This document describes how to force NNMi to poll an interface, detailing an alternate solution, which we believe is better than previously published methods. This document provides a step-by-step example of the recommended process.
Problem Statement

By default, NNMi uses SNMP to monitor interfaces that are connected in the NNMi topology or router interfaces that host an IP address. You may run into situations that require NNMi to use SNMP to monitor additional interfaces. This paper describes the steps you need to complete to do this.

Solution

The easiest way to configure NNMi to monitor an interface is to create a monitoring configuration policy that monitors interfaces with a specific custom attribute. After you create this new monitoring policy, you need to put the specific custom attribute on the interface. Finally, from the NNMi console, run a configuration poll on the node to let NNMi know that it needs to monitor the interface.
Solution Example

Refer to the node called nat-inside-router-1 in Figure 1. This node currently only has two connected interfaces, Fa0/0 and Fa1/0.

Figure 1: The nat-inside-router-1 Node
Router `nat-inside-router-1` also has a loopback interface that NNMi is monitoring because it has an IP address hosted on the loopback interface. Suppose you also need to monitor Fa1/0. See the Setting up Polling section to learn how to monitor Fa1/0.

**Figure 2: Router nat-inside-router-1 Loopback Interface**

![Figure 2: Router nat-inside-router-1 Loopback Interface](image)

**Setting up Polling**

This section describes a *one-time action* that you do not need to do for each additional managed interface.
Creating an Interface Group

The first step is to create an interface filter based on custom attributes.

1. From the NNMi console, click Configuration.
2. Click Interface Groups.
3. Click the New button to create a new Interface Group as shown in Figure 2.

Figure 3: Opening the Interface Group Form
See Figure 2 for steps 4 through 7.

4. Click the **Additional Filters** tab.
5. For this example, name this group **ForcePoll**.
6. Set the **customAttrValue** to **true**.
7. Click **Save and Close** the **Interface Group** form; click **Save and Close** for any outer forms as well.

**Figure 4: Creating a New Interface Group**
Creating a Monitoring Configuration Policy

The next step is to create a monitoring configuration policy by following these steps:

1. Click the **Monitoring Configuration** workspace.

**Figure 5: Click the Monitoring Configuration Workspace**

```
[Image of HP Network Node Manager interface]
```

See Figure 4 for steps 2 through 3.

2. Click the **Interface Settings** tab; then write down the current ordering values.

3. Click the **New** icon.

**Figure 6: Opening the Interface Settings Form**
4. In the Interface Settings form shown in Figure 7, enter an Ordering value that is lower (higher priority) than the values that you wrote down from the previous form. Entering a lower value causes this policy to always apply to any interface with this Custom Attribute setting.

5. Select ForcePoll as the Interface Group.

**IMPORTANT:** You **MUST** select the following check boxes:
- Enable SNMP Fault Polling
- Poll Unconnected Interfaces Hosting IP Addresses under Extend the Scope of Polling Beyond Connected Interfaces
- Poll Interfaces Hosting IP Addresses under Extend the Scope of Polling Beyond Connected Interfaces

6. Select the Enable ICMP Fault Polling check box if you want to ping any IP addresses that might be hosted on this interface.

Note: This example does not include any IP addresses hosted on this interface.

7. Click **Save and Close** on this form; click **Save and Close** for any outer forms as well.

**Figure 7: Configuring the Threshold Settings**
Put the Custom Attribute on the Required Interface

1. Open the interface that you want to force to be polled. This is interface Fa1/1 in this example.
See Figure 8 for steps 2 and 3. Click the **Custom Attributes** tab.

2. Click the **New** button.

**Figure 8: Adding the New Custom Attribute**

3. Set the **Name** to **ForcePoll** and the **Value** to **true**. Note that this text is case sensitive.

4. Click **Save and Close**; click **Save and Close** for any outer forms as well.
5. Reopen the form; then click the **Interface Groups** tab. NNMi shows that interface Fa1/1 is now in the **ForcePoll** group.

**Figure 9: Interface Fa1/1 is in the ForcePoll Group**

Run a Configuration Poll and a Status Poll on the Node

See Figure 8 for steps 1 and 2.

1. You must run a configuration poll on the node in order to activate the **ForcePoll** monitoring configuration policy.
2. Follow the configuration poll by a status poll to get the most up-to-date status.

**Figure 10: Run a Configuration Poll and a Status Poll**
You can see NNMi poll the node in the Status Poll output shown in Figure 11

**Figure 11: Status Poll Output**

<table>
<thead>
<tr>
<th>Status Poll of 15.2.135.11 - Mozilla Firefox</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Using client timeout value of 600 secs</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy:</th>
<th>Object Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target:</td>
<td>15.2.135.11</td>
</tr>
<tr>
<td>Poller:</td>
<td>NmMibPoller, Target Responding: true, Poll Successful: true, Poll Duration: 142 mSec</td>
</tr>
<tr>
<td>Object:</td>
<td>chTspRutIfTrackedPriority</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td>15.2.135.11[3]</td>
<td>10 (10)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy:</th>
<th>SNMP Agent Availability Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targets:</td>
<td>15.2.135.11</td>
</tr>
<tr>
<td>Poller:</td>
<td>NmMibPoller, Target Responding: true, Poll Successful: true, Poll Duration: 196 mSec</td>
</tr>
<tr>
<td>Object:</td>
<td>sysUpTime isel18776 (Normal)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy:</th>
<th>Interface Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targets:</td>
<td>15.2.135.11</td>
</tr>
<tr>
<td>Poller:</td>
<td>NmMibPoller, Target Responding: true, Poll Successful: true, Poll Duration: 171 mSec</td>
</tr>
<tr>
<td>Object:</td>
<td>ifAdminStatus ifOperStatus</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>1 (Up) 1 (Up)</td>
</tr>
<tr>
<td>Lo0</td>
<td>1 (Up) 1 (Up)</td>
</tr>
<tr>
<td>Fa1/1</td>
<td>2 (Down) 2 (Down)</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>2 (Up) 2 (Up)</td>
</tr>
</tbody>
</table>
3. After you refresh the node form, you see the interface being polled. Although this is not the best example, as the status of this interface is currently **Administratively Down**, the combined procedures still explain how to solve the initial problem.

**Figure 12: Shows Interface Down**

![Image of HP Network Node Manager i-series Software Forcing and Interface to Be Polled](image)

**Conclusion**

NNMi is flexible enough to assist you if you need to use SNMP to monitor additional interfaces. You can configure NNMi to monitor additional interfaces using a monitoring configuration policy and a specific custom attribute that you define. You then add this attribute to the interface, so that the interface can be monitored using SNMP. You can accomplish this by following the steps presented in this paper.