# Introduction

This Microsoft Network Policy Server MP Version is based the NPS management pack received from [Tero Ilenius](http://social.technet.microsoft.com/Forums/en-US/winserverNAP/thread/999d9969-2a96-4dfd-abcc-a0cf9fe350f5) but is rebuild from scratch by Bas Sterkenburg.

This document is based on the 1.0.1.86 version of the Microsoft.NetworkPolicyServer management pack.

If you have any questions or suggestions please feel free to contact me at NPS@Sterkenburg.tv

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes |
| 1.0.1.69 | 26-04-2012 | First release |
| 1.0.1.70 | 04-05-2012 | Added sealed MP version; bugfix performance views  |
| 1.0.1.75 | 02-06-2012 | Created a custom data source module to made overrides to the NAS Port-Type eventlog parameter. The following two rules are configured with the custom data source* NPS: Authentication failed and the user was denied access
* NPS: Authentication successful and the user was granted access
 |
| 1.0.1.76 | 13-06-2012 | All classes and monitors are declared as public now |
| 1.0.1.80 | 27-06-2012 | Added a monitor to check the expiration date of the certificate |
| 1.0.1.82 | 05-07-2012 | Updated the “Connection Request Policy” and “Connection Network Policy” Discovery. A lot of the configured values are also translated now. See Discovery for more information. |
| 1.0.1.84 | 11-12-2012 | Created a custom data source module to consolidate repeating event based on the “Trigger on Count, Sliding” module. The following rule is configured with the custom data source* NPS: Authentication failed and the user was denied access
 |
| 1.0.1.85 | 06-05-2013 | Altered the “Network Policy Servers Discovery” discover target to “Windows Server” so the NPS role on a Server 2012 will also work. (Note: The MP is not tested on a 2012 NPS Server) |
| 1.0.1.86 | 09-07-2014 | Changed the “Network Policy Servers Discovery” back to discover only Server 2008 (R2) servers and renamed the discovery to “Network Policy Servers 2008 Discovery”. Added a new discovery “Network Policy Servers 2012 Discovery” to discover NPS on Server 2012 (R2).(Note: The MP is not tested on a 2012 NPS Server) |

# Discovery

The first discovery is targeted to all Windows Server to determine if NPS role is installed or not. The discovery checks for existence of registry key HKLM\System\CurrentControlSet\Services\IAS.

## Scripted configuration discovery

If the NPS role is installed there are 4 scripted discoveries to discover the configuration:

* Network Policy Server Client Configuration Discovery (*netsh nps show client*)
* Network Policy Server Connection Request Policy Configuration (*netsh nps show crp*)
* Network Policy Server Connection Network Policy Configuration (*netsh nps show np*)
* Network Policy Server Log Configuration Discovery

Changes made in NPS can take up to 8 hours to be discovered, because the discovery scripts run every 28800 seconds (8 hours).

The Request Policy Configuration and Network Policy Configuration Discoveries do have some limitations. The discovery of the Condition attributes is limited to 6 and for the Profile attributes to 10.

With version 1.0.1.82 most lot of values are also translated. As I couldn’t found a complete list with all possible values it could be that it is displayed as a hex value. If you have a value that is not translated please let me know and I will try to update the discovery script.

Note: If you need more attributes to be discovered then the class needs to be updated and the discovery script.

# Groups

There are two groups:

* NPS Server Enabled Performance Counters
* NPS Client Enabled

## NPS Server Enabled Performance Counters

The NPS servers are added to the “NPS Server Enabled Performance Counters group” when the NPS performance are enabled. This is based on a registry discovery: HKLM\SYSTEM\CurrentControlSet\services\IAS\Performance\Disable Performance Counters.

If the value “Disable Performance Counters” is 0 or does not exist the NPS performance counters are enabled on the server. The group set the ENABLE override to all the performance rules and monitors targeted to the “Network Policy Servers” class.

## NPS Client Enabled

Discovered radius clients are added to the NPS Client Enabled group when they are enabled within NPS. The group set the ENABLE override to all monitors targeted to the “Network Policy Server Client Configuration” class.

Note: NPS Authentication Clients performance counters are automatically created on the NPS server for each client when there is an authentication request. When a client is enabled within NPS but is not used (there are no NPS Authentication Clients performance counters) the monitors are still green and workflow warnings will appear in the OpsMgr event log on the NPS server. To avoid this disable the client within NPS.

# Monitors and Performance rules

There is a monitor, “NPS Performance Counters Disabled”, which monitors the “Disable Performance Counters” registry value. This monitor checks the value every 3600 seconds (1 hour). If you change the value of the key to 0 to enable the NPS performance counters the monitor will go to green. It can take some time however before the NPS performance counters will not show up in the performance view. This is because the discovery of the value that is used by the group discovery runs on a other schedule.

