# Integrating NNA 2024 with Nagios XI and Core

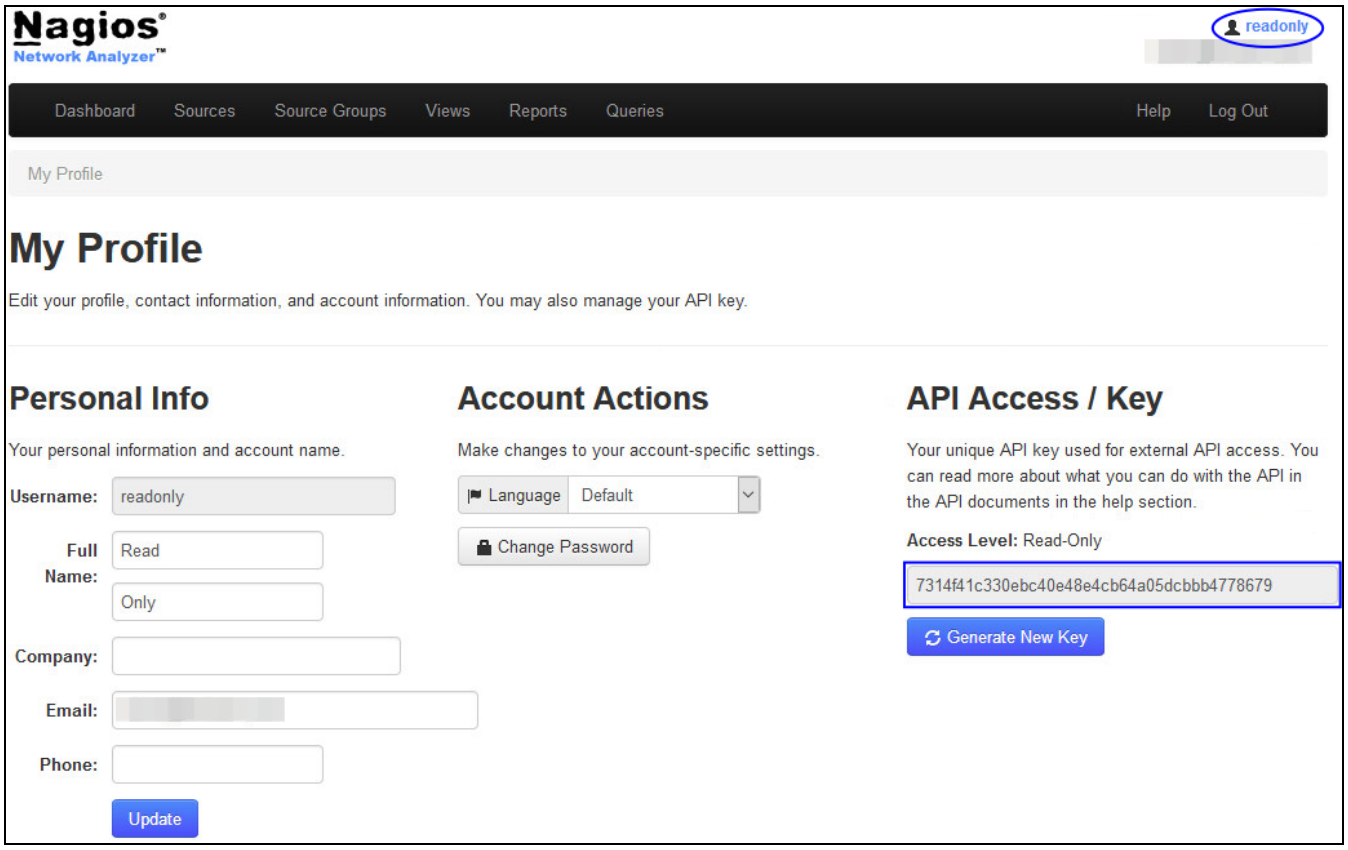
### Overview

Nagios Network Analyzer can be integrated with Nagios XI and Nagios Core, extending the capabilities of Nagios Network Analyzer. The differences between integrating Nagios XI and Nagios Core are as follows:

- Nagios XI
    - Host and Service Status pages provide a Network Traffic Analysis tab
        - Provides a pie chart and table for the past 24 hours
    - Generate Reports from within Nagios XI
    - Dynamically create host and service directives received from Network Analyzer for passive checks
- Nagios Core
    - Configure Network Analyzer to send passive check results to Nagios Core using NRDP

## Nagios XI - Configure Integration

In Nagios XI you configure the Nagios Network Analyzer Integration component with the details of the Nagios Network Analyzer server(s) that you would like integrated with Nagios XI. Integration is achieved by using an Authentication key that belongs to a Nagios Network Analyzer user account that has been granted API access. The first step is to get the API key that is required when configuring the component. Open Nagios Network Analyzer as the user with API access and then click the user's name in the top right corner of the screen.

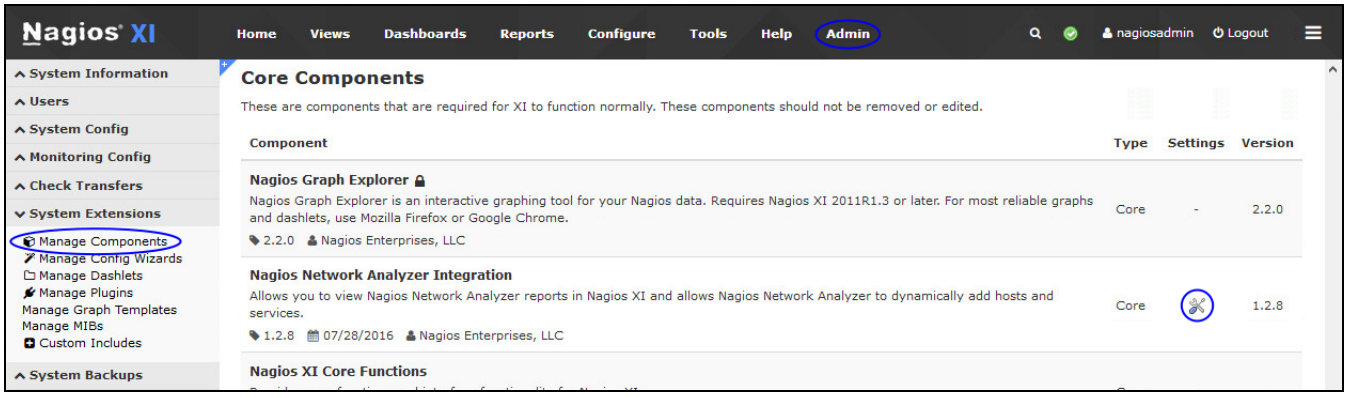



In the screenshot above you can see the API key. Copy this into your clipboard or text file to use in the next step. You can see that a dedicated user account has been created specifically for this purpose. The access level this account has been granted is "User" which means it has read only access. Using a dedicated account is a best practice, you can generate a new key if you suspect the existing key has been compromised.

