Using Nagios Cross-Platform Agent (NCPA) v3 for Passive Checks

Purpose

This document explains how to configure the Nagios Cross Platform Agent (NCPA) version 3 to send passive check results to Nagios XI or Nagios Core using the Nagios Remote Data Processor (NRDP).

Passive checks are defined by check results received from external devices or applications. It is the responsibility of these external devices or applications to send the check results, while Nagios simply waits for them. This contrasts with active checks, where Nagios is responsible for executing the checks on a schedule. Passive checks reduce the load on your Nagios server by decreasing the number of active checks performed. They are also useful for monitoring security-related and asynchronous events.

NRDP is a listener that receives passive check results and submits them to Nagios. It comes pre-installed with Nagios XI, and instructions for adding it to Nagios Core are provided in this documentation.

Solution Overview:

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

Running the agent in passive mode provides a straightforward method for monitoring services and metrics behind firewalls, proxies, and private address spaces. In most cases, no configuration or modification of remote firewalls is required to implement this type of monitoring.

However, firewall rules may be necessary to allow NCPA to send outbound check results to the Nagios server. The central NOC or data center where the Nagios server is located must also have firewall rules in place to allow inbound check results. The required network port is TCP 80 or 443.

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

With passive checks, NCPA is responsible for sending check results to Nagios. NCPA uses a built-in scheduler to execute checks at regular intervals, and all necessary checks are defined in one of the NCPA configuration files.

This solution applies to NCPA running on any operating system (OS) for which Nagios Enterprises provides pre-built packages. You can review this guide to learn more about supported OS':

Installing NCPA

Prerequisites

Before proceeding with the instructions in this document, ensure you have met the following prerequisites:

- The NDRP listener must be configured properly on the Nagios server.
  - For instruction on configuring NRDP on Nagios XI, refer to:
    - Configuring Inbound Checks with XI
  - For in instructions on installing and configuring NRDP on Nagios Core, refer to:
    - Installing NRDP From Source
- It is recommended to enable SSL/TLS for NRDP for secure communication. Refer to the following documentation (applies to both Nagios XI and Nagios Core):
  - NRDP – Configuring SSL/TLS
- NCPA must be installed on your remote machine. Follow the installation guide:
  - Installing NCPA

Configuration Files

NCPA supports multiple configuration files, allowing you to separate configurations for easier management and seamless upgrades. The locations of 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 Operating Systems:

```
/usr/local/ncpa/etc/ncpa.cfg
/usr/local/ncpa/etc/ncpa.cfg.d
```

The `ncpa.cfg` file is the main NCPA configuration file. This document will guide you through configuring this file to enable passive checks to be sent to your Nagios server using NRDP.

The `ncpa.cfg.d/` directory is used to store additional configuration files for NCPA passive checks. This document will also explain how to create and manage passive check configuration files in this directory.

Editing Files

Windows

- Use WordPad to edit these files, as Notepad may not display them correctly.
- You can also use alternative text editors such as Notepad++ or Geany.

Linux

- Use the `vi` text editor to modify files. To edit the `ncpa.cfg` file, run:

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

- When using the vi editor:
  - Press `i` to enter **insert mode** and make changes
  - Press **ESC** to exit **insert mode**
  - To save and exit, type `: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 server using NRDP:

1. Configure Handlers for NRDP by modifing the `[passive]` section setting as follows:

   Original:

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

   Change to:

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

2. The Sleep Interval determines how often passive checks are executed and sent. It's by default set to 300 seconds (5 minutes). Adjust as needed:

```
Sleep = 300
```

3. Locate and configure the `[nrdp]` section with values from your environment. For example:

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

4. Save and close the `ncpa.cfg` file by pressing **ESC**, then `:wq`, then **Enter**.

Configure Passive Checks

The next step is to create a configuration file that defines the passive check commands. The NCPA installer provides an example file named `example.cfg` in the `ncpa.cfg.d` directory, which will serve as a starting point for configuring passive checks.

- **Windows:** If you enabled passive checks during the NCPA installation, a file named `nrdp.cfg` was automatically created as a copy of `example.cfg`.
- **Linux/Mac OS X:** You will need to manually create a copy of `example.cfg`

To create the `nrdp.cfg` file in the `ncpa.cfg.d` directory, follow these steps:

Linux / Mac OS X

Open a terminal and execute the following commands:

```
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 privileges and run the following commands:

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

Define Passive Checks

Open the `nrdp.cfg` file in your editor. You will see the following default configuration:

```
#[passive checks]

#%HOSTNAME%|__HOST__ = system/agent_version
#%HOSTNAME%|Disk Used root = disk/logical/|/used_percent --warning 80 --critical 90
#%HOSTNAME%|Disk Usage = disk/logical/C:|/used_percent --warning 80 --critical 90 --units Gi
#%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
```

For a detailed explanation of how these commands are defined, refer NCPA Passive Check Configuration.

Enabling Passive Checks

The `[passive checks]` section and the five example commands are commented out (disabled) by default, as indicated by the `#` symbol at the beginning of each line.

To active these checks:

1. Remove the `#` symbol at the beginning of each line you want to enable
2. Ensure that `[passive checks]`is also uncommented to activate passive checks.

Adding a Disk Usage Check

Disk paths vary between operating systems. Below are examples you can add to `nrdp.cfg` to monitor disk usage.

Linux / Mac OS X

This check monitors the used disk space on the `/` (root) mount, with a warning at 80% and a critical alert at 90%:

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

Note: In NCPA, all `\` characters must be replaced with the `|` (pipe) symbol

Windows:

This check monitors the used disk space on the `E:\` drive, triggering a warning at 80% and a critical alert at 90%:

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

Note: Do not use a `:` (colon) in the service name, as it will cause the command to fail.

Once you have made the necessary changes, save and close the `nrdp.cfg` file.

Restarting Services

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 ncpa
net start ncpa
```

- RHEL / CENTOS / Oracle Linux 7.x+

```
systemctl restart ncpa
```

- Ubuntu 16.x +

```
sudo systemctl restart ncpa
```

- Debian 9.x +

```
systemctl restart ncpa
```

- SUSE SLES 15.x +

```
sudo systemctl restart ncpa
```

- Mac OS X

```
sudo launchctl stop com.nagios.ncpa
sudo launchctl start com.nagios.ncpa
```

Now that the `ncpa` service has been restarted, the next step is to verify that Nagios is receiving the check results.

