NCPA – Agent Installation Instructions

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to install the NCPA monitoring agent for Nagios on Windows and Linux machines. NCPA stands for Nagios Cross Platform Agent and is intended to simplify and universalize agent-based monitoring across different operating systems.

Target Audience

This document is intended for use by Nagios Administrators who wish to use NCPA to monitor servers. NCPA simplifies Admin's monitoring configurations and maintenance by allowing Nagios to monitor servers using the same agent regardless of platform.

NCPA Installation Overview

NCPA is packaged for all of its target platforms, including Windows, Linux (RPM and DEB), and Mac OS X as well as allowing source downloads to build packages for any system. While our build documentation and git repo have information on what is necessary to build NCPA, not all platforms will require exactly the same dependencies. This document is about installing the built packages though, which is straightforward for each type of system.

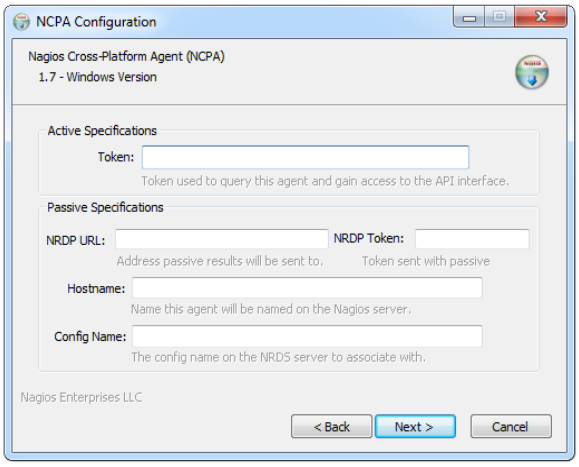
During the installation, you should note your firewall configuration. The install instructions do not explicitly state you need to open a port on your server's firewall, but depending on your systems installation and current firewall rules you may need to open the NCPA listener port 5693 which is the port NCPA receives checks from and displays the web UI on. If you cannot access the NCPA web interface after installation, check your firewall configuration. More information on how to manage your firewall settings are located in the **Configuring Windows Firewall for NCPA** and **Configuring Linux iptables for NCPA** sections of this document.

Downloading NCPA Installers

We have made a few pre-build installers for most popular systems available for each release of NCPA. You can download them from the nagios website at the official Nagios NCPA Builds page.

Installing NCPA on a Windows Machine

First, download the installer from the Nagios NCPA Builds page onto to the machine that you wish to install NCPA. Navigate to the location that the installer executable was downloaded, and double-click the installer. After agreeing to the license terms, you will find the configuration screen. This asks you to fill in some information for the NCPA configuration.



The first thing you will see is the Active Specifications section. NCPA can be used as an active agent by simply entering a token into the text box and clicking **Next**. This is the token that the NCPA agent will use as its form of authentication. You must remember this token, and enter it when configuring the device within the Nagios interface.

The fields following the token field are not necessary in order to get an active agent up and running on your system. If you are setting up the agent to send passive results back to Nagios, the additional pieces of information and specifications are required to continue.

NRDP URL:
This is the URL that the NCPA passive agent will send its check results and is set up in Nagios XI under **Admin → Inbound Transfers → NRDP**

NRDP Token:
This is the token you will be using when passing NCPA passive checks to Nagios for NRDP to accept the check. This is separate from the above token that is only used for active checks.

Revision 1.1 – August, 2014

Hostname:
The host that the passive agent will report service check status to in Nagios.

Config Name:
This is the NRDS config name that the agent will request when contacting the NRDS server.

After clicking **Next**, you will be asked to select a destination folder for NCPA on your Windows machine. Click **Install** and your machine will now have the NCPA services installed and started.

Silent Installations on Windows Machines

The installer also supports a silent install, which allows system administrators to easily manage their network workstations without disrupting the workflow of the office. There are four specifications currently supported by the NCPA installer, which are all analogs to the directives in the GUI installer. The following are the names of the directives that are available for a silent install.

TOKEN:
The token that will be used to access the agent's API and web interface.

NRDPURL:
This specifies the NRDP URL to use if passive checks are being implemented.

NRDPTOKEN:
This is the token that will be used to authenticate NRDP passive checks and to authenticate with NRDS.

HOST:
The host that the passive agent will report service check status to in Nagios.

CONFIG:
The name of the NRDS config the agent will be associated with.

All of the above directives are to be used as arguments from the command line of your windows machine:

```
ncpa-<version>.exe /S /directive=value
```

Below is an example of a command line install providing only a token for an active check:

```
ncpa-<version>.exe /S /token=welcome
```

This will set up NCPA on your windows machine with a token of "welcome" and start NCPA listener. If you wanted to set up NCPA for passive checks you would need to provide the NRDPURL, NRDPTOKEN, HOST and CONFIG directives as well.

To test your installation see the ***Testing Your Installation*** section of this document.

Installing NCPA On Linux Using RPM Packing (Red Hat/CentOS/OpenSUSE)

First, acquire the latest RPM package for your system from the Nagios NCPA Builds page. Download this to the machine you would like to monitor *not* to your personal workstation or your Nagios server.

Using the command line to download the RPM will look something like this:

```
cd /tmp
wget <link to rpm file>
```

Now that we have our RPM on our system (file will be named similar to ncpa-<version>.*<os type>*.*<x86|x64_86>*.rpm), we simply need to use our package manager to install it. Many commonly used package managers have the ability to install a local package. However, in this example we will use the rpm command. If you are using something like yum or zypper you can use that as well.

```
rpm -ivh --nomd5 <downloaded RPM file>
```

Now the NCPA services are installed and started. You will need to modify /usr/local/ncpa/etc/ncpa.cfg to specify a community string in the [api] section and set it to your token.

```
[api]
community_string=XXXXXX
```

After making changes to the ncpa.cfg, restart the ncpa_listener for the changes to take affect.

```
/etc/init.d/ncpa_listener restart
```

To test your installation see the ***Testing Your Installation*** section of this document.