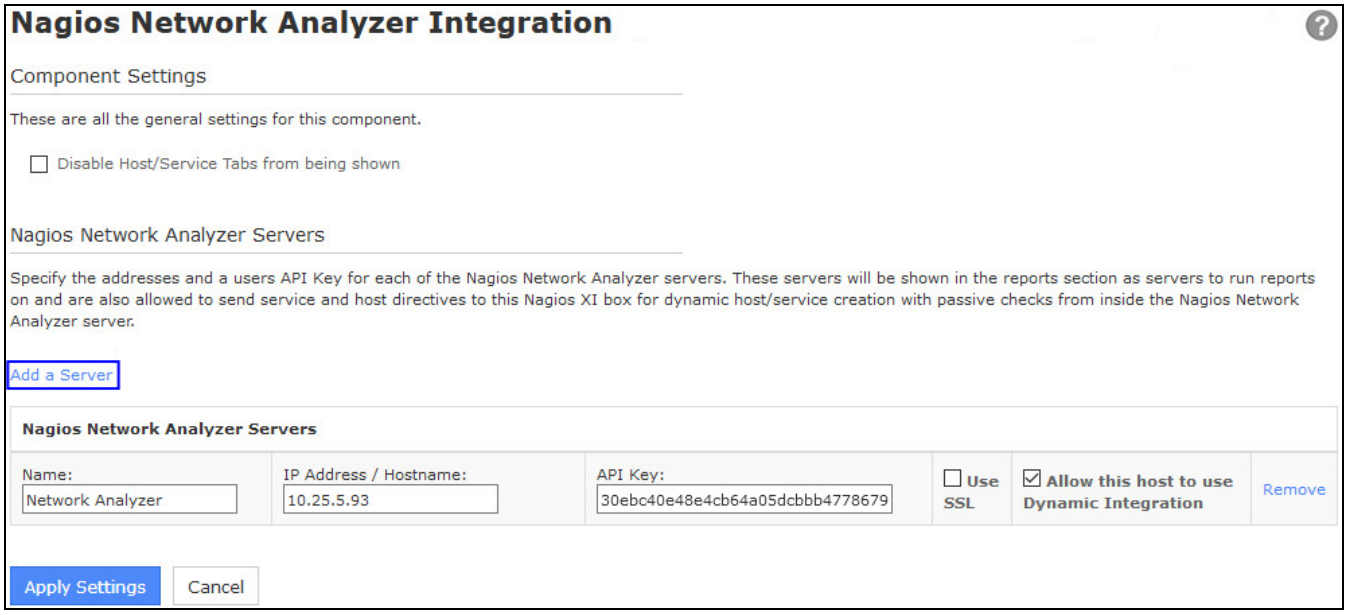
If the user account does not have an API Key on your My Profile page and it says No API Access, you will need to alter this user.

1. Login as an admin user and navigate to Administration > User Management. Edit the user and change API Access to Yes.

2. Now login to Nagios XI and navigate to Admin > System Extensions > Manage Components.




3. Locate the Nagios Network Analyzer Integration component and click the settings icon. The following screenshot shows the component settings window that appears.



4. In the screenshot above click the Add a Server link to display the fields for adding a Nagios Network Analyzer server. You can see that they have been populated, these fields will be explained.

- Name - This is the name that you will see in the Network Analyzer Server drop-downs throughout Nagios XI. For example on the Network Report, Network Query Report and Configuration Wizard.
- IP Address / Hostname - The network address that Nagios XI uses to communicate with Nagios Network Analyzer
- API Key - This is used for authentication with Nagios Network Analyzer as explained earlier
- Use SSL - Required if your Nagios Network Analyzer server is configured with SSL/TLS certificates
- Allow this host to use Dynamic Integration - This allows Nagios XI to create host and service directives received from Network Analyzer for passive checks (NRDP)

5. When you have finished populating the fields click the Apply Settings button. You can add more Network Analyzer servers by clicking on the Add a Server link.

6. You can remove a server that you have previously set up if you wish by clicking on the Remove link.

7. If you do not want the Network Traffic Analysis tabs to be shown under the Hosts and Services details screen in Nagios XI, check the Disable Host/Service Tabs from being shown checkbox.

This completes the initial steps for integrating Nagios Network Analyzer with Nagios XI.

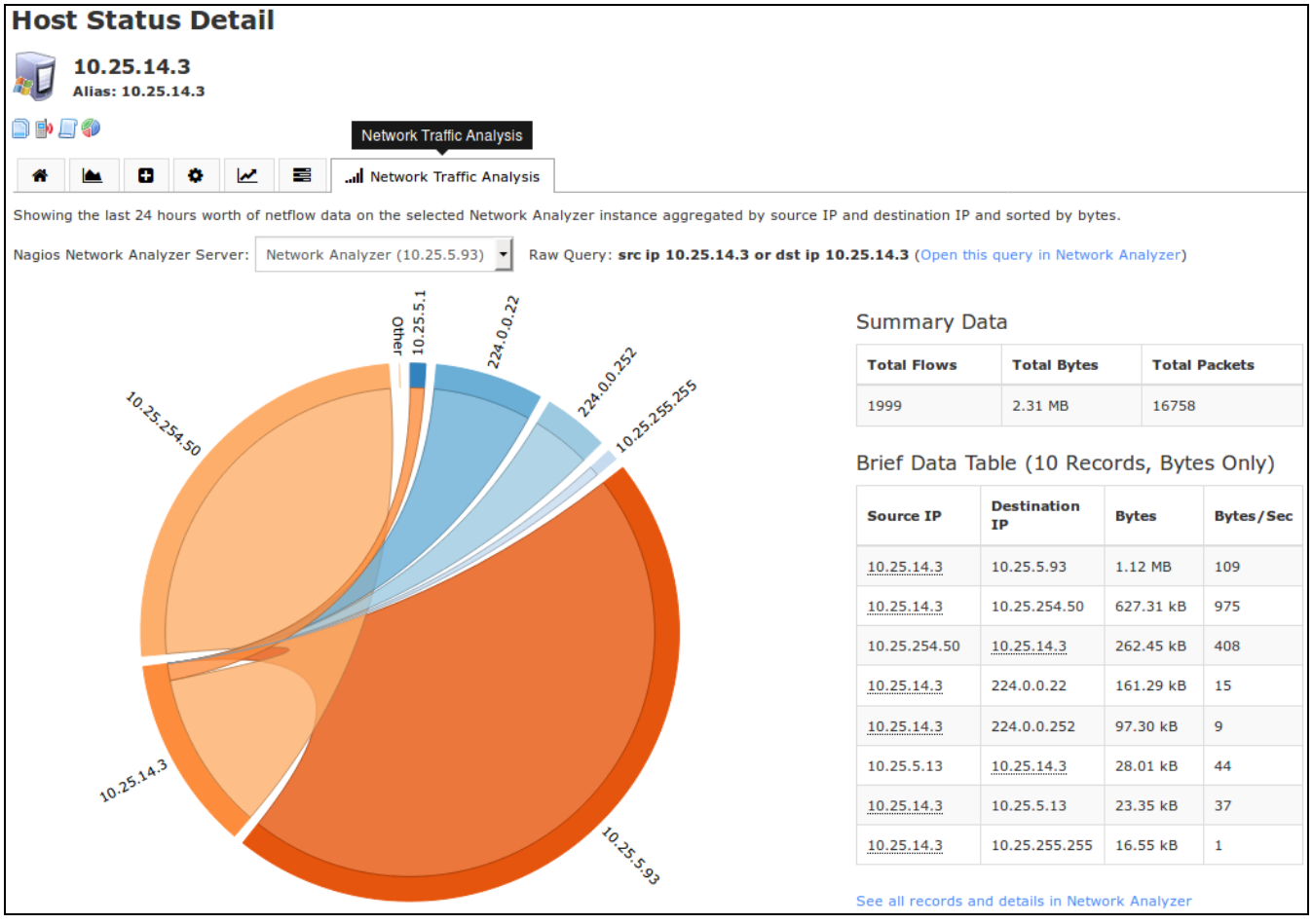
## Nagios XI - Generating Reports

Generating reports from Nagios Network Analyzer in Nagios XI is explained in detail in the following documentation:

