All SNMP agents and network devices managed by NerveCenter, are represented as nodes in NerveCenter database. NerveCenter needs to know which version of SNMP to use when communicating with any of these agents. NerveCenter uses whatever SNMP version is assigned to the node object in NerveCenter database. Whenever a node is added to NerveCenter database, the node should have an SNMP version associated with it. Such SNMP version information can be assigned manually or automatically.

This white paper describes how NerveCenter identifies the SNMP version implemented on an agent and classifies the corresponding node object in the NerveCenter database. It also describes various ways NerveCenter uses to classify nodes. Finally, it describes how and when NerveCenter automatically classifies newly added nodes to its database.

The document is organized in following sections:

The Need for Node Classification

Every SNMP agent residing on a network device is represented by a corresponding node object in NerveCenter database. Attributes of the agent, such as IP address, port number, SNMP version, and other attributes known to NerveCenter, are stored as properties of the corresponding node object in NerveCenter database. Whenever NerveCenter needs to communicate with any SNMP agent it monitors, it uses the required attributes from the corresponding node object in its database. When communicating with any SNMP agent, NerveCenter constructs an SNMP version-specific message based on the node's version information available in the NerveCenter database. Similarly, when receiving a message from a known agent, NerveCenter uses the version information available in the corresponding node object in its database to decide whether to process the message. To communicate with the agent on a managed device, NerveCenter must use the same SNMP version configured at the agent.

Many SNMP agent implementations available in the market support multiple versions of SNMP. Today's more complex enterprise networks are expected to have agents from multiple vendors supporting varied combinations of SNMP versions. A sophisticated network management product like NerveCenter, therefore, must provide a way to specify the SNMP version to be used when communicating with each of these agents. In very large networks, specifying this version information manually for each device quickly becomes an unmanageable task.

NerveCenter can classify nodes automatically based on SNMP version implementation on the corresponding agent, or you can manually classify nodes on a case-by-case basis. Finally, NerveCenter lets you specify the SNMP version to use when NerveCenter communicates with the SNMP agent.

How NerveCenter Classifies a Node

NerveCenter tries to classify a node based on the highest version of SNMP implemented on the corresponding SNMP agent. You can, however, limit the highest version NerveCenter attempts to classify by specifying a maximum classification version in the NerveCenter Administrator. When you specify a maximum classification version, NerveCenter never attempts to classify a node above the version you specified.

When classifying a node, you need to know whether a particular version is supported on the corresponding agent, NerveCenter sends an SNMP GetRequest message and listens for the response. Receipt of an SNMP response or SNMP error indicates that the particular version is supported on the corresponding agent. If NerveCenter receives a response other than an SNMP reply, NerveCenter concludes that the particular version is not supported on the agent. To ascertain support for SNMP v1 and SNMP v2c, NerveCenter sends a GetRequest message for `SysObjectID` with a read community of `public`.

To ascertain SNMP v3 agents, NerveCenter sends the GetRequest message to discover the `snmpEngineID` at the agent on behalf of the 'initial' user, as specified in the suggested engine discovery mechanism in RFC 2574.

Note Whenever NerveCenter ascertains that an agent supports SNMP v3, NerveCenter also assigns a default security level for communication with the node as `NoAuthNoPriv`. Please refer to NerveCenter online help for details about changing a node's default security level or configuring an initial user on SNMP v3 agents.

Irrespective of the SNMP version of the node, NerveCenter always tries to ascertain the node's SNMP version with the "Maximum Classification Version" specified.

If NerveCenter does not get SNMP responses or SNMP errors to its GetRequest messages, then NerveCenter designates such nodes as 'unknown'. For details of the algorithm NerveCenter uses to classify nodes, see *Node Classification Algorithm* on page 7.

The you can also test a particular version specified on a node. In the NerveCenter Client, select the node from the node list view and selecting **Test Version** from the right mouse click menu. This Test Version is similar to the GetRequest discussed above. If the agent does not support the version specified on the node, you get a test version failed error message.

