Purpose

This document describes how to configure the Nagios Cross Platform Agent (NCPA) to send passive check results to Nagios XI or Nagios Core using Nagios Remote Data Processor (NRDP).

Check results received from external devices / applications is what defines a **Passive** check. It's the responsibility of the external devices / applications to send the check results through, all Nagios [XI / Core] does is wait for the results *(as opposed to Active checks where Nagios [XI / Core] is responsible for performing the check on a schedule)*. Passive checks reduce the load on your Nagios [XI / Core] server by reducing the number of active checks run. Passive checks are also useful for security-related and asynchronous events you wish to monitor.

NRDP is a listener that receives the passive check results and submits them to Nagios [XI / Core]. It comes pre-installed on Nagios XI, adding it to Nagios Core is explained in this documentation.

Target Audience

This document is intended for use by Nagios XI or Nagios Core Administrators who want to understand how to configure NCPA to send passive check results.

Solution Overview

Configuring NCPA to work as a passive monitoring agent for remote machines is ideal for managed service providers and organizations with remote offices and roaming laptops.

Configuring the agent to operate in passive mode allows for a simple method of monitoring services and metrics behind firewalls, proxies, and private address spaces. Under most circumstances, no configuration or alteration of remote firewalls is required in order to implement this type of monitoring.

Firewall rules may be required to allow NCPA to send the outbound check results to the Nagios [XI / Core] server. The central NOC or datacenter where the Nagios [XI / Core] server is located will also need firewall

rules to allow the inbound check results to the Nagios [XI / Core] server. The required network port is TCP port 80 or 443.

Data communication between remote agents and the Nagios server may be encrypted to ensure secure transfers. Encryption is achieved when using HTTPS over port 443 using SSL/TLS certificates

With passive checks, it's the responsibility of NCPA to send the check results through to Nagios [XI / Core]. NCPA uses a scheduler to execute the checks on a regular basis, hence all the checks that need to be executed are defined in one of the NCPA configuration files.

This solution applies to NCPA running on any of the operating systems (OS) that Nagios Enterprises produces pre-built packages for. As of the time of writing this they are Windows / RHEL / CentOS / Oracle Linux / Ubuntu / Debian / SUSE SLES / openSUSE / Mac OS X / AIX.

Prerequisites

Before you continue following the instructions outlined in this document, you must have met the following prerequisites.

- The NDRP listener must be configured properly on the Nagios [XI / Core] server
  - Please refer to the following documentation on how to configure NRDP on Nagios XI:
    - Configuring Inbound Checks With XI
  - Please refer to the following documentation on how to install and configure NRDP on Nagios Core:
    - Installing NRDP From Source
- It is recommended to implement SSL/TLS for NRDP as per the following documentation (applies to either Nagios XI OR Nagios Core):
  - NRDP - Configuring SSL/TLS
- NCPA must be installed on your remote machine as per the following documentation:
  - Installing NCPA

Configuration Files

NCPA supports multiple configuration files, this allows you to separate your configurations to allow for seamless upgrades. The location for these files are as follows:

- Windows
  - `C:\Program Files (x86)\Nagios\NCPA\etc\ncpa.cfg`
  - `C:\Program Files (x86)\Nagios\NCPA\etc\ncpa.cfg.d\`
- All Other
  - `/usr/local/ncpa/etc/ncpa.cfg`
  - `/usr/local/ncpa/etc/ncpa.cfg.d/`

The `ncpa.cfg` is the main NCPA configuration file. This documentation will show you how to configure this file to enable passive checks to be sent to your Nagios [XI / Core] server using NRDP.

The `ncpa.cfg.d` directory is the location to store your NCPA Passive check configuration file(s). This documentation will show you how to create a file of passive check commands to be used by NCPA.

Editing Files

The following steps of this documentation you will be required to edit files.

In Windows, you will need to open the files in Wordpad to edit them. If you open them in Notepad they may not appear formatted correctly. You can of course use any other editor, Notepad++ or Geany are examples.

In Linux, you will need to edit the files using the vi text editor. To edit the `ncpa.cfg` file you would execute the following command:

```
sudo vi /usr/local/ncpa/etc/ncpa.cfg
```

When using the vi editor:

- To make changes press `i` on the keyboard first to enter insert mode
- Press `Esc` to exit insert mode
- When you have finished, save the changes in vi by typing `:wq` and press Enter

Configure ncpa.cfg

The first step is to configure the `ncpa.cfg` file to send passive check results to your Nagios [XI / Core] server using NRDP. You will need to provide your **NRDP URL**, **NRDP Token** and **hostname**. This example will use the following values:

- NRDP URL = `https://10.25.5.21/nrdp/`
- NRDP Token = `NRDP_T0k3n`
- hostname = `S1601`
  - This is how Nagios [XI / Core] will know what machine the check results came from

Open the `ncpa.cfg` file in your editor and locate the `[passive]` section:

```
[passive]
handlers = None
```

Configure handlers for NRDP:

```
[passive]
handlers = nrdp
```

In this same section is a `sleep` value:

```
sleep = 300
```

This has a default setting of 300 seconds (5 minutes). This is the frequency at which it will execute / send the passive checks. Change this value if required.