Integrating Nagios Network Analyzer Reports With Nagios XI

**Nagios XI - Network Traffic Analysis tab**

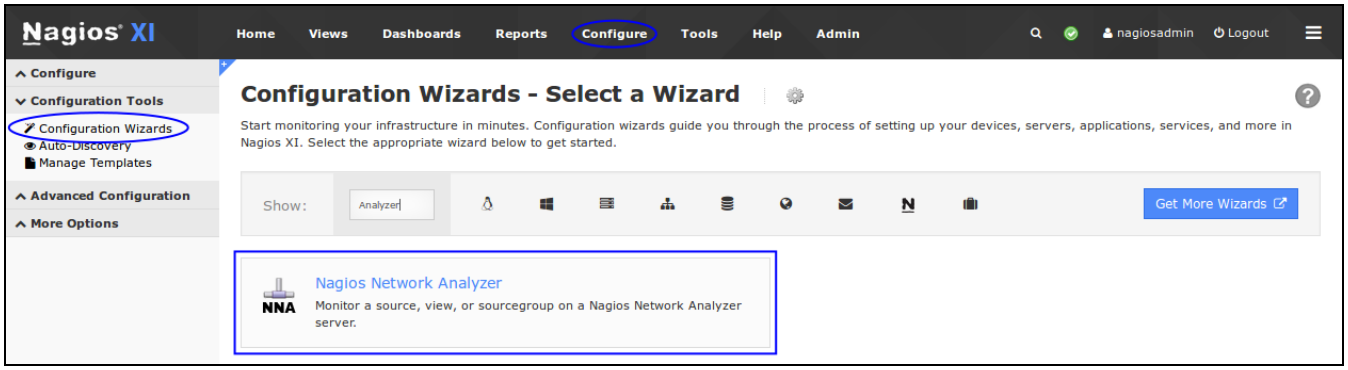
Nagios XI adds a Network Traffic Analysis tab to the host and service status pages. Here is an example from an host object being monitored by Nagios XI:



The host being monitored has the address 10.25.14.3 and this address was found when a raw query was performed against Nagios Network Analyzer. The pie chart shows the relationship between this address and the other address (be it source or destination). Hovering the mouse on the addresses in the chart will put the focus on this relationship and also highlight the data in the Brief Data Table.

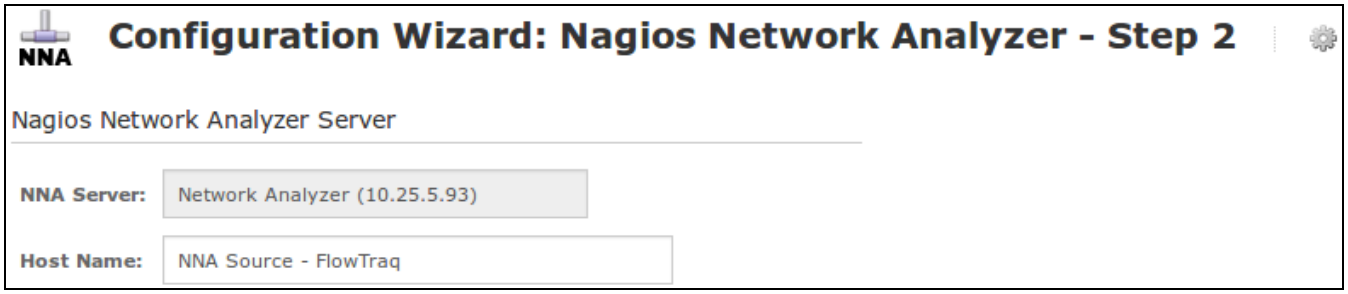
# Nagios XI - Configuration Wizard

To begin using the Nagios Network Analyzer wizard navigate via the top menu bar to Configure > Run a configuring wizard, and select the Nagios Network Analyzer wizard. In the following screenshot you can see how the search field allows you to quickly find a wizard.




On Step 1 you need to select the NNA Server and Source or Sourcegroup that the wizard will use in Step 2.

Click Next to progress to step 2.




On step 2 you will configure all of the options for monitoring.

To start off with make sure a valid Host Name has been entered. By default the format is:

NNA Source/Sourcegroup - <Selected Source/Sourcegroup Name>.

## Select What to Monitor

Select if you'd like to monitor including bytes, flows, packets and behavior on sources.
The graph on the right is provided to help with estimating the warning and critical thresholds.

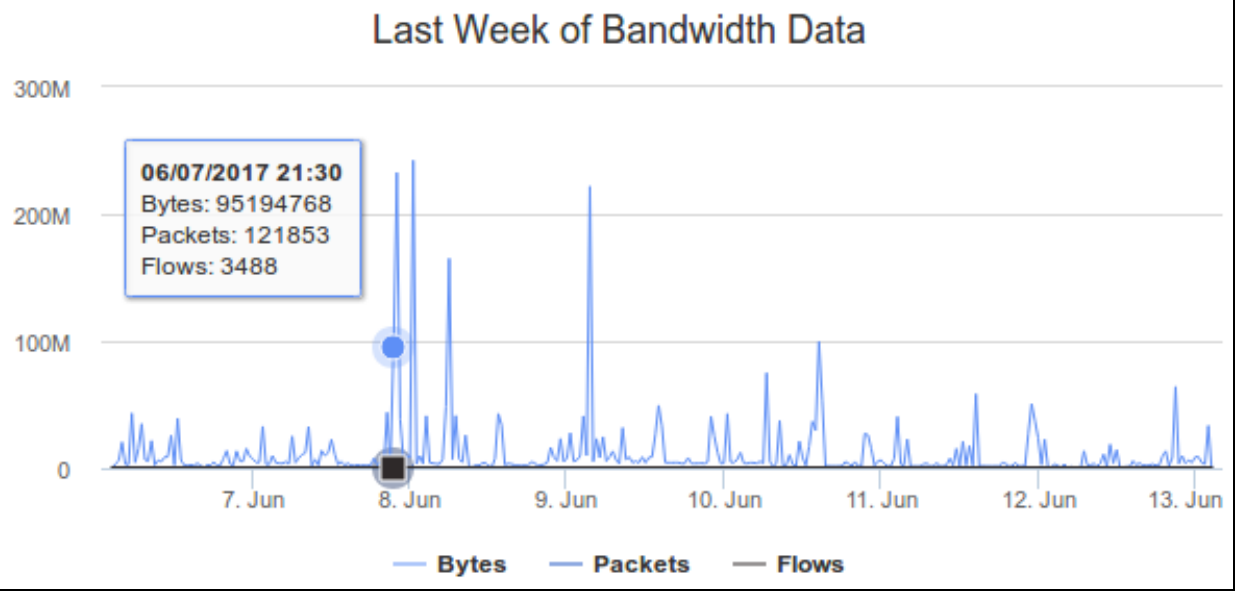
Default values are created by the following:
Warning Threshold: **20% above max value**,
Critical Threshold: **40% above max value**

☑ **Bytes**
Amount of bytes being transferred.
290617872 bytes 339054184 bytes

☑ **Flows**
Amount of flows being transferred.
5372 flows 6267 flows

☑ **Packets**
Amount of packets being transferred.
201317[illegible] packets 234870[illegible] packets

☑ **Abnormal Behavior**
If there is abnormal behavior on the source this check will return critical.



