How To Use the Nagios XI 2024 NSCA Addon

Purpose

This document describes how to use the Nagios XI 2024 NSCA Addon.

NSCA Overview

The NSCA addon consists of two parts:

- A server application that runs on your Nagios XI server and listens for client data transfers
- A client application that runs on remote systems and is used by external applications to send data to the Nagios XI server

Communication between clients and the server can be encrypted to ensure secure data transfer.

Configuration On The Nagios XI Server

NSCA is part of the Nagios XI distribution and is already installed and partially configured.

To enable and use NSCA on your Nagios XI server, you must perform the following steps:

- Enable Remote Access
- Restart xinetd
- Open Firewall Ports
- Configure NSCA Settings

These steps require you to establish a terminal session to your Nagios XI server as the root user.

Enable Remote Access

By default, NSCA can only allow connections from the Nagios XI server itself. To allow remote hosts and applications to send passive results to Nagios XI you will need to configure access.

To do this, open the following file in vi:

```
vi /etc/xinetd.d/nsca
```

When using the vi editor, to make changes press **i** on the keyboard first to enter insert mode. Press **Esc** to exit insert mode.

Nagios®

Edit the `only_from` variable to include the specific IP addresses you want to allow to send passive checks to Nagios XI. This is a space delimited list. To allow traffic from 192.168.4.111 you would make the change below:

```
only_from       = 127.0.0.1 192.168.4.111
only_from       = 127.0.0.1 192.168.4.0/24
```

You can also allow an IP range, for example the class C subnet of 192.168.4.0 is defined as:

```
only_from       = 127.0.0.1 192.168.4.0/24
```

You can remove or comment out the `only_from` line if you wish to allow traffic from all remote machines and applications.

When you have finished, save the changes in vi by typing:

```
:wq
```

and press **Enter**.

Restart xinetd

After updating `/etc/xinetd.d/nsca` you must restart the xinetd service with the following command:

RHEL | CentOS | Oracle Linux | Debian | Ubuntu

```
systemctl restart xinetd
```

Open Firewall Ports

The local firewall for the operating system requires TCP port 5667 to be opened to allow inbound traffic. Execute the following commands in your terminal session to open the ports permanently:

RHEL | CentOS | Oracle Linux

```
firewall-cmd --zone=public --add-port=5667/tcp
firewall-cmd --zone=public --add-port=5667/tcp --permanent
```

NAGIOS®

Ubuntu

Ubuntu does not have the firewall enabled by default, however, here are the commands if it is enabled:

```
ufw allow proto tcp from any to any port 11211
ufw reload
```

Debian

Debian does not have the firewall enabled by default, however, here are the commands if it is enabled:

```
iptables -I INPUT -p tcp --dport 11211 -j ACCEPT
```

Configure NSCA Settings

You will need to configure a password and decryption method that is used to decrypt data that is sent to NSCA.

You configure these settings by navigating to **Admin > Check Transfers > Inbound Transfers** in the Nagios XI interface.

Click the **NSCA** tab to access the NSCA settings.

- Check the box I have completed these steps to acknowledge that you updated the `/etc/xinetd.d/nsca` file.
- Select your **Decryption Method** and enter a Password
- Click the **Update Settings** button.

Nagios®

Please refer to the screenshot that shows these selections.
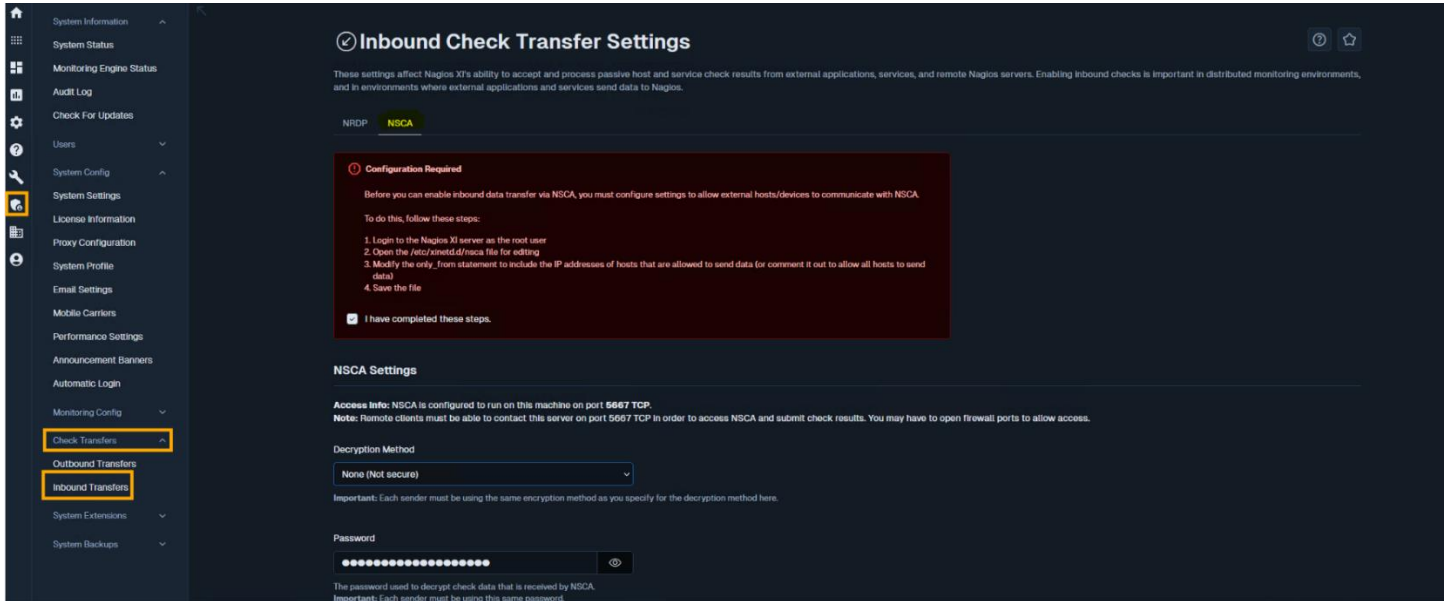
Client Installation

To send a passive check result from a remote server, an NSCA client must be used on the remote server. There are several Nagios addons that are distributed with an NSCA client implementation. You can find several of these addons on the Nagios Exchange website using the link.

If you need a command-line client for Linux/Unix systems, you can download and install the NSCA addon on the remote machine. The NSCA addon can be downloaded from here.

Instructions for installing the NSCA client can be found in the community contributed documentation located here.

The Windows agent NSClient++ can be configured to send check results to NSCA, please refer to the following documentation:

Using NSClient++ For Passive Checks

NRDP - An Alternative Solution

Nagios Remote Data Processor (NRDP) is the recommended solution for integrating passive check results with Nagios XI. Please refer to the NRDP Overview documentation for detailed information.

Finishing Up

This completes the documentation on how to use the Nagios XI NSCA addon in 2024. 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

Nagios®