

The Industry Standard in IT Infrastructure Monitoring

Purpose

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

Target Audience

This document is intended for use by Nagios XI Administrators.

NSCA Overview

The NSCA addon consists of two parts:

- A server application that runs on your Nagios 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 server

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

Configuration

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:

1. Enable remote access to NSCA

By default, NSCA can only be accessed from the Nagios XI server. In order to allow remote hosts and applications to send passive results to Nagios XI you will need to configure access. To do this, editing the following file:

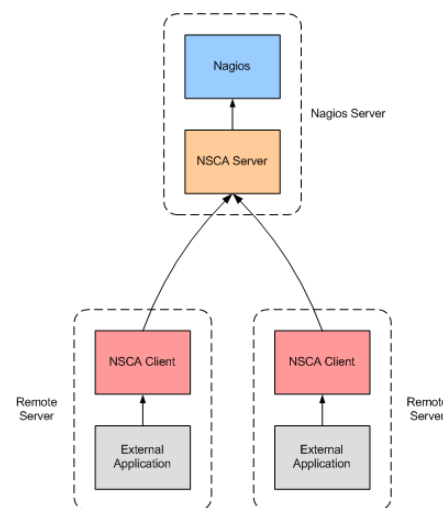
```
/etc/xinetd.d/nsca
```

Edit the *only_from* variable to include the specific IP addresses you want to allow traffic from. You can remove or comment out the *only_from* line if you wish to allow traffic from all remote machines and applications.

2. Restart xinetd

Once you save the file you must restart the xinetd service with the following command:

```
/etc/init.d/xinetd restart
```



3. 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 can configure these settings under the **Inbound Transfers** menu of the **Admin** section in the Nagios XI interface.

The screenshot shows the Nagios XI web interface. The top navigation bar includes Home, Views, Dashboards, Reports, Configure, Help, and Admin. The user is logged in as 'nagiosadmin'. The main content area is titled 'Inbound Check Transfer Settings'. It features a sidebar with a tree view of configuration options, including 'Quick Tools', 'System Status', 'Users', 'System Config', 'Monitoring Config', 'Check Transfers', and 'System Extensions'. The 'Check Transfers' section is expanded to show 'Outbound Transfers' and 'Inbound Transfers'. The 'Inbound Transfers' settings are displayed, including a radio button for 'NSCA', a text field for 'Access Info' (set to 'NSCA is configured to run on this machine on port 5667 TCP'), a dropdown for 'Decryption Method' (set to 'None (Not secure)'), and a password field. There are 'Update Settings' and 'Cancel' buttons at the bottom.

Client Installation

In order to send a passive check result from a remote server, an NSCA client must be used on that 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:

http://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