Next you can select what to monitor. Bytes, Flows and Packets all require warning and critical thresholds. Based off the existing data queried from the source, suggested threshold values will be populated. The graph underneath shows the last week of data, here you can hover the mouse to get an understanding of historic values which can help you determine thresholds.

Abnormal Behavior is a check that will report if there is a pattern of behavior that is not normal (relative to the existing history).

Use the check boxes to deselect any checks that you do not think are necessary.

Click Next and then complete the wizard by choosing the required options in Step 3 – Step 5.

To finish up, click on Finish in the final step of the wizard.

This will create the new hosts and services and begin monitoring. Once the wizard applies the configuration, click the View status details for xxxxx link to see the new host and services that were created.

| Host | Service | Status | Duration | Attempt | Last Check | Status Information |
|---|---|---|---|---|---|---|
| NNA Source - FlowTraq | Abnormal Behavior | Ok | 20m 5s | 1/5 | 2017-05-15 17:26:55 | OK - No abnormal behavior detected |
| | Bytes | Ok | 16m 25s | 1/5 | 2017-05-15 17:25:32 | OK - 135473 bytes sent/recieved |
| | Flows | Ok | 16m 42s | 1/5 | 2017-05-15 17:25:15 | OK - 187 flows sent/recieved |
| | Packets | Warning | 6m 5s | 5/5 | 2017-05-15 17:24:37 | WARNING - 1457 packets sent/recieved |

## Nagios XI and Nagios Core - NRDP Passive Checks

The following section applies to both Nagios XI and Nagios Core. To be able to send alerts using NRDP you will need to do the following:

- Nagios XI
    - Configure the Inbound Transfers on your Nagios XI server

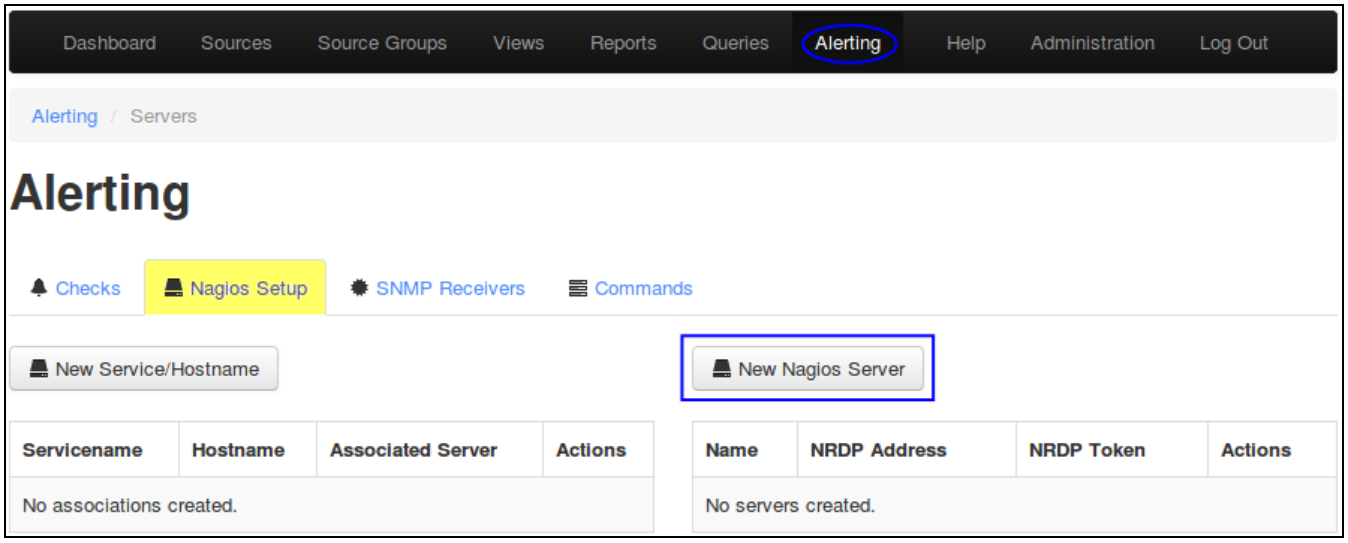
- Nagios Core
    - Install and configure NRDP

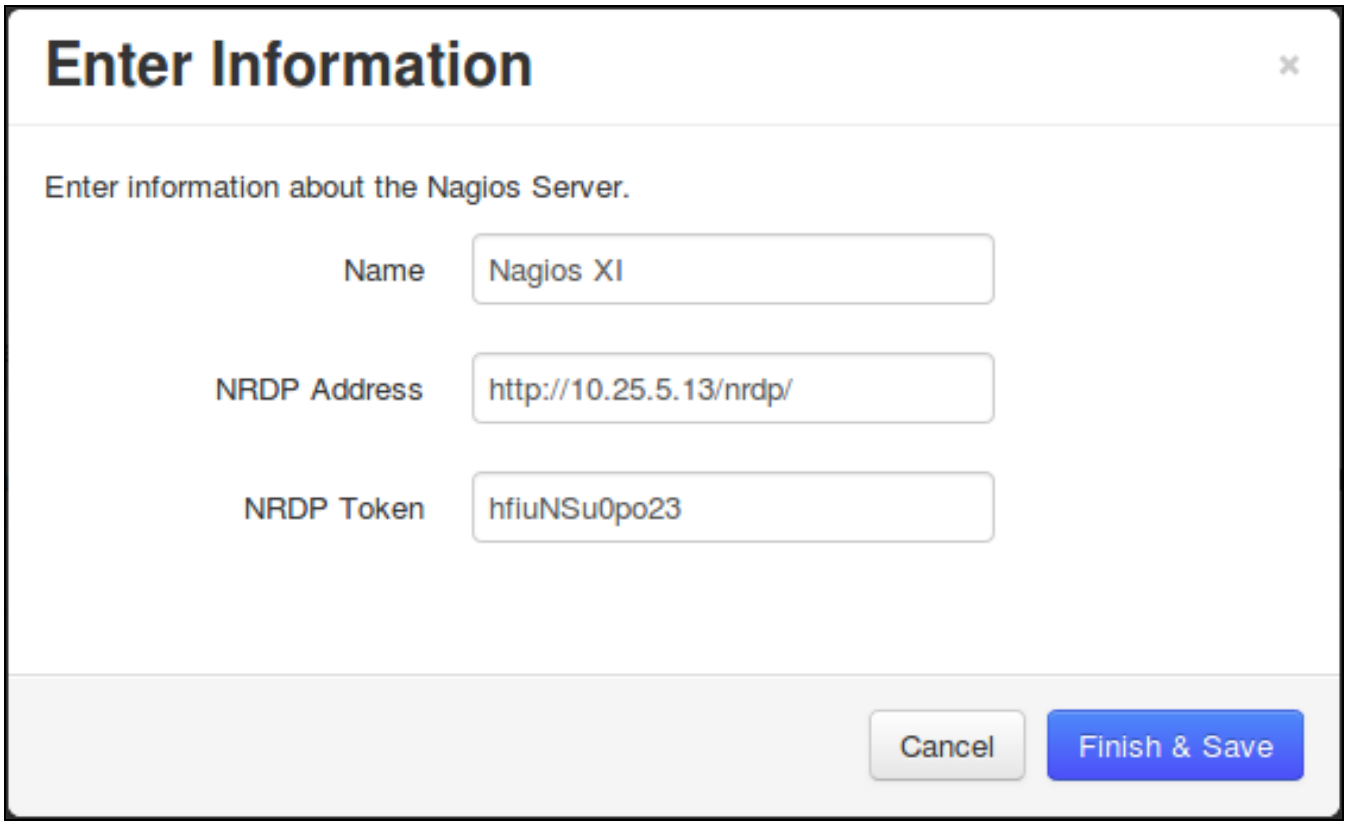
Please refer to the following documentation for Nagios XI or Nagios Core on how to perform these tasks:

NRDP Overview

Please take note of the NRDP Token you define in that documentation, you will need it in the following step.

In Nagios Network Analyzer navigate to Alerting and then click the Nagios Setup tab. Click the New Nagios Server button.






Here you need to provide the details of your Nagios XI or Nagios Core server.

**Name** - The human-readable name used to refer to this Nagios server in alerts.

**NRDP Address** - The address that NRDP results will be sent to. Be sure to include the http:// or https:// part as well.

**NRDP Token** - The token that Network Analyzer will attempt to use to connect to the NRDP server.

Network Analyzer validates your NRDP server settings by attempting to connect with the NRDP server right away, and if it cannot connect to the server or the token provided is invalid, it will warn you. Once added the screen will update reflecting this.

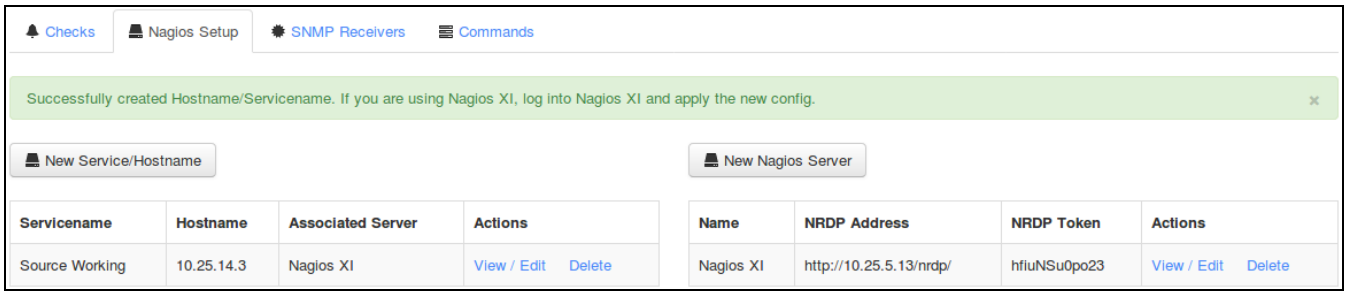

Now that the Nagios Server has been defined you now need to define a Service/Hostname that the NRDP passive checks will be sent to on your Nagios Server. Click the New Service/Hostname button.


**Servicename** - The name of the service that the alert will be sent to in Nagios XI or Core.

**Hostname** - The name of the host object that you want the service to be assigned to in Nagios XI or Core.

**Server** - The Nagios XI or Core service you want the alert to be sent to.

Click the Finish & Save button to create the Service/Hostname object. The screen will update like the following:



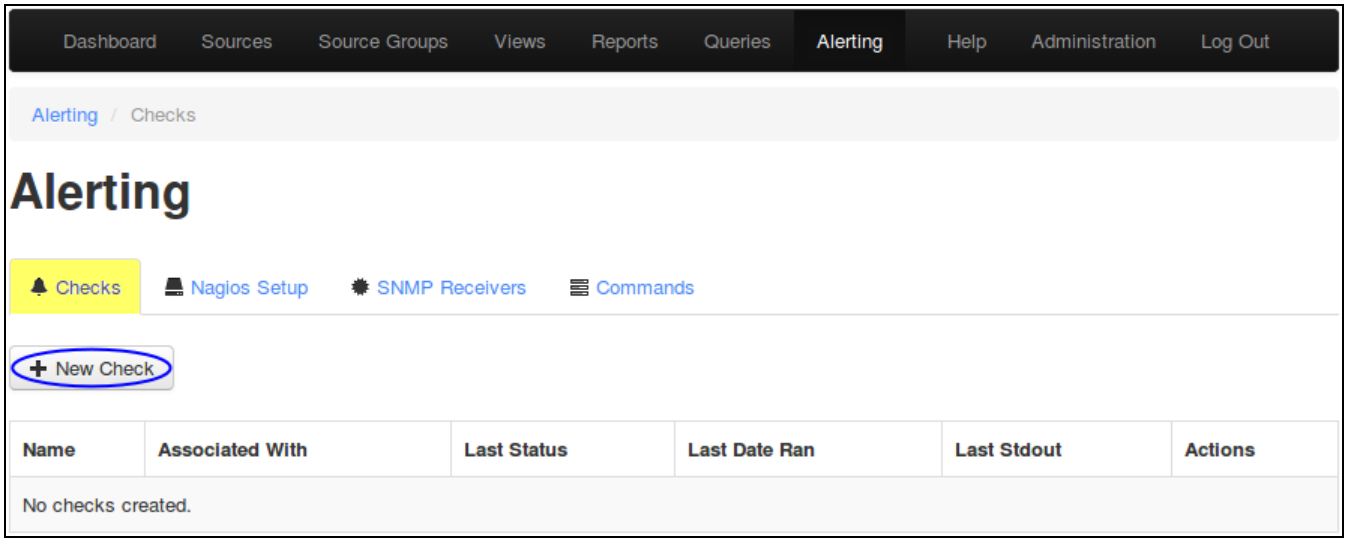

As per the notification, if your Nagios server is a Nagios XI server AND you have Dynamic Integration enabled all you need to do now is go into Core Configuration Manager in Nagios XI and apply configuration. This will create the new host and service objects ready to accept passive check results. If for some reason the services are not created, once the check in Network Analyzer has been created, the services will appear under Unconfigured Objects in Nagios XI (Admin > Monitoring Config).

