Nagios XI – How to Use the NSCA Addon

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to enable and use the Nagios Service Check Adapter (NSCA) addon with Nagios XI. NSCA allows remote Nagios servers and applications to send passive host and service check results to a Nagios XI server for processing.

Target Audience

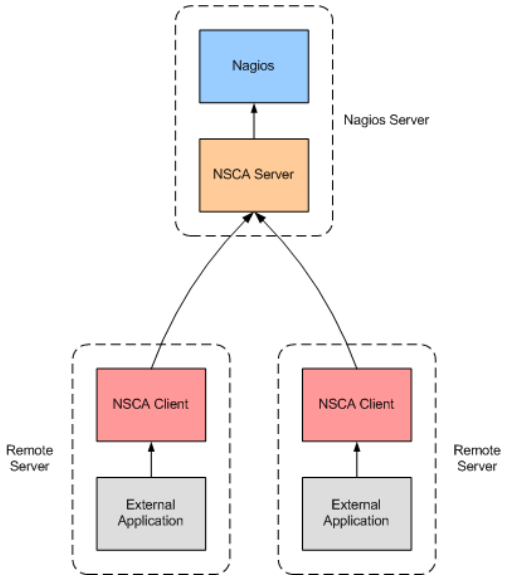
This document is intended for use by Nagios XI Administrators who wish to process passive service checks.

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 once you install Nagios XI manually or use a pre-installed Nagios XI virtual machine.

In order 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 allows connections from the Nagios XI server itself. In order to allow remote hosts and applications to send passive results to Nagios XI you will need to configure access. To do this, open the 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.*

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
```

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 5.x/6.x:

```
service xinetd restart
```

RHEL/CentOS 7.x:

```
systemctl restart xinetd
```

Open Firewall Ports

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

RHEL/CentOS 5.x/6.x:

IPv4

```
iptables -I INPUT -p tcp --destination-port 5667 -j ACCEPT
service iptables save
```

IPv6

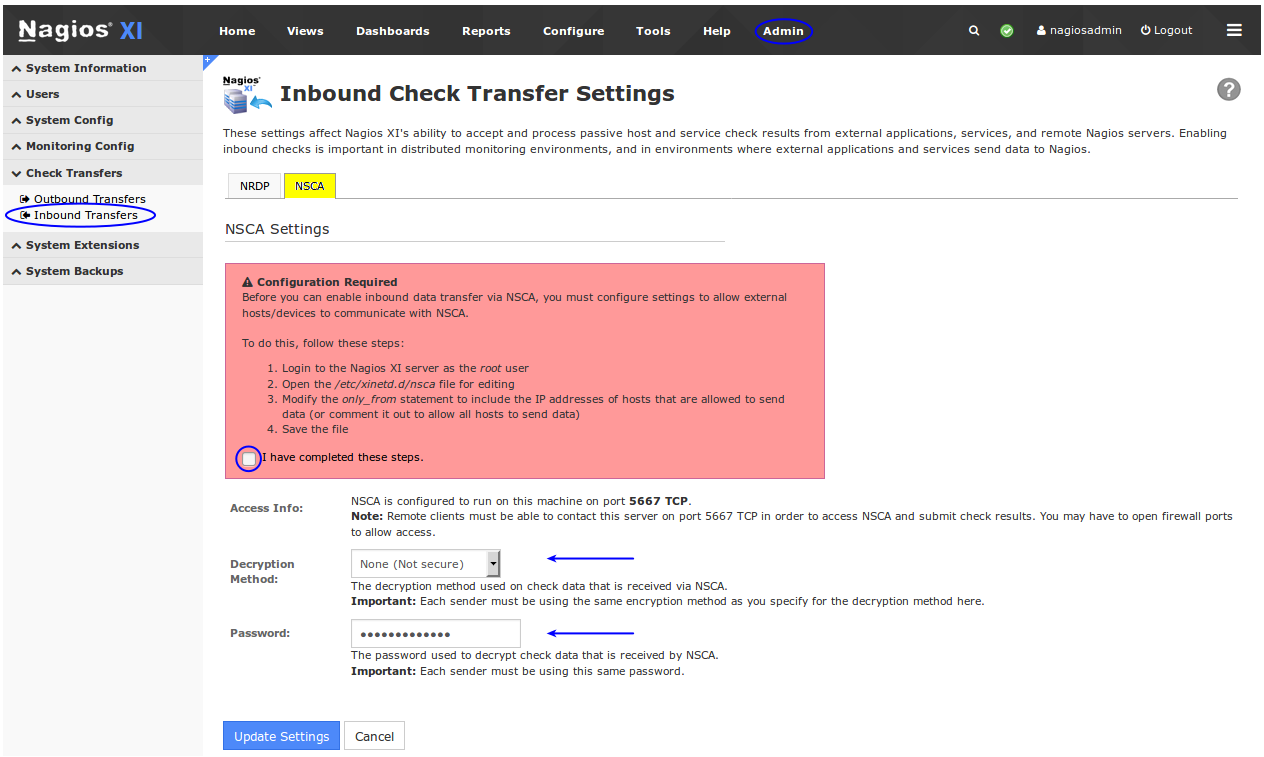
```
ip6tables -I INPUT -p tcp --destination-port 5667 -j ACCEPT
service ip6tables save
```

RHEL/CentOS 7.x:

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

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 **Decription Method** and enter a **Password**.

Finally click the **Update Settings** button.

Client Installation

In order 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. The link below will display Nagios addons that support NSCA:

https://exchange.nagios.org/index.php?option=com_mtree&task=search&Itemid=74&searchword=nsca

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:

http://www.nagios.org/download/addons

Instructions for installing the NSCA client can be found in the community contributed documentation located at:

http://nagios.sourceforge.net/download/contrib/documentation/misc/NSCA_Setup.pdf

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

https://assets.nagios.com/downloads/nagiosxi/docs/Using_NSClient_For_Passive_Checks.pdf

Finishing Up

After following this documentation your Nagios XI server is ready to receive inbound NSCA data. For any support related questions please visit the Nagios Support Forums at:

https://support.nagios.com/forum/