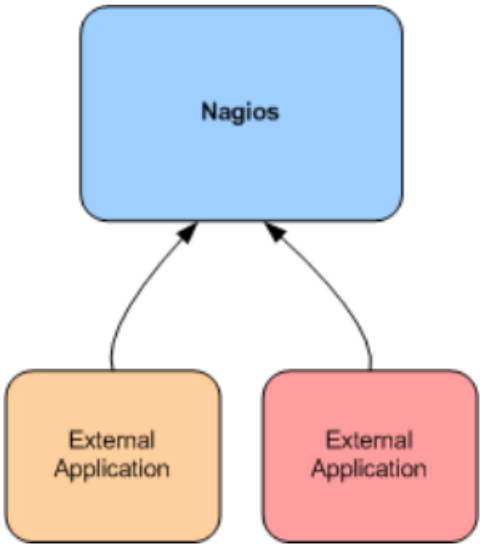
How To Configure Passive Services With Nagios XI

Purpose

This document describes how to How To Configure Passive Services With Nagios XI.

Passive Check Overview



Nagios does not actively check the status of a service that is configured only for passive checks. Instead, Nagios waits for external devices / applications to submit a check result for a particular service.

Passive checks are commonly used for **integrating** security alerts and event log data into Nagios and are also used in distributed monitoring environments.

A comparison between an active check and a passive check might also help:

UPS device loses input power and is running on batteries.

- With an **active** check, if Nagios XI was checking the device on a 5 minute interval then it might be up to 5 minutes before Nagios XI is aware that the device is on batteries.
- With a **passive** check, the device immediately sends an SNMP Trap to Nagios XI when it is running on batteries.

This example scenario used an SNMP Trap as the method for receiving a passive check. This document does not focus on SNMP Traps however it is a good example to demonstrate the differences between active and passive checks.

Sending Passive Checks To Nagios

To send passive service checks from external applications and servers to Nagios, you'll need to use the NSCA or NRDP addon to facilitate the transfer of data to the Nagios XI server. Instructions on using NSCA with Nagios XI can be found at:

- Using NSCA With XI
- NRDP Overview
- Using NCPA for Passive Checks

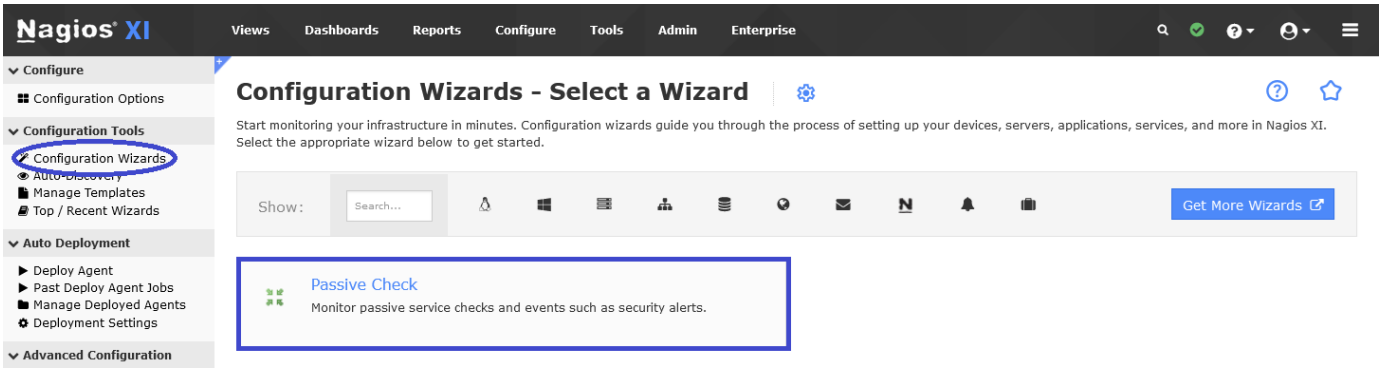
Configuring Passive Services Within Nagios XI

Each host or device that you wish to receive and process passive checks from must have a corresponding passive check service defined in Nagios XI. Nagios XI has the **Passive Check** wizard that makes the configuration of these passive checks quick and simple.