Installing NCPA On Linux Using DEB Packaging (Ubuntu/Debian)

This section is largely the same as the RPM section. First, acquire the latest DEB package for your system from the Nagios NCPA Builds page. Download this to the machine you would like to monitor *not* to your personal workstation or your Nagios server.

In the example we will use the command line to download it:

```
cd /tmp
wget <link to file>
```

Now that we have the DEB on our system (file will be names similar to ncpa-<version>.*amd64*.rpm), we simply need to install it. You can use any package manager you are comfortable with, but for the sake of portability, this example will use dpkg to install this particular package.

```
dpkg -i <downloaded DEB file>
```

Now the NCPA services are installed and started. You will need to modify /usr/local/ncpa/etc/ncpa.cfg to specify a community string in the [api] section and set it to your token

```
[api]
community_string=XXXXXX
```

After making changes to the ncpa.cfg, restart the ncpa_listener for the changes to take affect.

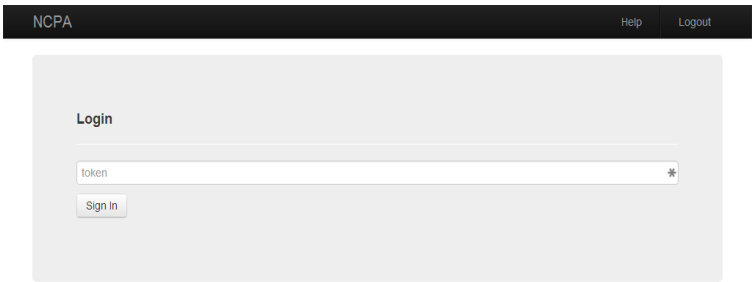
```
/etc/init.d/ncpa_listener restart
```

To test your installation see the ***Testing Your Installation*** section of this document.

Testing Your Installation

To ensure that installation was successful, try accessing the web interface of the agent. In order to do this you will need to know:

- The agent's IP address
- The token specified under [api] community_string (This is the token field in the Windows installer)



Once you have these pieces of information you can attempt to connect to the web interface using the following URL:

```
https://<agent's IP>:5693/
```

In the example URL above, `<agent's IP>` should be substituted for your agent's IP address. When you access the web interface of NCPA you should be asked to provide the token (the community_string in the config file) from above.

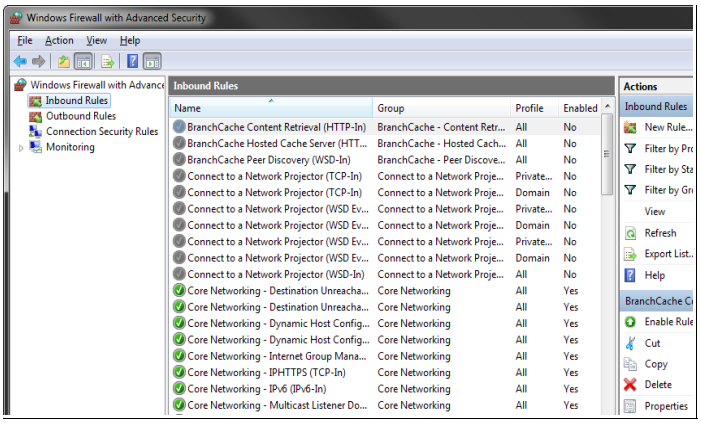
If you see this web page, it means that your NCPA installation is working properly – congratulations! As noted previously in the Installation Overview, if you get an error when trying to access this page immediately after installation, make sure your firewall is allowing traffic through on port 5693.

Configuring Windows Firewall for NCPA

You may have to enable some inbound firewall rules in order to view the NCPA dashboard via a web browser and allow Nagios to communicate with NCPA on port 5693.

In Windows, this can be done by following these steps:

1. Open up the **Control Panel**, click **System and Security**, then click **Windows Firewall** and go to the **Advanced Settings**
2. Click **Inbound Rules** in the left-hand panel and then click **Action** → **New Rule...**
3. Select **Port** and click **Next**
4. Select **TCP** and **Specific local ports**, and enter in **5693** then click Next
5. Leave all settings the same and click **Next**
6. Configure **Domain**, **Private**, and **Public** as required in your environment and click **Next**
7. Give the rule a name ("NCPA Inbound" works just fine) and an optional description, then click **Finish**



Configuring Linux iptables for NCPA

In Linux, only a few commands are needed to alter the iptables to allow NCPA to communicate with the Nagios server on port 5693. First you will need to edit your iptables rules list found in /etc/sysconfig/iptables (by default in CentOS systems) with your favorite text editor (we used vi) to add the following rule:

```
vi /etc/sysconfig/iptables
```

Add the following line to the OUTPUT ACCEPT section:

```
-A INPUT -p tcp --dport 5693 -j ACCEPT
```

Finally restart the iptables service to pick up the new rule we entered.

```
service iptables restart
```

Additional Documentation in the Web UI

Every install of the NCPA agent has built-in documentation and web interface located in the **Help** tab of the web UI (https://<agent's ip>:5693/). This gives the options to view or change configuration settings remotely as well as access additional info on NCPA.

Finishing Up

Now that NCPA is installed on the remote machine, you can monitor the machine using the NCPA monitoring wizard in Nagios XI.

If you have any questions about using NCPA, please contact our technical support team on our support forum at: http://support.nagios.com/forum