Specifying a Maximum Classification Version

You can specify the maximum classification version as the highest SNMP version up to which you want NerveCenter to classify a node. NerveCenter will never attempt to classify a node for any version above the version you specify here. For example, if you select v2, NerveCenter never tries to classify the node above SNMP v2c; that is, NerveCenter will never send SNMP v3 requests to any nodes.

Note If you want NerveCenter to detect whether SNMP v3 is supported at an agent, the agent must have an initial user configured for discovery. Please refer to the Agent Setup section in NerveCenter online help to know how to configure agents for discovery.

❖ **To set the maximum classification version:**

1. Open NerveCenter Administrator.
2. Connect to the NerveCenter Server.
3. Select the **Classify** tab.
4. Select the highest level you want to classify from the **Maximum Version** drop-down list box.
5. Select the **Save** button.

Classifying Nodes Manually

There are three different ways to manually classify nodes with NerveCenter:

- **Classify All Nodes** Admin menu option
- **Classify** option on the Node List window pop-up menu
- **Classify** button on the SNMP page of the Node Definition window

Note When NerveCenter attempts to manually classify a node, any earlier SNMP version-specific information for that node object in its database is lost. For example, if a node was marked earlier as an SNMP v3 node and as a result of a new manual classification, the node is now marked as 'unknown', then the SNMP v3-related security information such as security level and authentication protocol is lost. Also note that NerveCenter does not poll for nodes that have an SNMP version value of 'unknown'.

Classifying All Nodes

The Classify All Nodes option can be very useful when the user needs to classify all available nodes in NerveCenter database. NerveCenter classifies nodes using this option based on the highest supported SNMP version at the corresponding agents up to the 'maximum classification version' specified by the user. If NerveCenter cannot determine the supported SNMP version at any particular agent, it marks the version for the corresponding node object in its database as 'unknown' and assigns the `AutoClassifyFailed` error status to the node.

❖ **To use the Classify All nodes option:**

1. Open NerveCenter Client.
2. Connect to the NerveCenter Server.
3. From the **Admin** menu, select **Classify All Nodes**.

Classifying Select Nodes

Classifying select nodes can be useful when you only want to classify a group of selected nodes from all the available nodes in NerveCenter database. Like the Classify All Nodes option, NerveCenter classifies select nodes based on the highest supported SNMP version at the corresponding agents up to the 'maximum classification version' specified by the user. If NerveCenter cannot determine the supported SNMP version at any particular agent, it marks the version for the corresponding node object in its database as 'unknown' and assigns the `AutoClassifyFailed` error status to the node.

❖ **To classify nodes using the Client's Node List window pop-up menu:**

1. Open NerveCenter Client.
2. Connect to the NerveCenter Server.
3. From the **Admin** menu, choose **Node List**.
4. Select a group of nodes or node you wish to classify from the node list.

Note You can either use the Shift key + Left mouse button combination or use the Shift key + Down arrow key combination to select consecutive nodes from the node list. If you need to select nonconsecutive nodes from the node list, use CTRL key + Left mouse button combination.

5. Right-click to display the Node List window pop-up menu.
6. Select the **Classify** option.

Classifying a Node from the Node Definition Page

Classifying a node from the Node Definition page can be useful when you want to add a new node to NerveCenter database, and you are not sure about the SNMP version supported at the node's agent. If NerveCenter cannot determine the supported SNMP version at any particular agent, it marks the version for the corresponding node object in its database as 'unknown' and assigns the `AutoClassifyFailed` error status to the node.

❖ **To use Classify button on the SNMP page of the Node Definition window:**

1. Open NerveCenter Client.
2. Connect to the NerveCenter Server.
3. From the **Admin** menu, choose **Node List**.
4. Double-click the node from the node list you wish to classify.