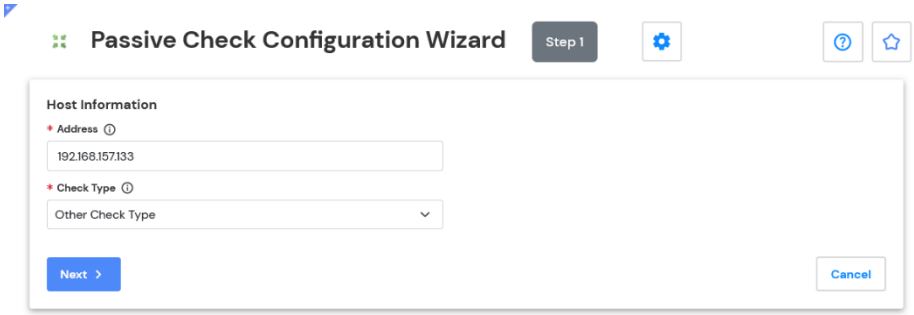
The Passive Check wizard should already be installed on your system. If you need to install the Passive Check wizard it can be download from: http://assets.nagios.com/downloads/nagiosxi/wizards/passivecheck.zip

To install the wizard in Nagios XI, navigate to **Admin > System Extentions > Manage Config Wizards**. Use the **Browse** button and the **Upload Wizard** button to upload the passivecheck.zip wizard

To begin using the Passive Check wizard navigate via the top menu bar to **Configure > Run a configuring wizard** and select the **Passive Check Wizard**. In the following screenshot you can see how the search field allows you to quickly find a wizard.

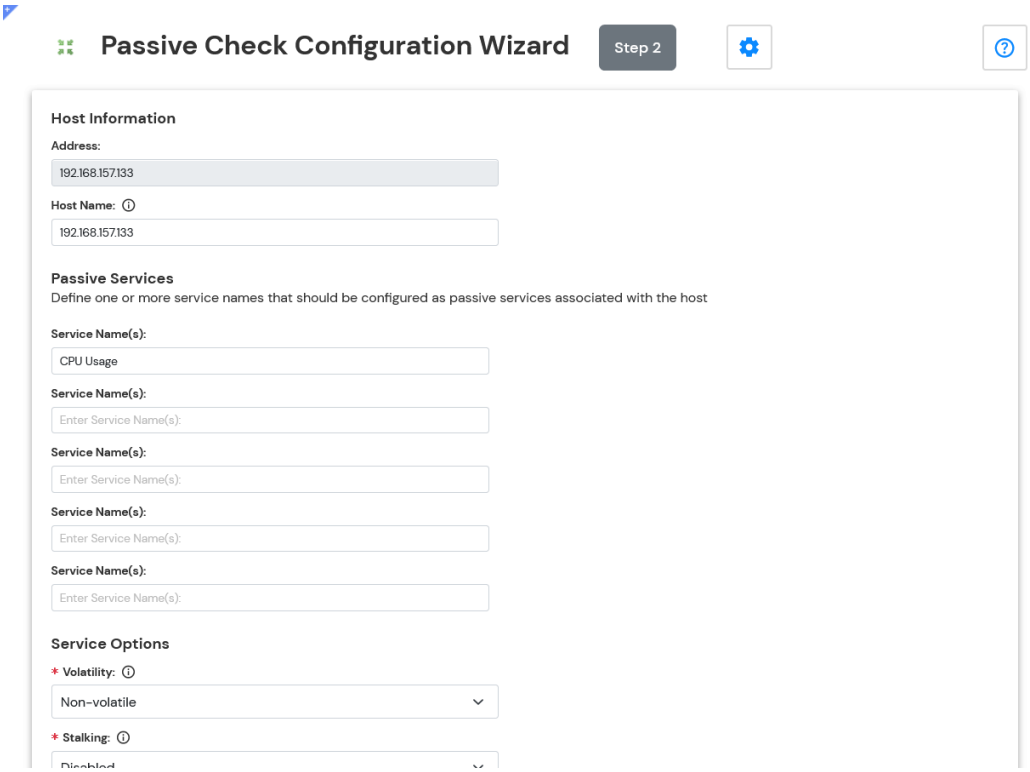


When you run the passive check wizard, it will first ask you for the **Address** of the host that is associated with the passive checks.



You can also specify the **Check Type** for the passive check by selecting **Security-Related Check**, or **Other Check Type** from the drop-down.

