

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to configure inbound checks in Nagios XI. Inbound checks are used in federated and distributed monitoring environments, as well as environments where the monitoring server receives passive check results from external applications and services.

Target Audience

This document is intended for use by Nagios administrators.

Other Documentation

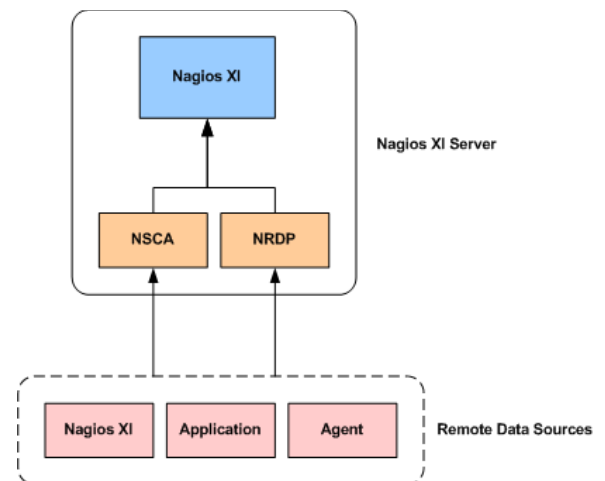
The reader should be familiar with the following documentation in order to configure and use inbound checks, including:

- **Monitoring Unconfigured Objects With Nagios XI**
 - https://assets.nagios.com/downloads/nagiosxi/docs/Monitoring_Unconfigured_Objects_With_XI.pdf
- **Configuring Outbound Checks With Nagios XI**
 - https://assets.nagios.com/downloads/nagiosxi/docs/Configuring_Outbound_Checks_With_XI.pdf

Inbound Transfer APIs

There are two different APIs for handling inbound check transfers (passive checks) in Nagios XI:

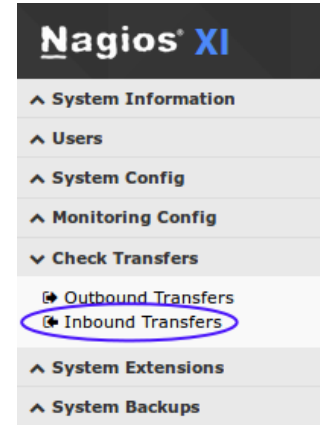
- **NRDP**
 - NRDP is a newer web-based API that operates over port 80 (HTTP)
- **NSCA**
 - NSCA operates over TCP port 5667, and while it is older than NRDP, it is supported by many more Nagios addons than the newer NRDP API



Accessing Transfer Settings

You can configure inbound check transfers by selecting the **Inbound Transfers** option in the Administrative interface of Nagios XI.

The inbound check transfer settings page allows you to configure both the NSCA and NRDP APIs.



NRDP Configuration

External applications, services, and remote servers must use an authentication token when sending check results to the NRDP API.

You can configure multiple authentication tokens to support different clients if you wish. The first time you configure NRDP, a random token will be generated for you. You can change the token to an alpha-numeric string of your choosing.

Click the **Update Settings** button to save the NRDP settings.

A screenshot of the Nagios XI 'Inbound Check Transfer Settings' page. At the top, there are tabs for 'NRDP' (selected) and 'NSCA'. Below the tabs, the page is titled 'NRDP Settings'. Under 'Access Info', it states the NRDP API can be accessed at <http://192.168.4.18/nrdp/> and includes a note about port 80 (HTTP) or 443 (HTTPS). Under 'Authentication Tokens', it explains that tokens are used for remote hosts and applications, and a text area contains the token 'gmr57j8796m0'. At the bottom, there are 'Update Settings' and 'Cancel' buttons.