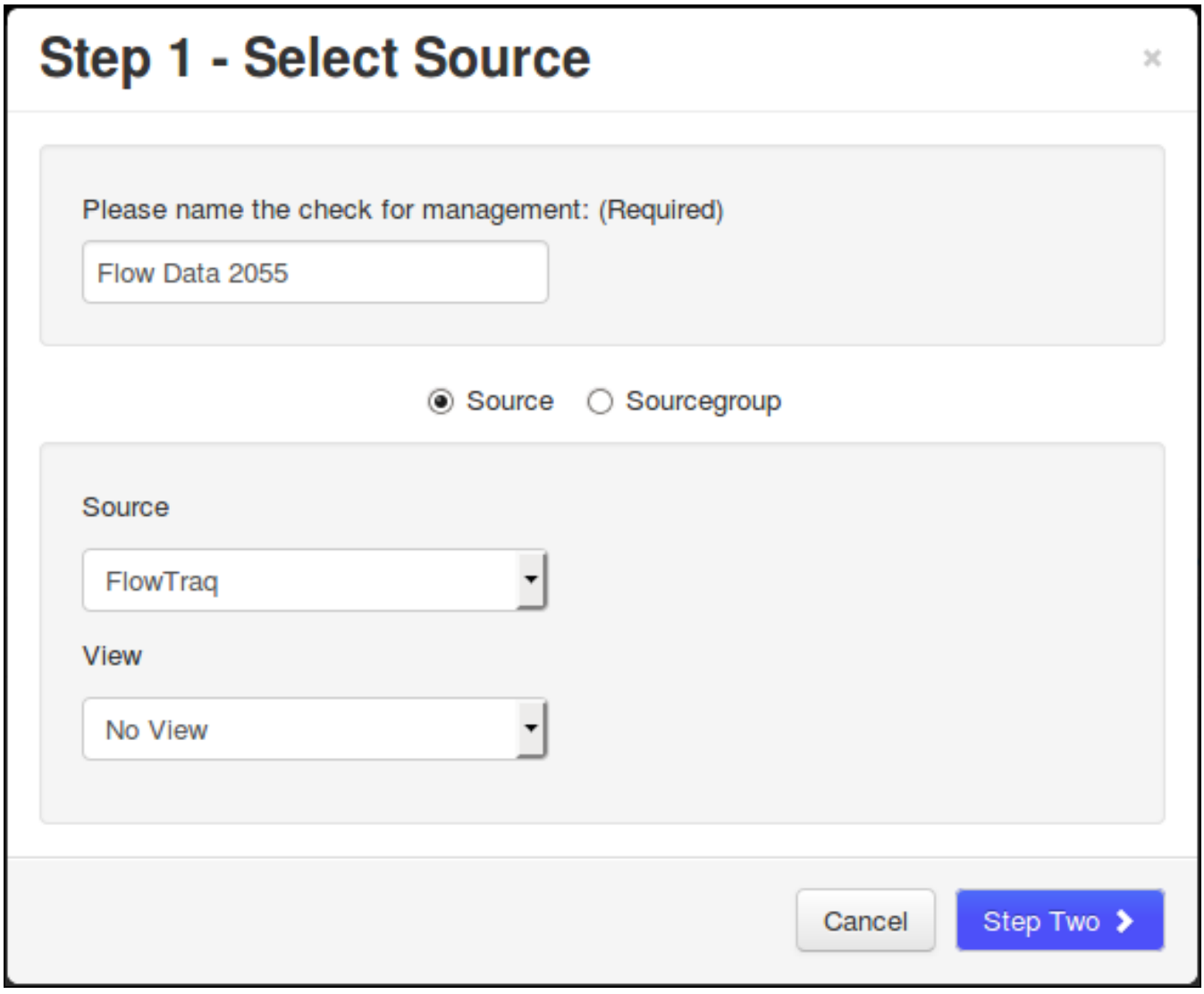
If you have Nagios Core, you will need to create your own passive services to accept these check results. Details on how to do this are outside the scope of this documentation however on the following page is a simple example:

```
define service {
    service_description       Source Working
    host_name                 10.25.14.3
    use                       generic-service
    active_checks_enabled     0
    passive_checks_enabled    1
    flap_detection_enabled    0
    check_period              24x7
    max_check_attempts        1
```

```
    check_interval          5
    retry_interval          1
    check_freshness         0
    contact_groups          admins
    notification_interval   60
    notification_period     24x7
    notification_options    w,u,c,r
}
```

The last remaining step is to define an alert so Nagios XI or Nagios Core will receive check results. The following example creates an alert that will notify if a source has no flow data received on the port that the flow data is being received on. Click the Checks tab and then click the New Check button.