The next screen of the wizard allows you to define one or more **Service Names** that should be defined as passive checks. The following screenshot shows several services have been added.

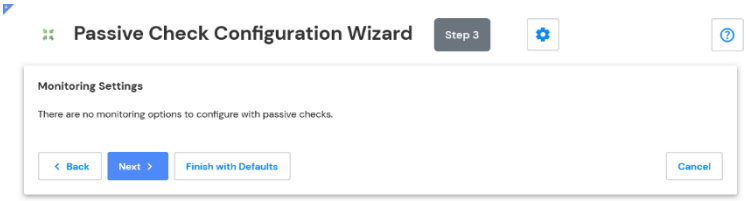


You can specify **Volatility** and **Stalking** options for the services to match your monitoring requirements. Both options are useful when monitoring security-related events.

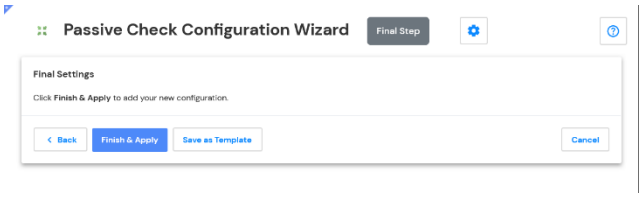
Volatile events generate alerts each time anything other than an OK state event is received. (i.e. Critical, Warning, Unknown)

Stalking services will have their own output data (textual alert information) logged by Nagios each time newly received output differs from the most recent previously received output

Step 3 of the wizard has no options as there are no monitoring settings for passive checks.



Steps 4 and 5 have the standard options available in configuration wizards, please populate the settings as required



Once you've reached the Final Step click **Apply** to add the new passive objects.

When the configuration is successfully applied, click the **View status details for xxx** link which should direct you to a screen like the following.

Showing 1-4 of 4 total records

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.157.133	CPU Usage	Pending	N/A	1/1	N/A	No check results for service yet...
	HTTP	Ok	1h 11m 57s	1/5	2024-11-28 20:11:18	HTTP OK: HTTP/1.1 302 Found - 237 bytes in 0.007 second response time
	Ping	Ok	1h 12m 43s	1/5	2024-11-28 20:10:33	OK - 192.168.157.133: rta 1.154ms lost 0%
	SSH	Ok	1h 11m 51s	1/5	2024-11-28 20:11:25	SSH OK - OpenSSH_8.7 (protocol 2.0)

Last Updated: 2024-11-28 20:13:16

If the server is successfully receiving passive check results you should start to see these services receive data:

Showing 1-4 of 4 total records

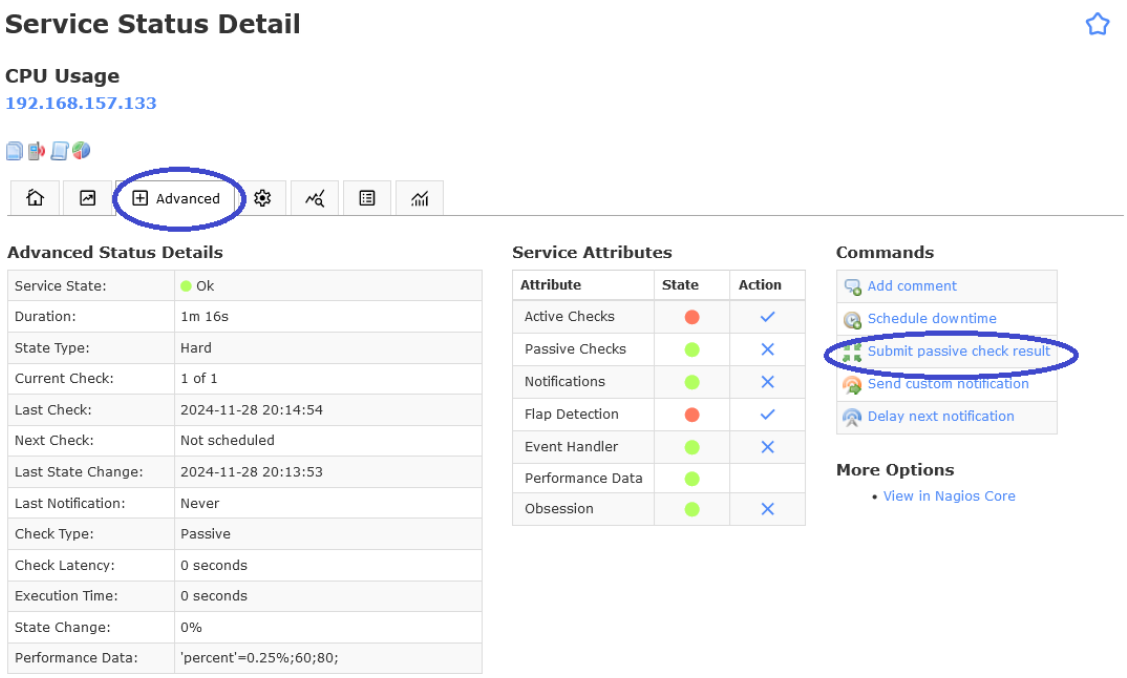
Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.157.133	CPU Usage	Ok	8s	1/1	2024-11-28 20:13:50	OK: Percent was 7.82 %
	HTTP	Ok	1h 12m 42s	1/5	2024-11-28 20:11:18	HTTP OK: HTTP/1.1 302 Found - 237 bytes in 0.007 second response time
	Ping	Ok	1h 13m 28s	1/5	2024-11-28 20:10:33	OK - 192.168.157.133: rta 1.154ms lost 0%
	SSH	Ok	1h 12m 36s	1/5	2024-11-28 20:11:25	SSH OK - OpenSSH_8.7 (protocol 2.0)