NSCA Configuration

Before you can enable inbound check transfers via the NSCA API, you must configure your Nagios XI server as follows:

- Login to the Nagios XI server as the **root** user
- Open the `/etc/xinetd.d/nsca` file for editing
- Modify the **only_from** statement to include the IP addresses of hosts that are allowed to send data (or comment it out to allow all hosts to send data)
- Save the file
- Restart the `xinetd` service using the following command:
 - `service xinetd restart`

External applications, services, and servers that send passive checks results to Nagios XI using the NSCA API *should* encrypt the transmitted data.

The Nagios XI server and each client must be using the same:

- **Decryption / encryption method**
- **Password**

Click the **Update Settings** button to save your settings.

Inbound Check Transfer Settings

These settings affect Nagios XI's ability to accept and process passive host and service check results from external applications, services, and remote Nagios servers. Enabling inbound checks is important in distributed monitoring environments, and in environments where external applications and services send data to Nagios.

NRDP NSCA

NSCA Settings

▲ Configuration Required
Before you can enable inbound data transfer via NSCA, you must configure settings to allow external hosts/devices to communicate with NSCA.

To do this, follow these steps:

1. Login to the Nagios XI server as the `root` user
2. Open the `/etc/xinetd.d/nsca` file for editing
3. Modify the `only_from` statement to include the IP addresses of hosts that are allowed to send data (or comment it out to allow all hosts to send data)
4. Save the file

I have completed these steps.

Access Info: NSCA is configured to run on this machine on port **5667 TCP**.
Note: Remote clients must be able to contact this server on port 5667 TCP in order to access NSCA and submit check results. You may have to open firewall ports to allow access.

Decryption Method:
The decryption method used on check data that is received via NSCA.
Important: Each sender must be using the same encryption method as you specify for the decryption method here.

Password:
The password used to decrypt check data that is received by NSCA.
Important: Each sender must be using this same password.

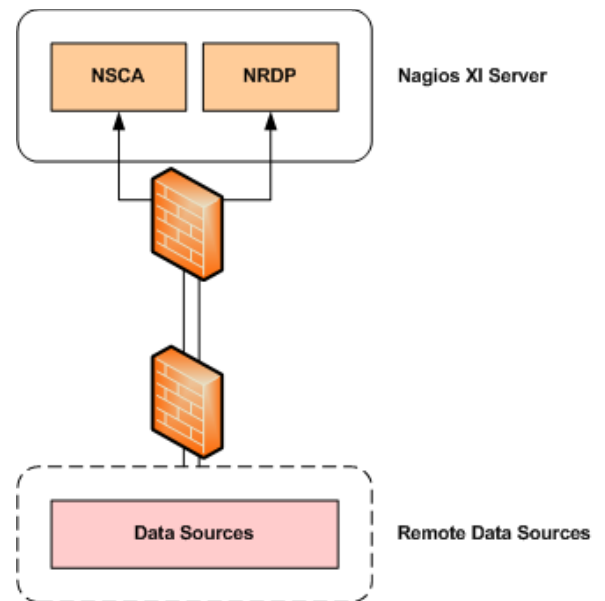
Firewall Configuration

Modification of firewall settings between the remote data sources and the Nagios XI server may be required in order to allow inbound check results to be sent to Nagios XI.

The NRDP API works on **TCP port 80** using the HTTP protocol.

NSCA uses a custom protocol that runs on **TCP port 5667**.

Firewalls must be configured to allow inbound and outbound traffic over the ports used by the API(s) you choose to utilize for handling inbound checks.



Configuring Objects

Nagios XI must be configured to monitor hosts and services that it received passive check results for. If it is not configured with a host or service when a passive check arrives, Nagios XI will add that host or services to a list of Unconfigured objects (Admin > Monitoring Config > Unconfigured Objects).

The Nagios administrator can then easily configure the host and service in the monitoring engine. Information on monitoring Unconfigured objects can be found in the following documentation:

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

Finishing Up

If you still have questions about configuring inbound checks, or for any other support related questions, please visit the [Nagios Support Forums](#) at:

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