   The Node Definition window displays.
5. Select the **SNMP** tab.
6. Click the **Classify** button to classify the node.

Classifying Nodes Automatically

In addition to manually adding and classifying nodes, NerveCenter can automatically detect agents on network devices it monitors and add the corresponding node objects for these automatically detected agents. Moreover, NerveCenter can be configured to recognize agents residing on network devices from other network management platforms like OpenView, another NerveCenter, and so on. In such circumstances, if the version information is not available about these automatically detected agents, NerveCenter assigns the version information to corresponding node objects as 'unknown'. Since NerveCenter does not poll nodes having 'unknown' version, its default behavior is to automatically classify these automatically detected agents.

When NerveCenter Attempts to Autoclassify Nodes

When NerveCenter's autoclassification feature is enabled, NerveCenter attempts to autoclassify a node in the following situations:

- When nodes are imported via a node file (using ImportUtil or NerveCenter Client), and a node has no SNMP version information or the SNMP version is 'unknown'. (Such a scenario might occur if you were importing nodes from a previous version of NerveCenter.)
- When nodes are imported from another NerveCenter Server, and a node has no SNMP version or the SNMP version of the node is 'unknown'.
- When a new node is added to the NerveCenter database because a trap was received from a corresponding agent or source previously unknown to NerveCenter.
- When NerveCenter is co-resident with OpenView Network Node Manager and OpenView sends nodes to NerveCenter. In this case, NerveCenter does not know the SNMP version of the newly added node from OpenView.

Note When NerveCenter receives SNMP v3 traps from unknown agents with an `AuthNoPriv` or an `AuthPriv` security level, then NerveCenter processes these traps on behalf of the poll user and in the poll context configured in NerveCenter. (See NerveCenter online help for more information.) When autoclassification is enabled, NerveCenter attempts to classify these unknown nodes up to the 'maximum classification version' specified by the user.

Enabling and Disabling Auto-classification

Follow the steps below to enable/disable the node auto-classification feature in the NerveCenter Administrator.

❖ **To enable or disable node auto-classification:**

Note When auto-classification is disabled, then NerveCenter sets the nodes discovered by OpenView as SNMP v1.

1. In the NerveCenter Administrator, select the **Classify** tab.
2. To enable auto-classification, check the **Auto Classify** checkbox.

   NerveCenter auto-classification is enabled for whichever version you select, but NerveCenter will never attempt to auto-classify a node for any version above your selection. For example, if you select v2, NerveCenter can send classification requests only for v1 and v2.
3. To disable auto-classification, uncheck the **Auto Classify** checkbox.

Note If you disable auto-classification, bear in mind that NerveCenter does not poll nodes whose SNMP version is unknown.

4. Select the **Save** button.

Performance Tuning for Node Classification

An enterprise network management product like NerveCenter is expected to monitor a huge network, and SNMP v3-specific operations for large numbers of nodes can cause bursts of traffic on the network. To help you to control this type of sudden SNMP v3-related rise of traffic on the network, the NerveCenter Administrator provides the Maximum Requests Per Cycle feature.

Whenever NerveCenter needs to:

- Automatically classify a group of nodes
- Manually classify a group of nodes
- Perform other SNMP v3-specific operations for a group of nodes

NerveCenter carries out these operations in small chunks of nodes specified by Maximum Requests Per Cycle. (As the cycle is approximately one second, this parameter is the number of requests per second.)

❖ To set the Maximum Requests Per Cycle:

Tip A good Maximum Requests Per Cycle is 500.

1. Open NerveCenter Administrator.
2. Connect to the NerveCenter server.
3. Select **Classify** tab.
4. In the **Maximum Requests Per Cycle** field, enter maximum number of requests you want NerveCenter to process approximately per second.
5. Select the **Save** button.

Node Classification Algorithm

The NerveCenter node classification algorithm is depicted in Figure 1:

Figure 1. NerveCenter Node Classification Algorithm