Last Updated: 2024-11-28 20:14:01

Manually Submitting A Passive Check Result

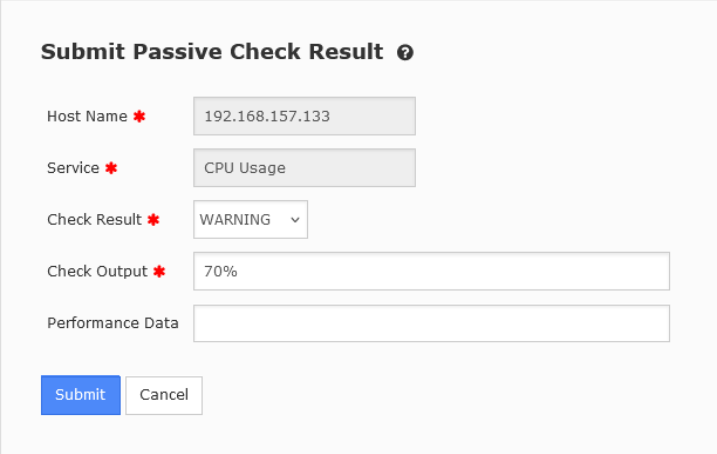
Sometimes you will want to manually submit a passive check result for a service. This capability is particularly useful for resetting services to an OK state once the issue has been handled.

You can do this by navigating to **Home > Details > Service Detail** and clicking your passive check to bring up the **Service Status Detail** screen. Select the **Advanced** tab and click on **Submit passive check result**. The following example is from the Windows Update Status service shown above that is in a critical state.

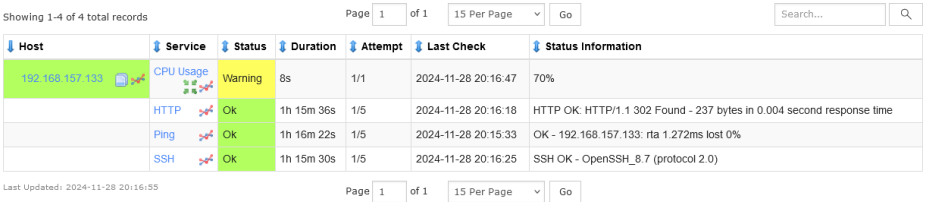


You can specify the **Check Result** (service state) from the drop down, enter **Check Output** (textual data) for the passive check and any **Performance Data** collected by the check.

Click the **Commit** button to submit the passive check to Nagios.



Once the passive check is processed, the status of the passive check will be updated. This will remain until the next passive check result is received.