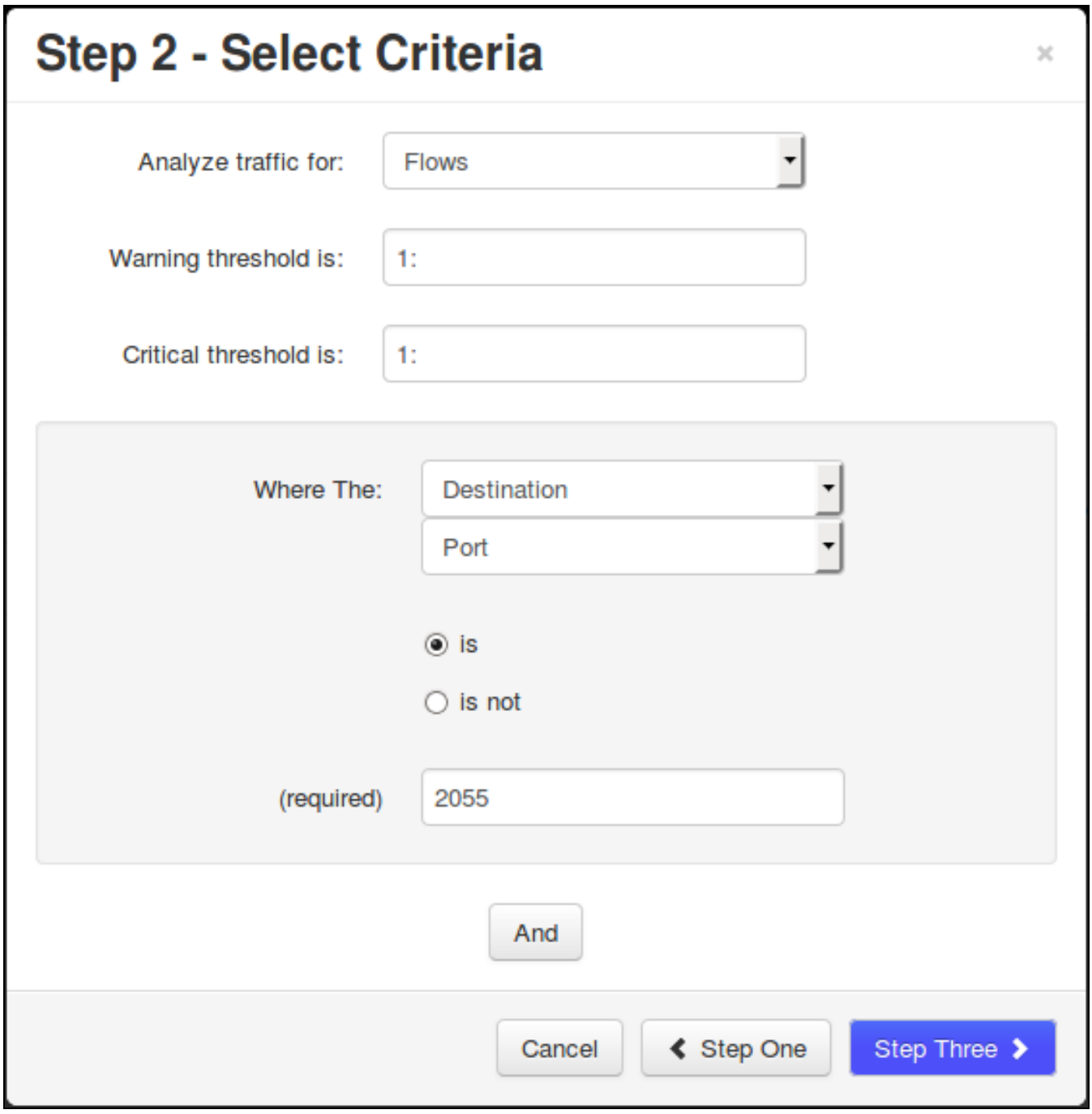

**Step 1**

You must enter a name for the check for management/organizational purposes. It can contain only whitespaces and alphanumeric characters.

Then you need to select your source or source group. This is the source the check will get values from. If you select a source, you can select a view to test against as well.

Click the Step Two button to proceed to Step 2.

**Step 2**




Analyze traffic for - This is the metric you would like to get the number for to check against. If you want a packet count, pick Packets. If you want total bytes, pick Bytes.

There are several other options, but the point is there are multiple dimensions to the traffic on your network, and this specifies which one will be checked.

Warning and Critical - Once Network Analyzer has extracted a number from the metric you selected, it will use these thresholds to determine if the number is in a WARNING, CRITICAL or OK state. In this example 1: means that if less than 1 was received then it will be in a CRITICAL state (meaning no flows were received).

More detailed information on thresholds is explained in the Nagios Threshold Values section of this document.

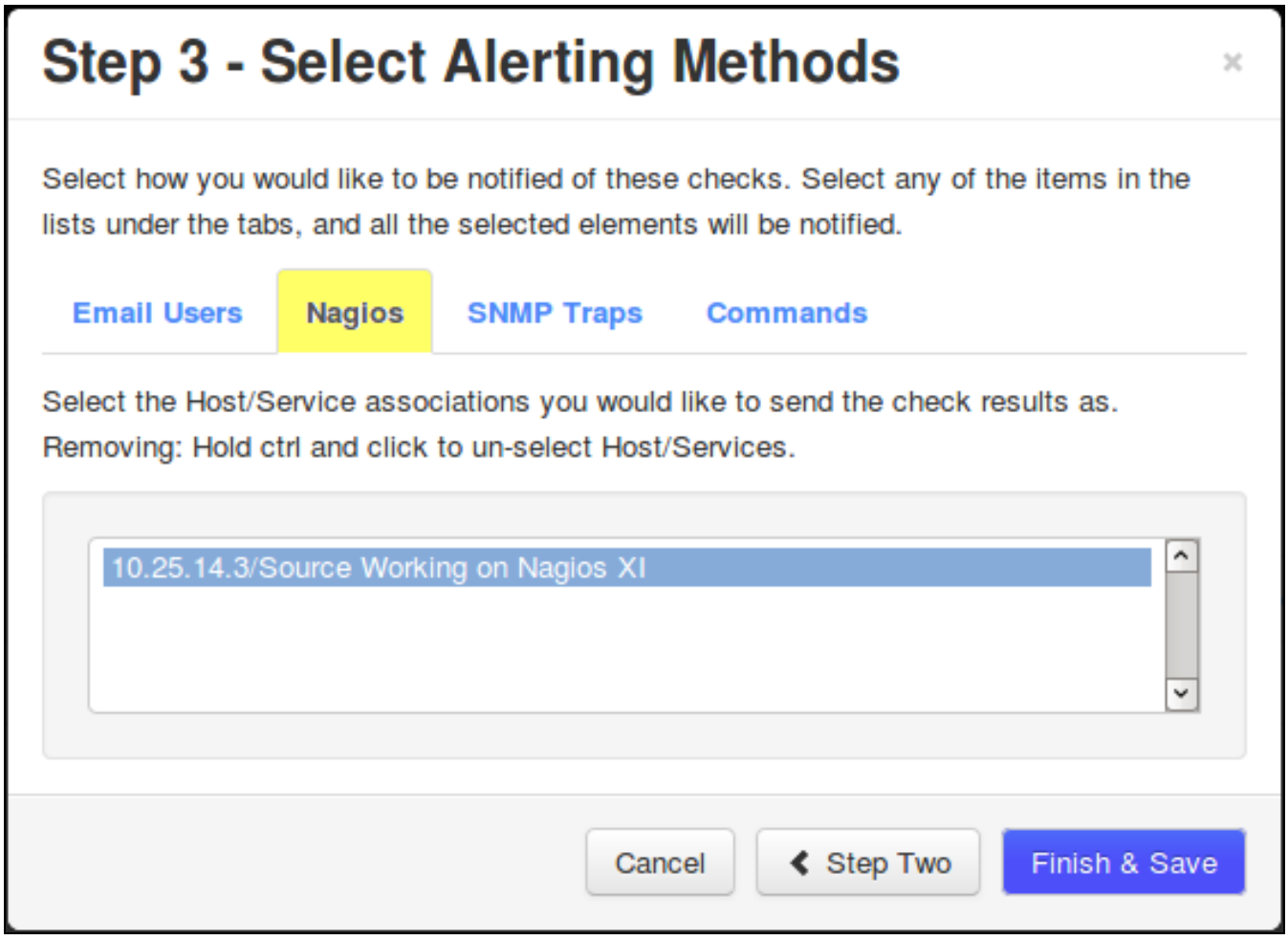
The bottom half of step 2 is how you filter what data the check is looking at, this allows granularity.

In the screenshot on the previous page, Flows is the type of traffic being analyzed. The filter criteria used is:

- Destination - The direction of the flow traffic being looked at
- Port - This check testing to make sure flow data is actually being received, seeing as the flow data is received on a port then this makes it easy to check
- is - This is the operation, we want to make sure the destination port IS 2055
- 2055 - Here the port number 2055 has been defined

Based on those selections, if no flow data is received it will be in a CRITICAL state, otherwise it will be OK.

You can specify as many of these filters as you would like by clicking the And button at the bottom. It will add a new box where you can specify additional filters. Please note that it is a Boolean AND, where the traffic must meet all specifications that are chosen for the check to be used.