At this time only “NPS Authentication Server” and “NPS Authentication Clients” performance counters are monitored and collected.

## Certificate monitor

The “NPS Certificate Monitor” monitors the expiration date of the certificates in the personal computer store. The monitor uses PowerShell and has tree states:

* Critical state if certificate has less than 7 days validity before expiring
* Warning state if certificate has less than 21 days validity before expiring

When no certificate is found or when the certificate has more than 22 days validity before expiring the monitor is healthy.

# Alert Rules

Within the Alert rules the company knowledge presents a URL link to the MS TechNet site for more information about the alert.

## Configure: NPS: Authentication failed and the user was denied access

The default is to alert on all “Authentication failed and the user was denied access” event.

There are six overridable parameters to set for this alert rule.

* **Parameter**
* **ParameterOperator**
* **NasPortType**
* **TCSConsolidateParameter**
* **TCSIntervalSeconds**
* **TCSCompareCount**

The first 3 are used for the alert rule configuration, the last 3 are used for the “Trigger on Count, Sliding” condition detection.

**Parameter** is used to configure which evenlog parameter to use.

Configuration example: **Params/Param[14]** ;parameter 14 is used.

**ParameterOperator** is used to configure how the operator must behave.

Configuration examples:

* **MatchesRegularExpression**
* **DoesNotMatchRegularExpression**
* **Equal**
* **NotEqual**

**NasPortType** is used to filter on the value that is the output of the used parameter.

Nas Port-Type value examples:

* **Ethernet** ;used for 802.1x wired
* **Wireless - IEEE 802.11** ;used for 802.1x wireless
* **Virtual** ;used for VPN
* For more values see your NPS configuration

Configuration examples by using **ParameterOperator** configured as “**MatchesRegularExpression**” to alert only on NAS Port-Types “Ethernet” and “Wireless - IEEE 802.11” configure the **NasPortType** with: **^(Ethernet|Wireless - IEEE 802.11)$**

Or for alert only on NAS Port-Types “Ethernet”: **^(Ethernet)$**

For alerting on all NAS Port-Types except “Ethernet” and “Wireless - IEEE 802.11”: configure the **ParameterOperator** to “**DoesNotMatchRegularExpression**” and configure the **NasPortType** with: **^(Ethernet|Wireless - IEEE 802.11)$**

Or for alert on all on NAS Port-Types expect “Ethernet”: **^(Ethernet)$**

To filter out the event that is generated after the “authentication timer reauthenticate” configuration on the switch the rule has a consolidate condition.

**TCSConsolidateParameter** is used to configure which evenlog parameter to consolidate on during the condition detection. The default is configured for **Params/Param[2]** (FQDN). When there is already a open alert the repeat count will be updated by one.

**TCSIntervalSeconds** is used to configure the items occurrence within a time interval in seconds. The default is configured for **60 seconds**. This means that there must be x events (see TCSCompareCount) within 60 seconds before a alert is created.

**TCSCompareCount** is used to configure after how many repeated events a alert must be created. The default is configured for 2 events. So when 2 events occurs within the configured TCSIntervalSeconds a alert will be created.

# Event Collection

It me be wise to disable the “NPS: Authentication successful and the user was granted access” event collection rule in a large environment.

## Configure: NPS: Authentication successful and the user was granted access

The default is to collect all “Authentication successful and the user was granted access” events.

There are three overridable parameters to set:

* **Parameter**
* **ParameterOperator**
* **NasPortType**

**Parameter** is used to configure which evenlog parameter to use.

Configuration example: **Params/Param[14]** ;parameter 14 is used.

**ParameterOperator** is used to configure how the operator must behave.

Configuration examples:

* **MatchesRegularExpression**
* **DoesNotMatchRegularExpression**
* **Equal**
* **NotEqual**

**NasPortType** is used to filter on the value that is the output of the used parameter.

Nas Port-Type value examples:

* **Ethernet** ;used for 802.1x wired
* **Wireless - IEEE 802.11** ;used for 802.1x wireless
* **Virtual** ;used for VPN
* For more values see your NPS configuration

Configuration examples by using **ParameterOperator** configured as “**MatchesRegularExpression**” to collect only on NAS Port-Types “Ethernet” and “Wireless - IEEE 802.11” event configure the **NasPortType** with: **^(Ethernet|Wireless - IEEE 802.11)$**

Or for collecting only on NAS Port-Types events “Ethernet”: **^(Ethernet)$**

For collecting all NAS Port-Types events except “Ethernet” and “Wireless - IEEE 802.11”: configure the **ParameterOperator** to “**DoesNotMatchRegularExpression**” and configure the **NasPortType** with: **^(Ethernet|Wireless - IEEE 802.11)$**

Or for collecting only on NAS Port-Types events “Ethernet”: **^(Ethernet)$**

# Views

There are multiple views under Microsoft Network Policy Server for alerts, states, performance and events.