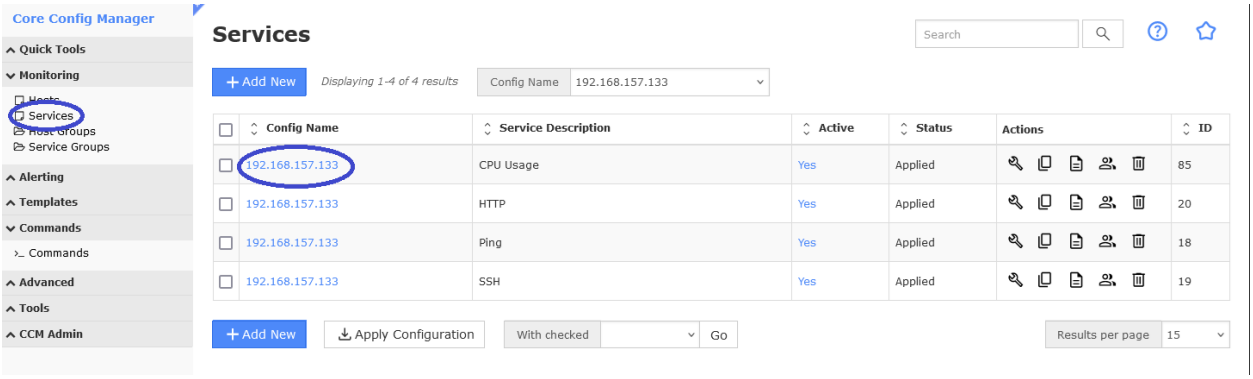
Extending Passive Checks With Freshness Checks

As explained earlier, it's the responsibility of the external devices / applications to send the check results through, all Nagios XI does is wait for the passive check results. If Nagios XI stops receiving passive check results from a device / application then Nagios XI will not know this has happened, it still has services in the state they were in the last time a passive check results is received.

Nagios XI has the ability to keep an eye on passive check results for host and service objects, if Nagios XI hasn't heard from the passively monitored device / application for a specified amount of time then it can take action. The most common action is to submit a check result to Nagios XI with a critical state, this ensures that notifications are triggered, and it appears as critical in the monitoring interface.

This process is called **freshness checking**, and this section will show you how to set up freshness checks for your individual needs. This guide is going to demonstrate how to configure freshness for the **Drive C: Disk Usage** service. We will configure it so that if no passive check result has been received in 15 minutes (900 seconds) then it will put the service into critical state.

Navigate to **Configure > Core Config Manager > Monitoring Services** and click the appropriate service to be edited.

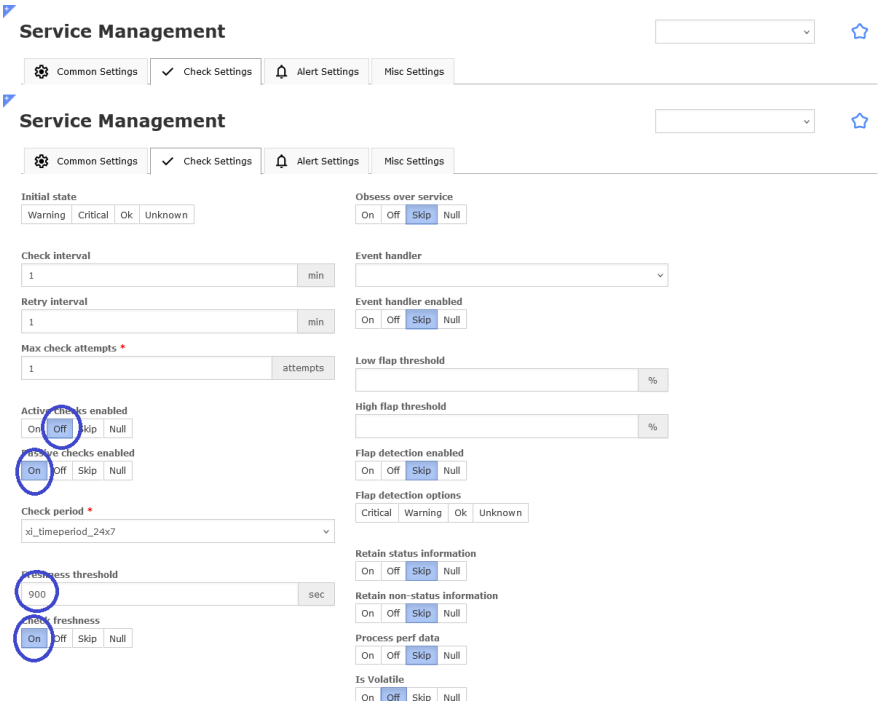


First, we'll start by defining the freshness threshold and other relevant settings, click the **Check Settings** tab. On this screen you'll need to specify a few options:

Active checks enabled

Off

This ensures that the check command on the **Common Settings** tab used to put the service into a critical state will NOT be executed **unless** the freshness threshold is exceeded. The check command will be defined in the next step.