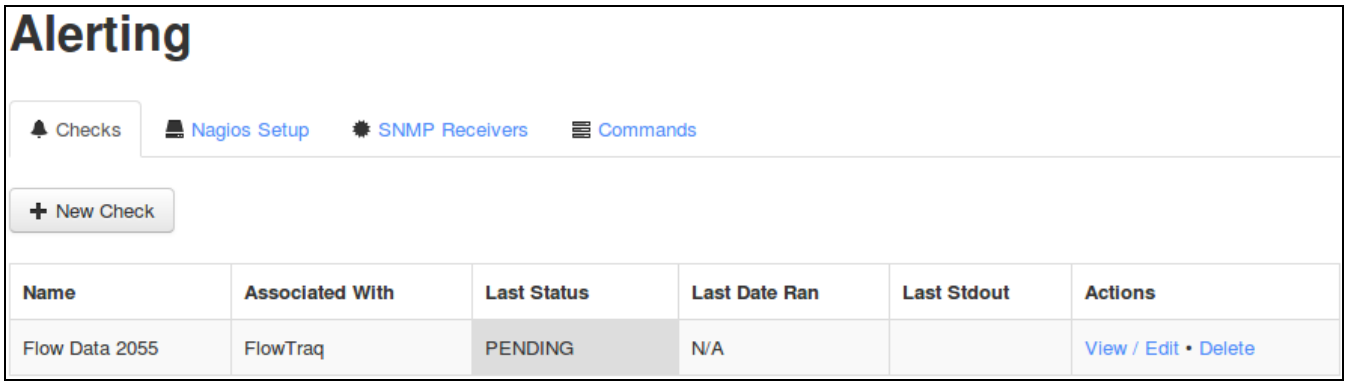



Click the Step Three button to proceed to Step 3.

Here you select the alerting method. In this example the Nagios tab has been selected and the Servicename/Hostname that was previously defined has been selected.

Click the Finish and Save button to create the alert.

The check will be created and will appear on the screen in a pending state:




Here is an example of the check when it had a CRITICAL state:

| Name | Associated With | Last Status | Last Date Ran | Last Stdout | Actions |
|---|---|---|---|---|---|
| Flow Data 2055 | FlowTraq | CRITICAL | 2017-05-15 21:35:10 | flows on FlowTraq with filter `dst port 2055` is 0 \| flows=0;1:;1:;0 | View / Edit • Delete |

Here is an example of the check when it had a OK state:

| Name | Associated With | Last Status | Last Date Ran | Last Stdout | Actions |
|---|---|---|---|---|---|
| Flow Data 2055 | FlowTraq | OK | 2017-05-15 21:40:10 | flows on FlowTraq with filter `dst port 2055` is 3 \| flows=3;1:;1:;0 | View / Edit • Delete |

Here is the service in Nagios when it had a CRITICAL state:

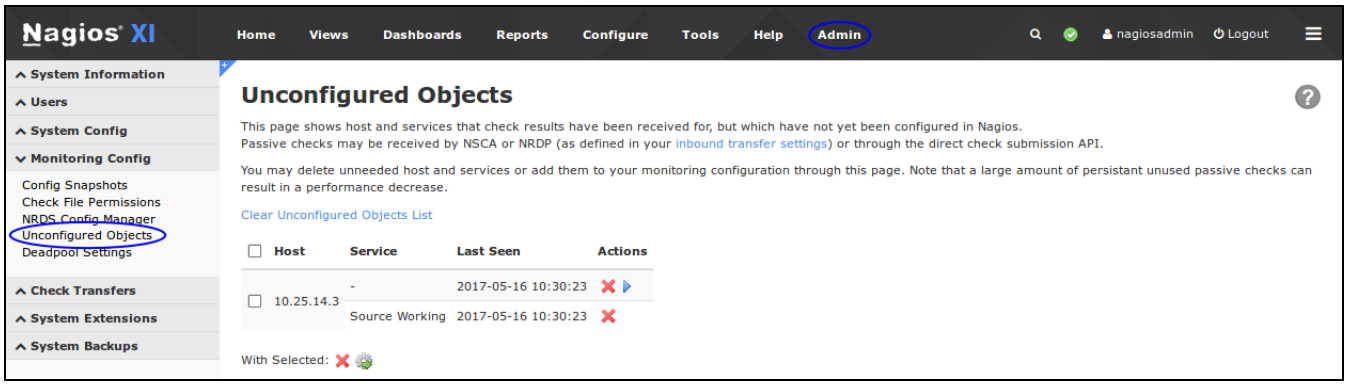
| Host | Service | Status | Duration | Attempt | Last Check | Status Information |
|---|---|---|---|---|---|---|
| 10.25.14.3 | Source Working | Critical | 34s | 1/1 | 2017-05-16 10:40:10 | flows on FlowTraq with filter `dst port 2055` is 0 |

Here is the service in Nagios when it had an OK state:

| Host | Service | Status | Duration | Attempt | Last Check | Status Information |
|---|---|---|---|---|---|---|
| 10.25.14.3 | Source Working | Ok | 1m 4s | 1/1 | 2017-05-16 10:35:10 | flows on FlowTraq with filter `dst port 2055` is 1 |

The checks are run every five minutes, it's important to understand that every five minutes the check will fire off a notification to Nagios XI or Nagios Core. Based on the WARNING and CRITICAL thresholds you defined on the check, Nagios will receive the check results with the state from the check.

Note: If the services did not appear in Nagios XI after applying configuration, the services will appear under Unconfigured Objects in Nagios XI (Admin > Monitoring Config).




Check the box on the left and click the gear icon below to run the Unconfigured Objects wizard. More information on Unconfigured Objects can be found in the following documentation:

Monitoring Unconfigured Objects With XI

---

## Leveraging The API

You can also query the check results directly from the API. Here is an example using the query defined in the previous section (assuming you are already logged into Nagios Network Analyzer):

http://na_ip_address/nagiosna/index.php/api/checks/read?q[name]=Flow%20Data%202055

This will return JSON output:

[{"cid":"1","rawquery":"dst port 2055","name":"Flow Data 2055","warning":"1:","sid":"1","-

gid":null,"vid":null,"active":"1","critical":"1:","aberrant":"0","lastval":"1","lastrun":"2017-05-16 10:50:10","lastcode":"0","laststdout":"flows on FlowTraq with filter `dst port 2055` is 1 | flows-s=1;1:;1:;0","metric":"flows","assoc_with":"FlowTraq"}]

You can also use a curl command from another machine, however this requires your API key to be submitted with the token argument, for example (this is one long command):

curl -g "http://na_ip_address/n-agiosna/in-dex.php/api/checks/read?token=7314f41c330ebc40e48e4cb64a05dcbbb4778679&q[name]=Flow%20Data%202055"

When used in a script you can programmatically access the data in the JSON object and do what you like with it.

## Nagios Threshold Values

Nagios Thresholds can be complicated to initially understand, however once grasped they can be very powerful. Documentation on Nagios thresholds is available here:

https://nagios-plugins.org/doc/guidelines.html#THRESHOLDFORMAT

The Nagios Threshold standards were designed with many different use cases, for example negative numbers are valid values. However in the case of Nagios Network Analyzer, the alert value being tested will always be 0 or greater (no negative numbers are involved).

## Network Ports

The following network ports are used for communication between Nagios Network Anaylzer and Nagios XI or Nagios Core:

- Nagios XI Integration communicates with the Nagios Network Analyzer server on TCP 80 or 443

- Nagios Network Analyzer when using NRDP for sending passive check to Nagios XI or Nagios Core occurs on on TCP 80 or 443