Verify Results in Nagios

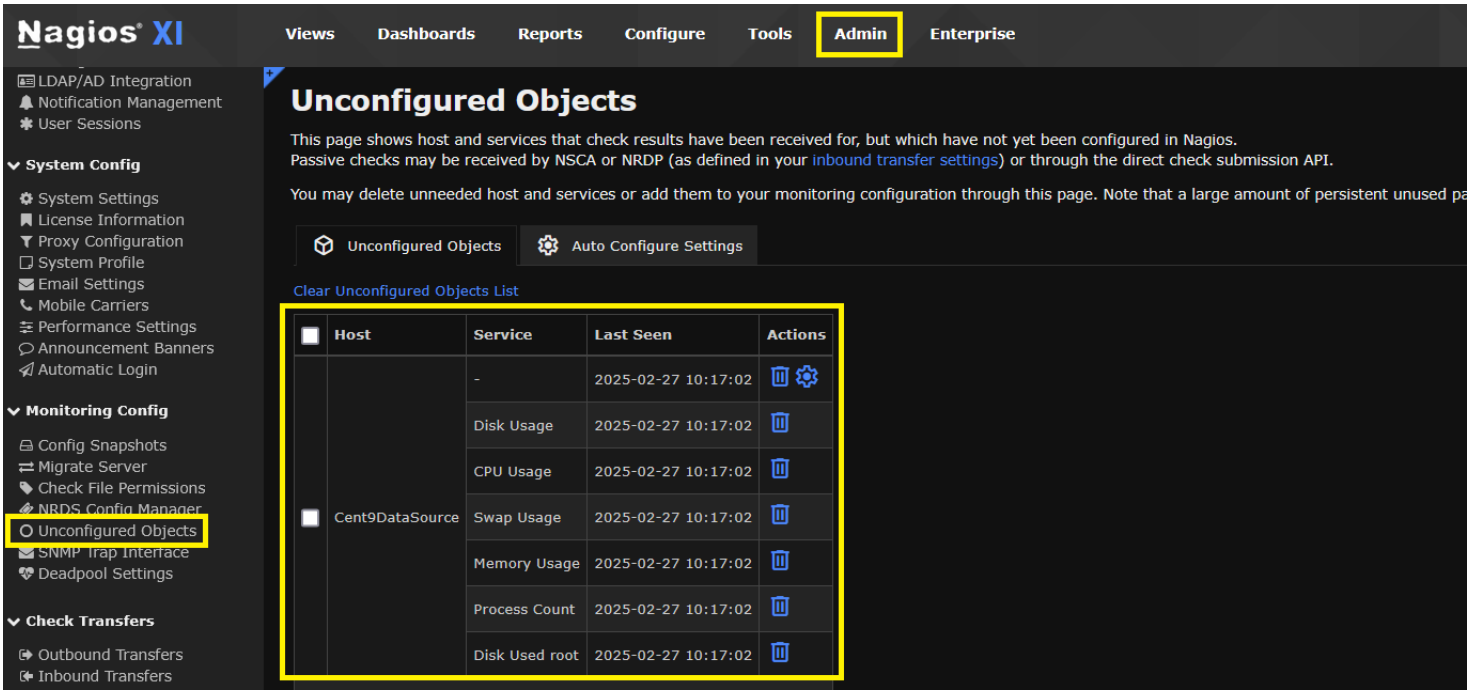
Now that NCPA is configured, it will begin sending passive check results to your Nagios server. You can verify if they have been received by checking the `nagios.log` file. Run the following command on your Nagios XI server to check the log:

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

The output should look something like:

```
[1739848245] Error: Got host check result for 'S1601', but no such host can
be found
[1739848245] Error: Got check result for service 'CPU Usage' on host
'S1601'. Unable to find service
[1739848245] Error: Got check result for service 'Disk Usage' on host
'S1601'. Unable to find service
[1739848245] Error: Got check result for service 'Swap Usage' on host
'S1601'. Unable to find service
[1739848245] Error: Got check result for service 'Memory Usage' on host
'S1601'. Unable to find service
[1739848245] Error: Got check result for service 'Process Count' on host
'S1601'. Unable to find service
[1739848245] Error: Got check result for service 'Disk Usage E' on host
'S1601'. Unable to find service
```

Don't be alarmed by these error messages—they simply indicate that Nagios does not yet have object definitions for these check results, so they cannot be processed. If you are using Nagios XI, you can find these unconfigured objects under **Admin** > **Monitoring Config** > **Unconfigured Objects**:



Configure Nagios

Now that Nagios is receiving the check results you need to create the host and service objects to ensure they are properly processed.

Nagios XI

Follow the steps in the following documentation to create the required monitoring objects:

Monitoring Unconfigured Objects With XI

Nagios Core

Refer to this KB article for example host and service definitions for Nagios Core:

NRDP – Passive Host And Service Definitions

Once you have created the objects in Nagios you will be successfully using NCPA for passive checks.

Finishing Up

This completes the documentation on Using Nagios Cross-Platform Agent (NCPA) for passive checks. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library