Passive checks enabled

On

This ensures the service is receiving passive check results. *If this is already on Skip then it may already be inheriting the setting from a template.*

Freshness threshold

900

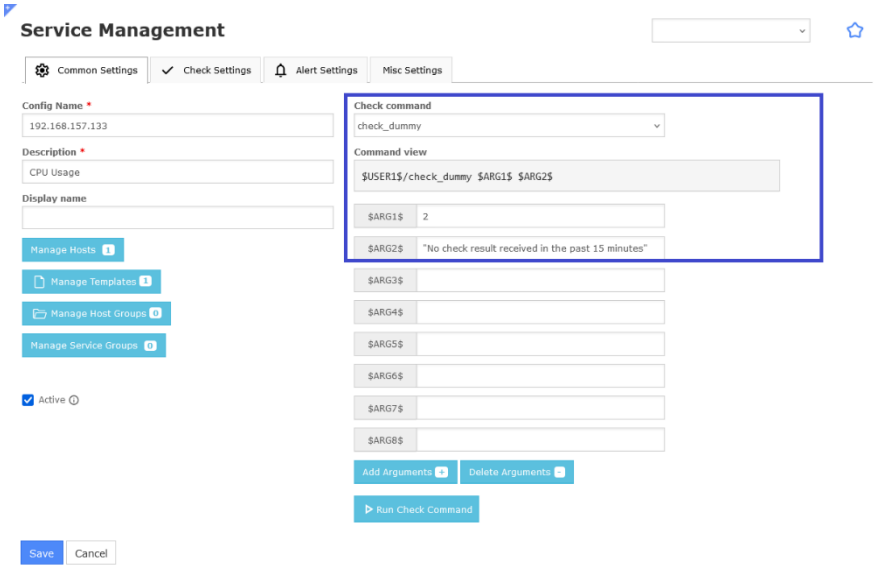
If Nagios XI does not hear from the specified host or service in the specified freshness threshold period, it will execute the check command that will be defined on the **Common Settings** tab.

Check freshness

On

This enables the freshness checks for the host or service object.

Next, we'll define the check command to be executed when the freshness threshold is exceeded, click the **Common Settings** tab.



On this screen you'll need to specify a few options:

Check command

```
check_dummy
```

This is the plugin that is executed when the freshness threshold is exceeded. check_dummy is a simple command that allows you to provide a return code (**$ARG1$** field) and the status text to provide (**$ARG2**$ field).

$ARG1$

```
2
```

The number 2 is how Nagios XI knows a service is in the **critical** state

$ARG2$

```
"No check result received in the past 15 minutes"
```

This is the status that will be shown in Nagios XI.

Once you've made these changes click the **Save** button and then **Apply Configuration**.

The following screenshot shows that the freshness threshold was exceeded for this service.

Service Status for this Host Last updated: 2024-11-28 20:00:19

Service	Status	Duration	Attempt	Last Check	Status Information
HTTP	Ok	59m 0s	1/5	2024-11-28 19:56:18	HTTP OK: HTTP/1.1 302 Found - 237 bytes in 0.003 second response time
Ping	Ok	59m 46s	1/5	2024-11-28 19:55:33	OK - 192.168.157.133: rta 0.889ms lost 0%
SSH	Ok	58m 54s	1/5	2024-11-28 19:56:25	SSH OK - OpenSSH_8.7 (protocol 2.0)
CPU Usage	Critical	4m 47s	1/1	2024-11-28 19:55:32	CRITICAL: No check result received in the past 15 minutes

In this example we used the check_dummy plugin, however you could use any plugin that is available in Nagios XI.

Unconfigured Objects

The following documentation describes how to configure monitoring of previously unconfigured hosts and services that a Nagios XI server has received passive check results for.

Monitoring Unconfigured Objects With XI

Finishing Up

This completes the documentation on How To Configure Passive Services With Nagios XI. 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