Locate the `[nrdp]` section:

```
[nrdp]
parent =
token =
hostname = NCPA 2
```

Update these values with the correct values for your environment, for example:

```
[nrdp]
parent = https://10.25.5.21/nrdp/
token = NRDP_T0k3n
hostname = S1601
```

This completes the changes required for the `ncpa.cfg` file. Save and close the file.

Configure Passive Checks

The next step is to create the configuration file that contains the passive check commands. The NCPA installer provides an example file in the `ncpa.cfg.d` directory called `example.cfg` and this will be used as a starting point for your passive checks. If you are using Windows and enabled passive checks when installing NCPA then a `nrdp.cfg` file was created (it is a copy of `example.cfg`).

Create a copy of the `example.cfg` file called `nrdp.cfg` in the `ncpa.cfg.d` directory using the following steps:

Linux / Mac OS X / AIX

```
cd /usr/local/ncpa/etc/ncpa.cfg.d/
sudo cp example.cfg nrdp.cfg
sudo chown nagios:nagios nrdp.cfg
```

Windows

Open a command prompt with administrative rights and execute the following commands:

```
cd "C:\Program Files (x86)\Nagios\NCPA\etc\ncpa.cfg.d"
copy example.cfg nrdp.cfg
```

If you are prompted to overwrite `nrdp.cfg` then the file already exists, you don't need to overwrite it.

Define Passive Checks

Open the `nrdp.cfg` file in your editor and you will see the following:

```
#[passive checks]

#%HOSTNAME%|__HOST__ = system/agent_version
#%HOSTNAME%|CPU Usage = cpu/percent --warning 60 --critical 80 --aggregate avg
#%HOSTNAME%|Swap Usage = memory/swap --warning 60 --critical 80 --units Gi
#%HOSTNAME%|Memory Usage = memory/virtual --warning 80 --critical 90 --units Gi
#%HOSTNAME%|Process Count = processes --warning 300 --critical 400
```

A detailed explanation of how these commands are defined can be found in the following documentation: https://www.nagios.org/ncpa/help/2.0/passive.html#configuring

The `[passive checks]` section and five example commands all begin with a **#** symbol. This means that they are commented out and they are not being used. Simply remove the a **#** symbol to make the checks active. Make sure you remove the **#** before `[passive checks]` to enable passive checks.

You can see that there is no disk usage check in the example file, this is simply because there is no easy example that fits all scenarios as each OS has a different way of addressing disks. Here is an example you can add to the `nrdp.cfg` file to check the used disk space with a warning at 80% used and critical at 90% used. A separate example for Windows and Linux / Mac OS X / AIX is provided on the following page.

Linux / Mac OS X / AIX

This example checks the used disk space on the `/` (root) mount. In NCPA all `\` and `/` must be represented as the `|` (pipe symbol).

```
#%HOSTNAME%|Disk Used root = disk/logical/|/used_percent --warning 80 --critical 90
```

Windows

This example checks the used disk space on the `E:\` drive. In NCPA all `\` and `/` must be represented as `|` (pipe symbol).

```
#%HOSTNAME%|Disk Used E = /disk/logical/E:|/used_percent --warning 80 --critical 90
```

Note: You cannot use the `:` (colon) in the service name otherwise it will cause that command to fail.

This completes the changes required for the `nrdp.cfg` file. Save and close the file.

Restart Service

You need to restart the NCPA Passive service to apply the changes you just made. The command required for this will differ depending on your OS and version.

Windows

```
net stop ncpapassive
net start ncpapassive
```

RHEL / CentOS / Oracle Linux 5.x / 6.x

```
service ncpa_passive restart
```

RHEL / CentOS / Oracle Linux 7.x

```
systemctl restart ncpa_passive.service
```

Ubuntu 12.x / 13.x / 14.x

```
sudo service ncpa_passive restart
```

Ubuntu 15.x +

```
sudo systemctl restart ncpa_passive.service
```

Debian 7.x

```
service ncpa_passive restart
```

Debian 8.x +

```
systemctl restart ncpa_passive.service
```

openSUSE / SUSE SLES 11.x

```
sudo /sbin/service ncpa_passive restart
```

openSUSE Leap 42.x + / SUSE SLES 12.x +

```
sudo systemctl restart ncpa_passive.service
```

AIX

```
stopsrc -s ncpa_passive
startsrc -s ncpa_passive
```

Mac OS X

```
sudo launchctl stop org.nagios.ncpa_passive
sudo launchctl start org.nagios.ncpa_passive
```

Now that the `ncpa_passive` service has been restarted the next step will be to check that Nagios [XI / Core] is receiving the check results.

Check Nagios

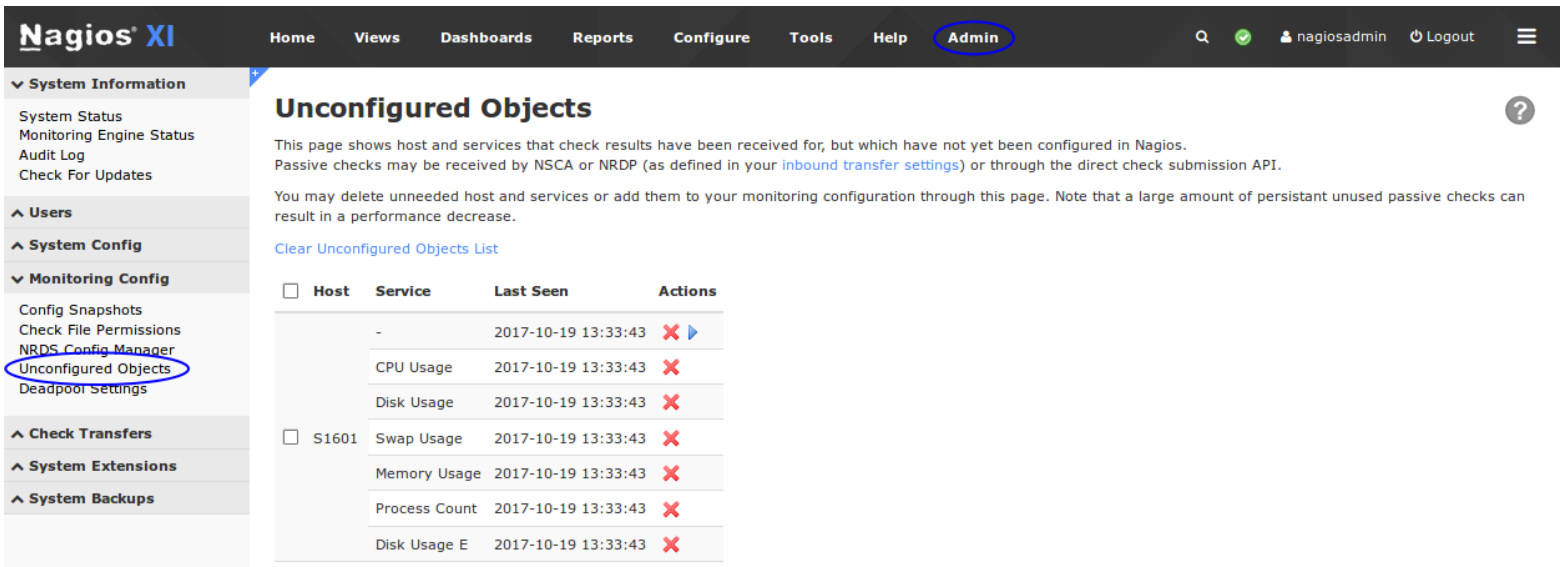
Now that NCPA is configured it will start sending passive check results to your Nagios [XI / Core] server. You can check to see if they have been received as they will be logged in the `nagios.log` file. Execute the following command on your Nagios XI server to check the log file:

```
grep 'Error: Got' /usr/local/nagios/var/nagios.log
```

The output should be something like the following:

```
[1508380204] Error: Got host checkresult for 'S1601', but no such host can be found
[1508380204] Error: Got check result for service 'CPU Usage' on host 'S1601'. Unable to find service
[1508380204] Error: Got check result for service 'Disk Usage' on host 'S1601'. Unable to find service
[1508380204] Error: Got check result for service 'Swap Usage' on host 'S1601'. Unable to find service
[1508380204] Error: Got check result for service 'Memory Usage' on host 'S1601'. Unable to find service
[1508380204] Error: Got check result for service 'Process Count' on host 'S1601'. Unable to find service
[1508380204] Error: Got check result for service 'Disk Usage E' on host 'S1601'. Unable to find service
```

Don't be alarmed that they are error messages, this is simply because Nagios [XI / Core] does not have any object definitions for these check results so it cannot process them. If you have Nagios XI you will see these appear under **Admin** > **Monitoring Config** > **Unconfigured Objects**.



Configure Nagios

Now that Nagios [XI / Core] is receiving the check results you need to create the host and service objects so they will be correctly processed.

Nagios XI

Please refer to the steps in the following documentation to create the monitoring objects:

Monitoring Unconfigured Objects With XI

Nagios Core

Please refer to the following KB article which provides you with example host and service definitions for Nagios Core:

NRDP - Passive Host And Service Definitions

Once you have created the objects in Nagios [XI / Core] you will be successfully using NCPA for passive checks.

Further Reading

The NCPA agent has built-in documentation in web interface, this is located on the **Help** tab. This gives the options to view or change configuration settings remotely as well as access additional info on NCPA. This is also available on the official NCPA website.

Finishing Up

This completes the documentation on using the Nagios Cross Platform Agent for Passive Checks.
If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb