Cyber security

Md. Abdul Hai Al Hadi
Date: 19 March 2021

Objectives:

1. What is Nagios?
2. Why we need Nagios?
3. Disadvantages of using Nagios?
4. All products of Nagios?
5. How we use and understand Nagios XI that monitors systems, networks and critical IT Infrastructure?
6. How we use and understand Nagios Log Server?

What is Nagios?

Any organization can contain a complex system of computers, servers, services, applications and more. A large amount of data are floating around in the cloud. It requires an interpreter, a guide, a watch-guard, in order to make sense of it and help promote efficiency and network security. Monitoring and managing infrastructure's data has all been streamlined through one suite of solutions. So, it's called **"The industry standard in IT infrastructure monitoring".**
Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes.

Nagios Core, formerly known as **Nagios**, is a free and open-source computer-software application that monitors systems, networks and infrastructure.

Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

Why We Need Nagios?

Here, are Important reasons to use Nagios monitoring tool are:

- Detects all types of network or server issues.
- Helps us to find the root cause of the problem which allows us to get the permanent solution to the problem.
- Active monitoring of our entire infrastructure and business processes.
- Allows us to monitors and troubleshoot server performance issues.

- Helps us to plan for infrastructure upgrades before outdated systems create failures.
- We can maintain the security and availability of the service.
- Automatically fix problems in a panic situation.

Disadvantages of Using Nagios

- Important feature like wizards or interactive dashboard are only available on Nagios XI, which is quite an expensive tool.
- Nagios core has a confusing interface.
- There're many configuration files which are very hard to configure for users.
- Nagios can't monitor network throughput.
- The tool not allows us to manage the network but only allows to monitor the network.
- Nagios makes no difference between various devices like servers, routers, or switches as it treats every device as a host.

All products of Nagios?

1. Nagios XI
2. Nagios Log Server
3. Nagios Network Analyzer
4. Nagios Fusion
5. Nagios Core

Nagios XI

we will be able to see exactly where the problem comes from on our infrastructure, and handle it quickly and efficiently, saving the time and money for our organization before it affects critical business processes.

Nagios Log Server

The powerful enterprise-grade log monitoring and management application
that allows us to quickly and easily view, sort and configure logs from any source on any given network, allowing us to start making sense of our data.

Nagios Network Analyzer

The commercial-grade network flow data analysis solution that provides us with network traffic and bandwidth information of our infrastructure, making it easier for us to see where the bandwidth is dipping or spiking.

Nagios Fusion

Provides a centralized visual operational status, and enables faster problem resolution over our entire IT infrastructure. Now we can determine which service is down, what is taking up the bandwidth, where is the data is coming from, and how to resolve it. Servers, applications, routers, switches, and more, all able to monitored and manage with Nagios, making us the master of our data.

Nagios Core

The open source industry standard in IT infrastructure monitoring and alerting.

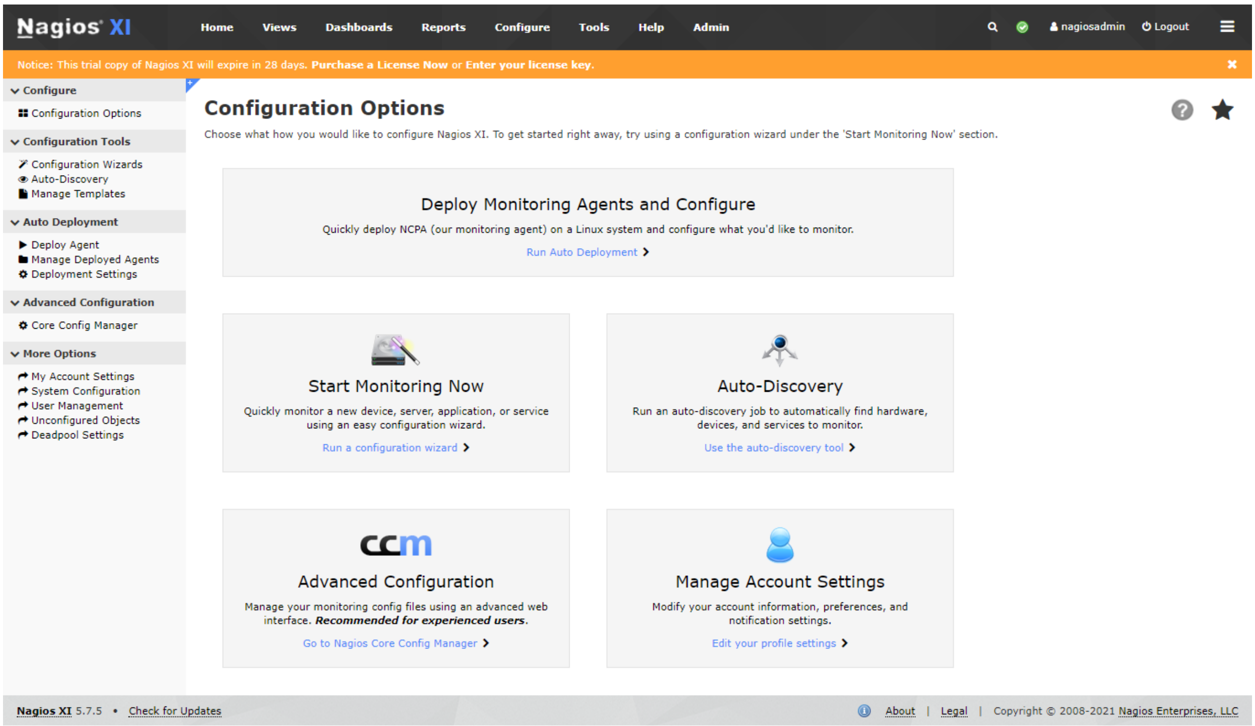
Recommended Software: Nagios XI

http://nagiosxi.demos.nagios.com/nagiosxi/login.php

How we use and understand Nagios XI that monitors systems, networks and critical IT Infrastructure?

Configure, monitoring setup

Add or modify items to be monitored.



Notice: This trial copy of Nagios XI will expire in 28 days. **Purchase a License Now** or **Enter your license key.**

Configuration Options

Choose what how you would like to configure Nagios XI. To get started right away, try using a configuration wizard under the 'Start Monitoring Now' section.

Deploy Monitoring Agents and Configure

Quickly deploy NCPA (our monitoring agent) on a Linux system and configure what you'd like to monitor.

Run Auto Deployment ›

Start Monitoring Now

Quickly monitor a new device, server, application, or service using an easy configuration wizard.

Run a configuration wizard ›

Auto-Discovery

Run an auto-discovery job to automatically find hardware, devices, and services to monitor.

Use the auto-discovery tool ›

Advanced Configuration

Manage your monitoring config files using an advanced web interface. ***Recommended for experienced users.***

Go to Nagios Core Config Manager ›

Manage Account Settings

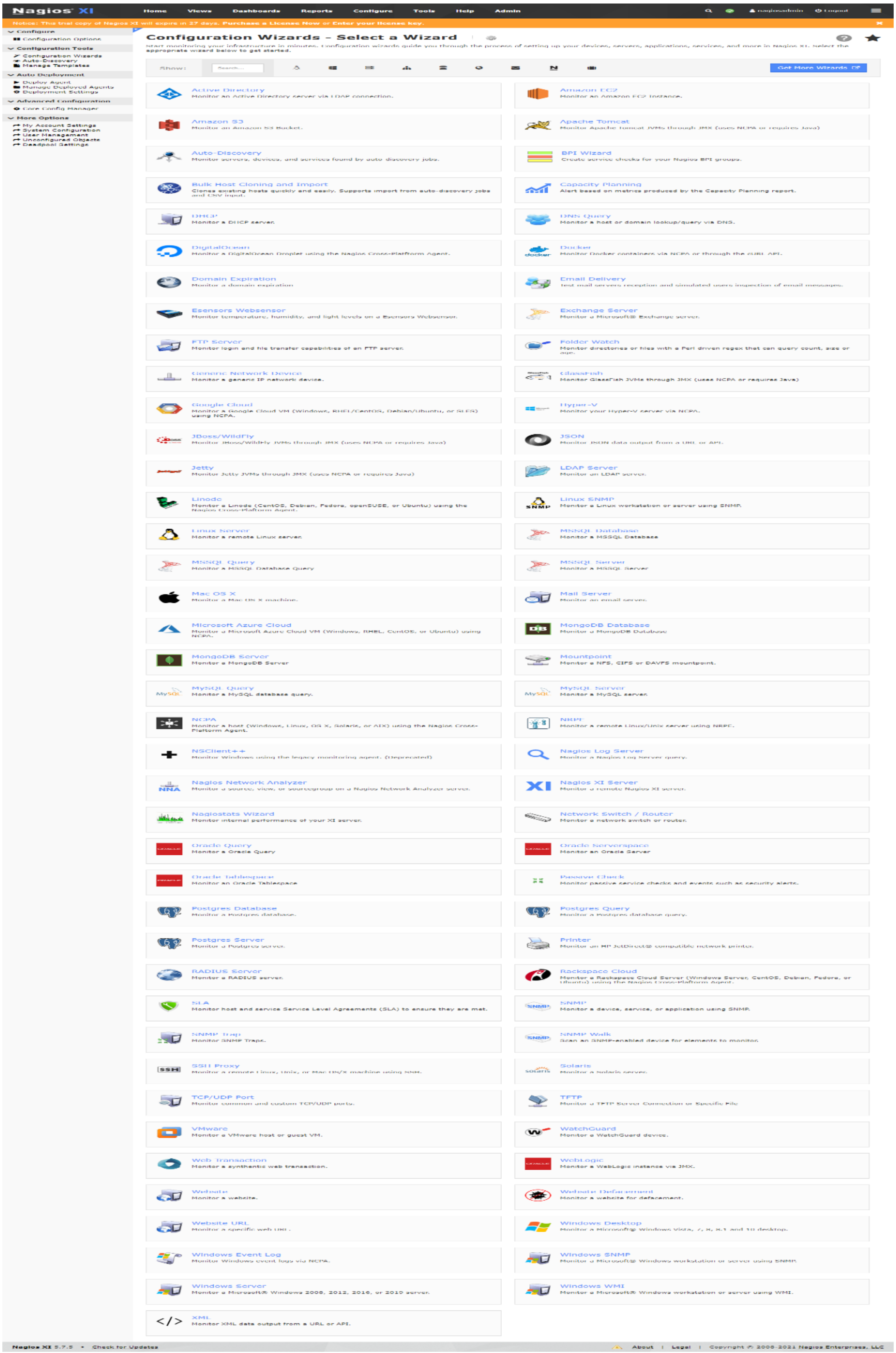
Modify your account information, preferences, and notification settings.

Edit your profile settings ›

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Configuration Wizards,



Notice: This trial copy of Nagios XI will expire in 27 days. Purchase a License Now or Enter your license key.

Configuration Wizards - Select a Wizard

Start monitoring your infrastructure in minutes. Configuration wizards guide you through the process of setting up your devices, servers, applications, services, and more in Nagios XI. Select the appropriate wizard below to get started.

Active Directory
Monitor an Active Directory server via LDAP connection.

Amazon EC2
Monitor an Amazon EC2 Instance.

Amazon S3
Monitor an Amazon S3 Bucket.

Apache Tomcat
Monitor Apache Tomcat JVMs through JMX (uses NCPA or requires Java)

Auto-Discovery
Monitor servers, devices, and services found by auto discovery jobs.

BPI Wizard
Create service checks for your Nagios BPI groups.

Bulk Host Cloning and Import
Clones existing hosts quickly and easily. Supports import from auto-discovery jobs and CSV input.

Capacity Planning
Alert based on metrics produced by the Capacity Planning report.

DHCP
Monitor a DHCP server.

DNS Query
Monitor a host or domain lookup/query via DNS.

DigitalOcean
Monitor a DigitalOcean Droplet using the Nagios Cross-Platform Agent.

Docker
Monitor Docker containers via NCPA or through the cURL API.

Domain Expiration
Monitor a domain expiration

Email Delivery
Test mail servers reception and simulated users inspection of email messages.

Esensors Websensor
Monitor temperature, humidity, and light levels on a Esensors Websensor.

Exchange Server
Monitor a Microsoft® Exchange server.

FTP Server
Monitor login and file transfer capabilities of an FTP server.

Folder Watch
Monitor directories or files with a Perl driven regex that can query count, size or age.

Generic Network Device
Monitor a generic IP network device.

GlassFish
Monitor GlassFish JVMs through JMX (uses NCPA or requires Java)

Google Cloud
Monitor a Google Cloud VM (Windows, RHEL/CentOS, Debian/Ubuntu, or SLES) using NCPA.

Hyper-V
Monitor your Hyper-V server via NCPA.

JBoss/WildFly
Monitor JBoss/WildFly JVMs through JMX (uses NCPA or requires Java)

JSON
Monitor JSON data output from a URL or API.

Jetty
Monitor Jetty JVMs through JMX (uses NCPA or requires Java)

LDAP Server
Monitor an LDAP server.

Linode
Monitor a Linode (CentOS, Debian, Fedora, openSUSE, or Ubuntu) using the Nagios Cross-Platform Agent.

Linux SNMP
Monitor a Linux workstation or server using SNMP.

Linux Server
Monitor a remote Linux server.

MSSQL Database
Monitor a MSSQL Database

MSSQL Query
Monitor a MSSQL Database Query

MSSQL Server
Monitor a MSSQL Server

Mac OS X
Monitor a Mac OS X machine.

Mail Server
Monitor an email server.

Microsoft Azure Cloud
Monitor a Microsoft Azure Cloud VM (Windows, RHEL, CentOS, or Ubuntu) using NCPA.

MongoDB Database
Monitor a MongoDB Database

MongoDB Server
Monitor a MongoDB Server

Mountpoint
Monitor a NFS, CIFS or DAVFS mountpoint.

MySQL Query
Monitor a MySQL database query.

MySQL Server
Monitor a MySQL server.

NCPA
Monitor a host (Windows, Linux, OS X, Solaris, or AIX) using the Nagios Cross-Platform Agent.

NRPE
Monitor a remote Linux/Unix server using NRPE.

NSClient++
Monitor Windows using the legacy monitoring agent. (Deprecated)

Nagios Log Server
Monitor a Nagios Log Server query.

Nagios Network Analyzer
Monitor a source, view, or sourcegroup on a Nagios Network Analyzer server.

Nagios XI Server
Monitor a remote Nagios XI server.

Nagiostats Wizard
Monitor internal performance of your XI server.

Network Switch / Router
Monitor a network switch or router.

Oracle Query
Monitor a Oracle Query

Oracle Serverspace
Monitor an Oracle Server

Oracle Tablespace
Monitor an Oracle Tablespace

Passive Check
Monitor passive service checks and events such as security alerts.

Postgres Database
Monitor a Postgres database.

Postgres Query
Monitor a Postgres database query.

Postgres Server
Monitor a Postgres server.

Printer
Monitor an HP JetDirect® compatible network printer.

RADIUS Server
Monitor a RADIUS server.

Rackspace Cloud
Monitor a Rackspace Cloud Server (Windows Server, CentOS, Debian, Fedora, or Ubuntu) using the Nagios Cross-Platform Agent.

SLA
Monitor host and service Service Level Agreements (SLA) to ensure they are met.

SNMP
Monitor a device, service, or application using SNMP.

SNMP Trap
Monitor SNMP Traps.

SNMP Walk
Scan an SNMP-enabled device for elements to monitor.

SSH Proxy
Monitor a remote Linux, Unix, or Mac OS/X machine using SSH.

Solaris
Monitor a Solaris server.

TCP/UDP Port
Monitor common and custom TCP/UDP ports.

TFTP
Monitor a TFTP Server Connection or Specific File

VMware
Monitor a VMware host or guest VM.

WatchGuard
Monitor a WatchGuard device.

Web Transaction
Monitor a synthentic web transaction.

WebLogic
Monitor a WebLogic instance via JMX.

Website
Monitor a website.

Website Defacement
Monitor a website for defacement.

Website URL
Monitor a specific web URL.

Windows Desktop
Monitor a Microsoft® Windows Vista, 7, 8, 8.1 and 10 desktop.

Windows Event Log
Monitor Windows event logs via NCPA.

Windows SNMP
Monitor a Microsoft® Windows workstation or server using SNMP.

Windows Server
Monitor a Microsoft® Windows 2008, 2012, 2016, or 2019 server.

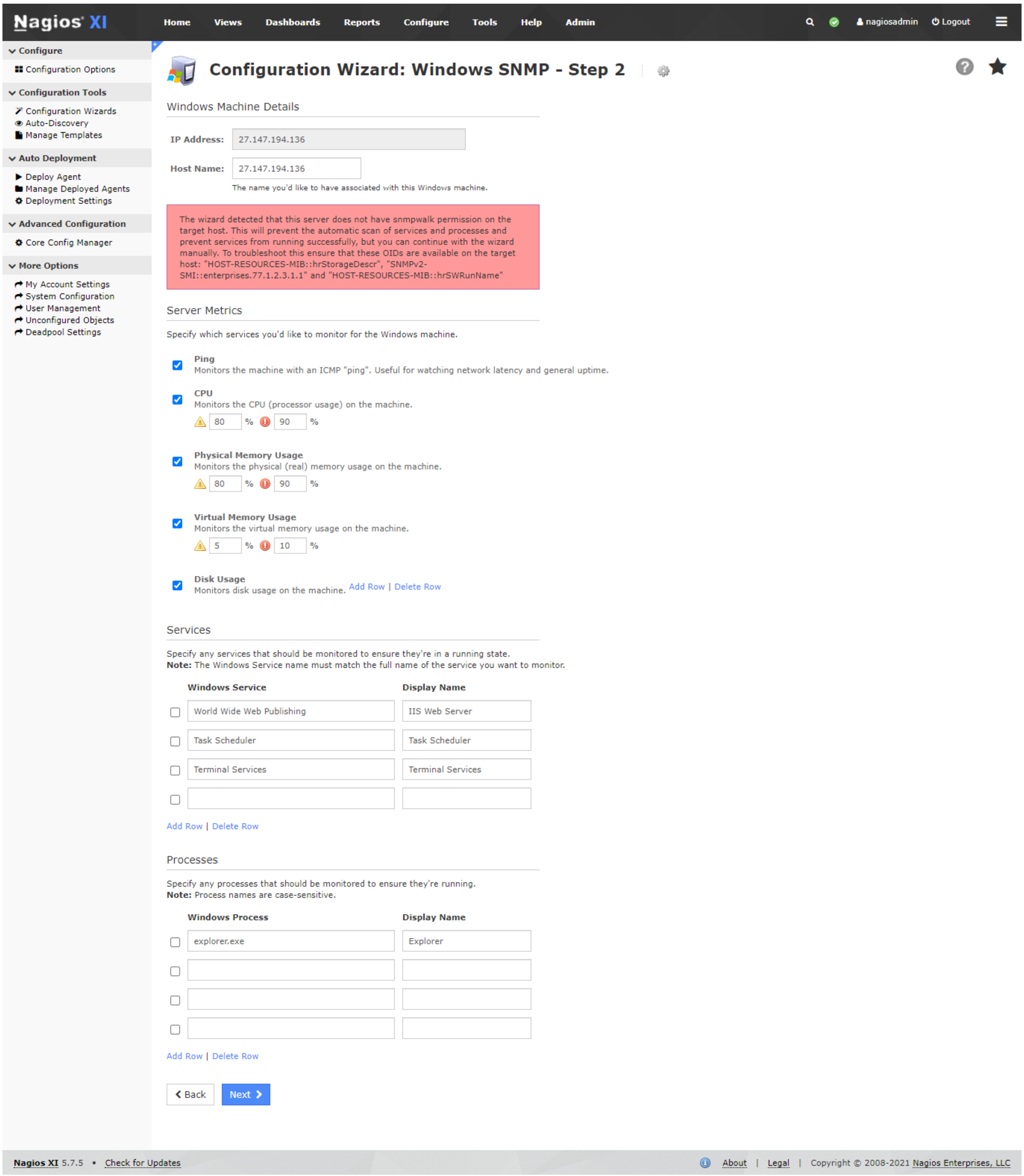
Windows WMI
Monitor a Microsoft® Windows workstation or server using WMI.

XML
Monitor XML data output from a URL or API.

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Configuration Wizards Step 2,



Configuration Wizard: Windows SNMP - Step 2

Windows Machine Details

IP Address: 27.147.194.136

Host Name: 27.147.194.136

The name you'd like to have associated with this Windows machine.

The wizard detected that this server does not have snmpwalk permission on the target host. This will prevent the automatic scan of services and processes and prevent services from running successfully, but you can continue with the wizard manually. To troubleshoot this ensure that these OIDs are available on the target host: "HOST-RESOURCES-MIB::hrStorageDescr", "SNMPv2-SMI::enterprises.77.1.2.3.1.1" and "HOST-RESOURCES-MIB::hrSWRunName"

Server Metrics

Specify which services you'd like to monitor for the Windows machine.

☑ **Ping**
Monitors the machine with an ICMP "ping". Useful for watching network latency and general uptime.

☑ **CPU**
Monitors the CPU (processor usage) on the machine.
⚠ 80 % ❗ 90 %

☑ **Physical Memory Usage**
Monitors the physical (real) memory usage on the machine.
⚠ 80 % ❗ 90 %

☑ **Virtual Memory Usage**
Monitors the virtual memory usage on the machine.
⚠ 5 % ❗ 10 %

☑ **Disk Usage**
Monitors disk usage on the machine. Add Row | Delete Row

Services

Specify any services that should be monitored to ensure they're in a running state.
Note: The Windows Service name must match the full name of the service you want to monitor.

	Windows Service	Display Name
□	World Wide Web Publishing	IIS Web Server
□	Task Scheduler	Task Scheduler
□	Terminal Services	Terminal Services
□		

Add Row | Delete Row

Processes

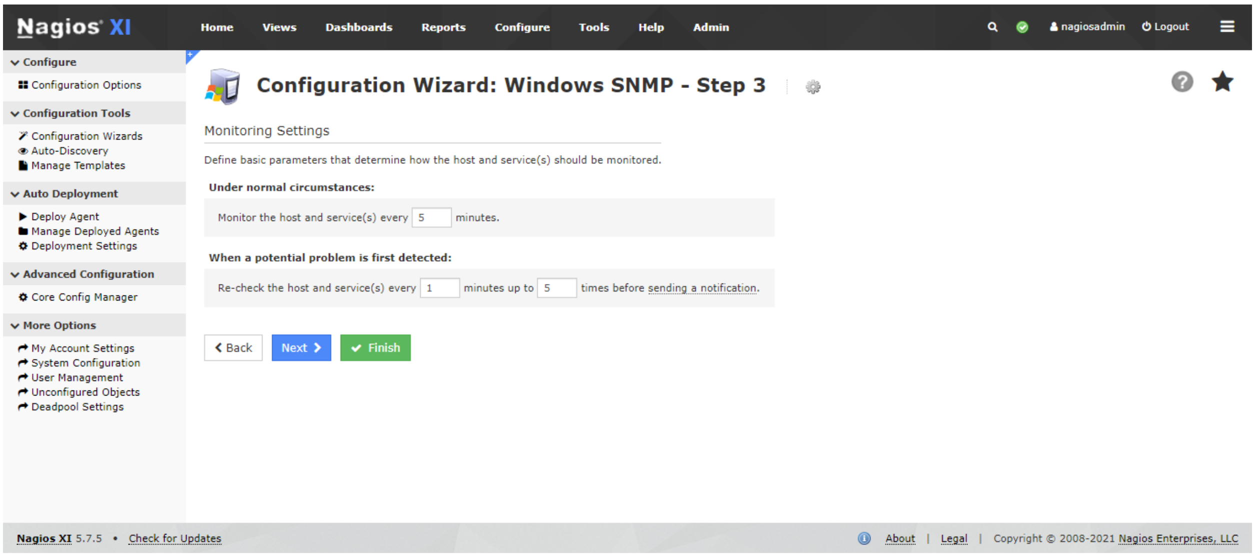
Specify any processes that should be monitored to ensure they're running.
Note: Process names are case-sensitive.

	Windows Process	Display Name
□	explorer.exe	Explorer
□		
□		
□		

Add Row | Delete Row

Nagios XI 5.7.5 • Check for Updates
About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Configuration Wizards Step 3,



Configuration Wizard: Windows SNMP - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

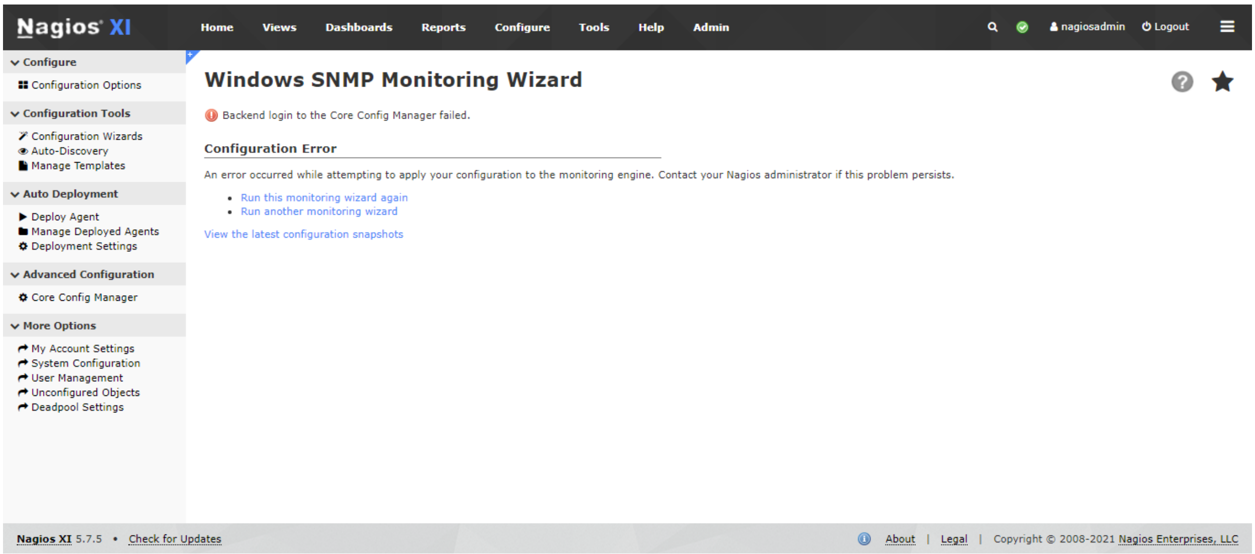
Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:

Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.

Back
Next
Finish
Nagios XI 5.7.5 • Check for Updates
About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Configuration Wizards Step 4,



Windows SNMP Monitoring Wizard

Backend login to the Core Config Manager failed.

Configuration Error

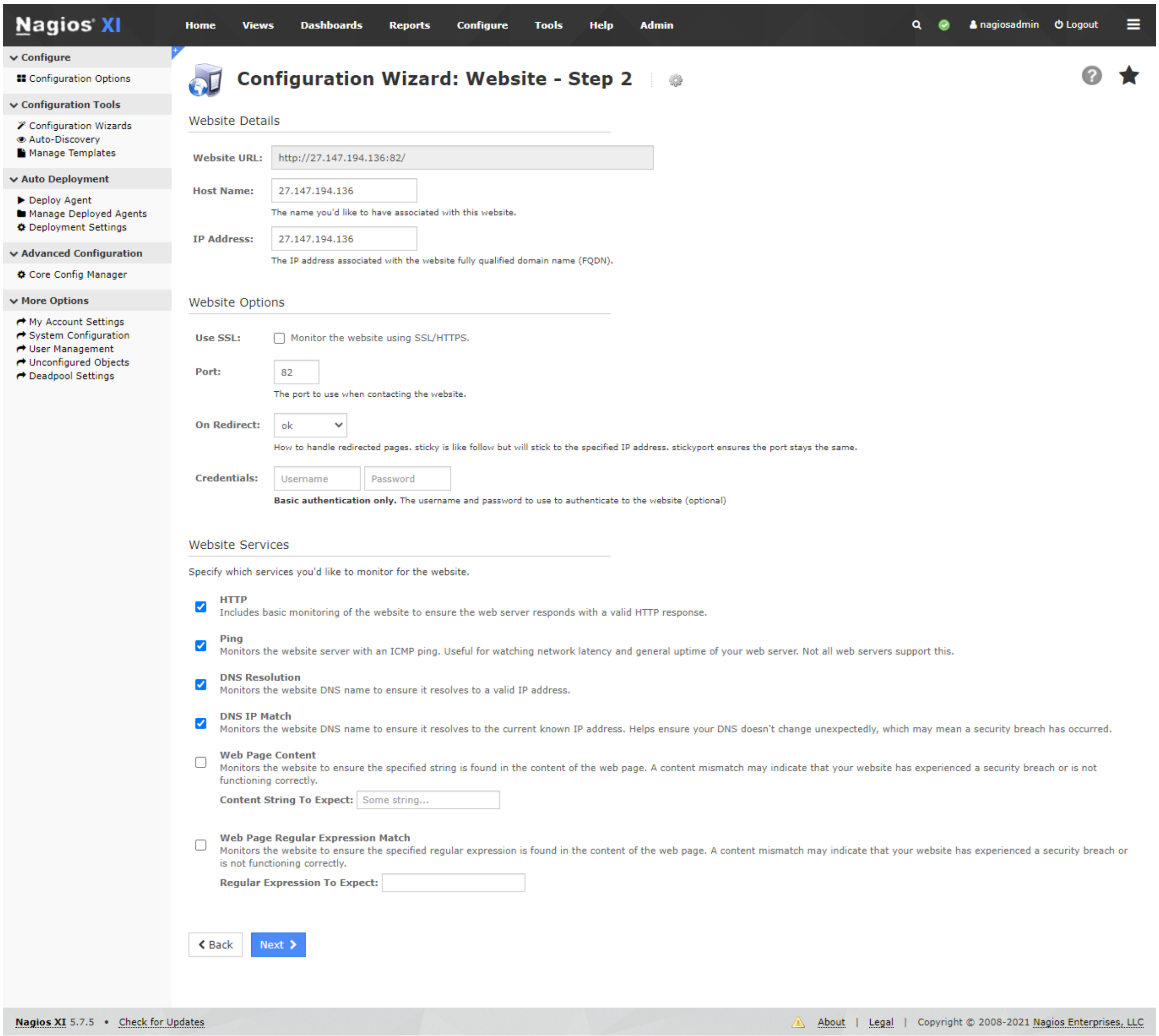
An error occurred while attempting to apply your configuration to the monitoring engine. Contact your Nagios administrator if this problem persists.

- Run this monitoring wizard again
- Run another monitoring wizard

View the latest configuration snapshots

Nagios XI 5.7.5 • Check for Updates
About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Web site monitor,



Configuration Wizard: Website - Step 2

Website Details

Website URL: http://27.147.194.136:82/

Host Name: 27.147.194.136

The name you'd like to have associated with this website.

IP Address: 27.147.194.136

The IP address associated with the website fully qualified domain name (FQDN).

Website Options

Use SSL: □ Monitor the website using SSL/HTTPS.

Port: 82

The port to use when contacting the website.

On Redirect: ok

How to handle redirected pages. sticky is like follow but will stick to the specified IP address. stickyport ensures the port stays the same.

Credentials: Username Password

Basic authentication only. The username and password to use to authenticate to the website (optional)

Website Services

Specify which services you'd like to monitor for the website.

☑ **HTTP**
Includes basic monitoring of the website to ensure the web server responds with a valid HTTP response.

☑ **Ping**
Monitors the website server with an ICMP ping. Useful for watching network latency and general uptime of your web server. Not all web servers support this.

☑ **DNS Resolution**
Monitors the website DNS name to ensure it resolves to a valid IP address.

☑ **DNS IP Match**
Monitors the website DNS name to ensure it resolves to the current known IP address. Helps ensure your DNS doesn't change unexpectedly, which may mean a security breach has occurred.

□ **Web Page Content**
Monitors the website to ensure the specified string is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.

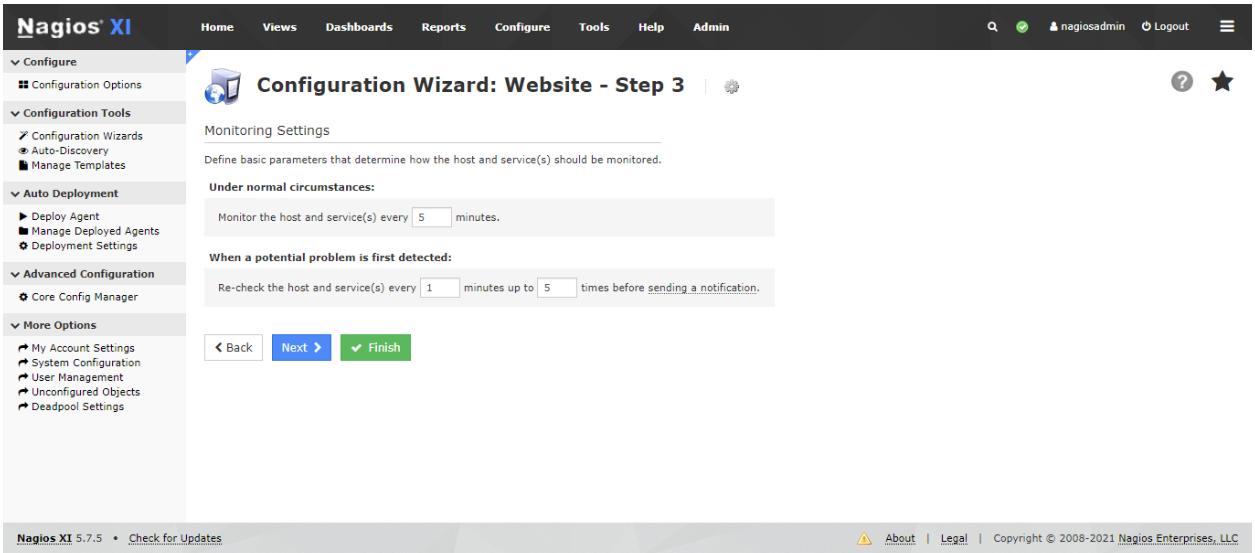
Content String To Expect: Some string...

□ **Web Page Regular Expression Match**
Monitors the website to ensure the specified regular expression is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.

Regular Expression To Expect:

Back
Next
Nagios XI 5.7.5 • Check for Updates
About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Web site monitor, Step 2,



Configuration Wizard: Website - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

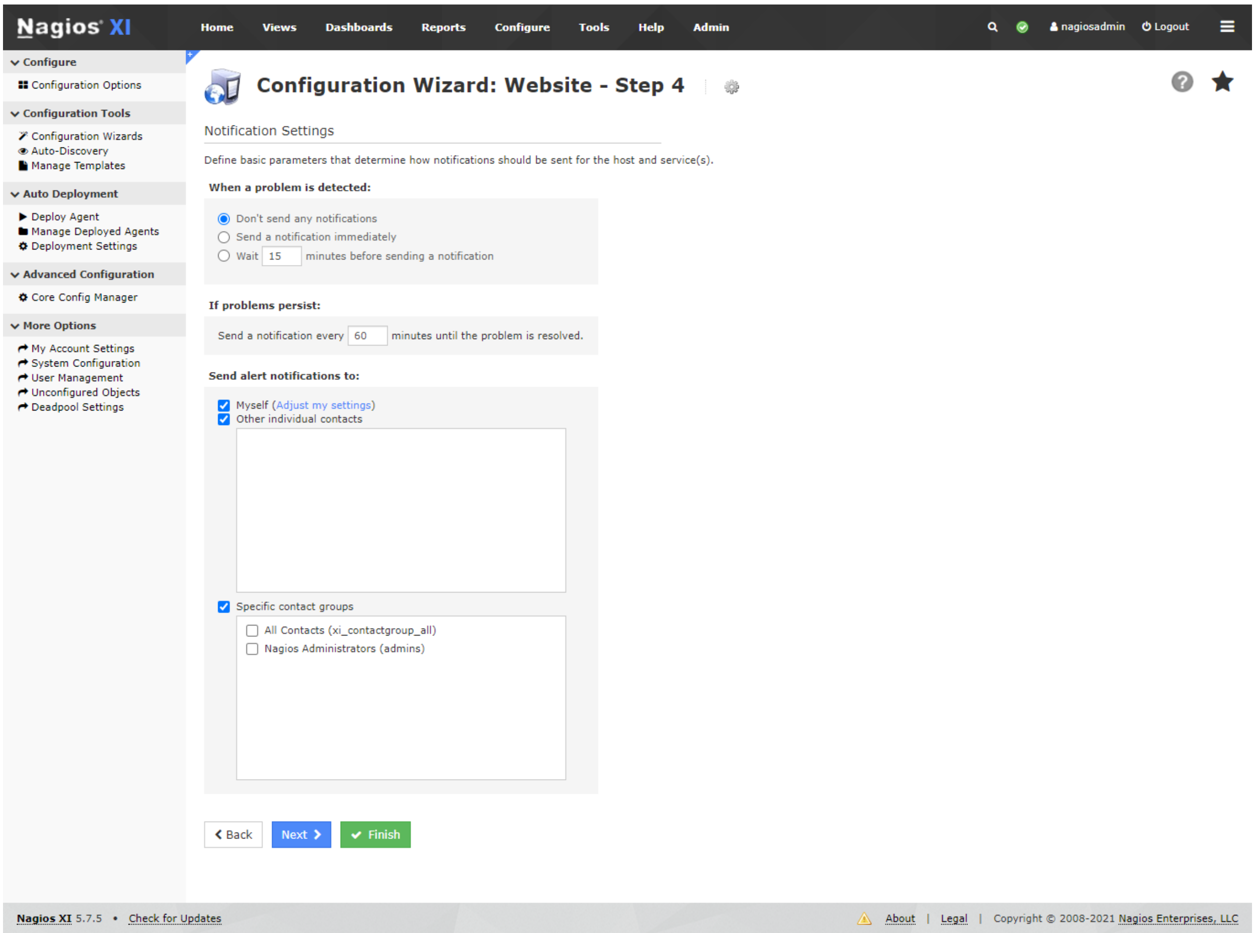
Under normal circumstances:

Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:

Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.

Web site monitor, Step 3,



Configuration Wizard: Website - Step 4

Notification Settings

Define basic parameters that determine how notifications should be sent for the host and service(s).

When a problem is detected:

● Don't send any notifications
○ Send a notification immediately
○ Wait 15 minutes before sending a notification

If problems persist:

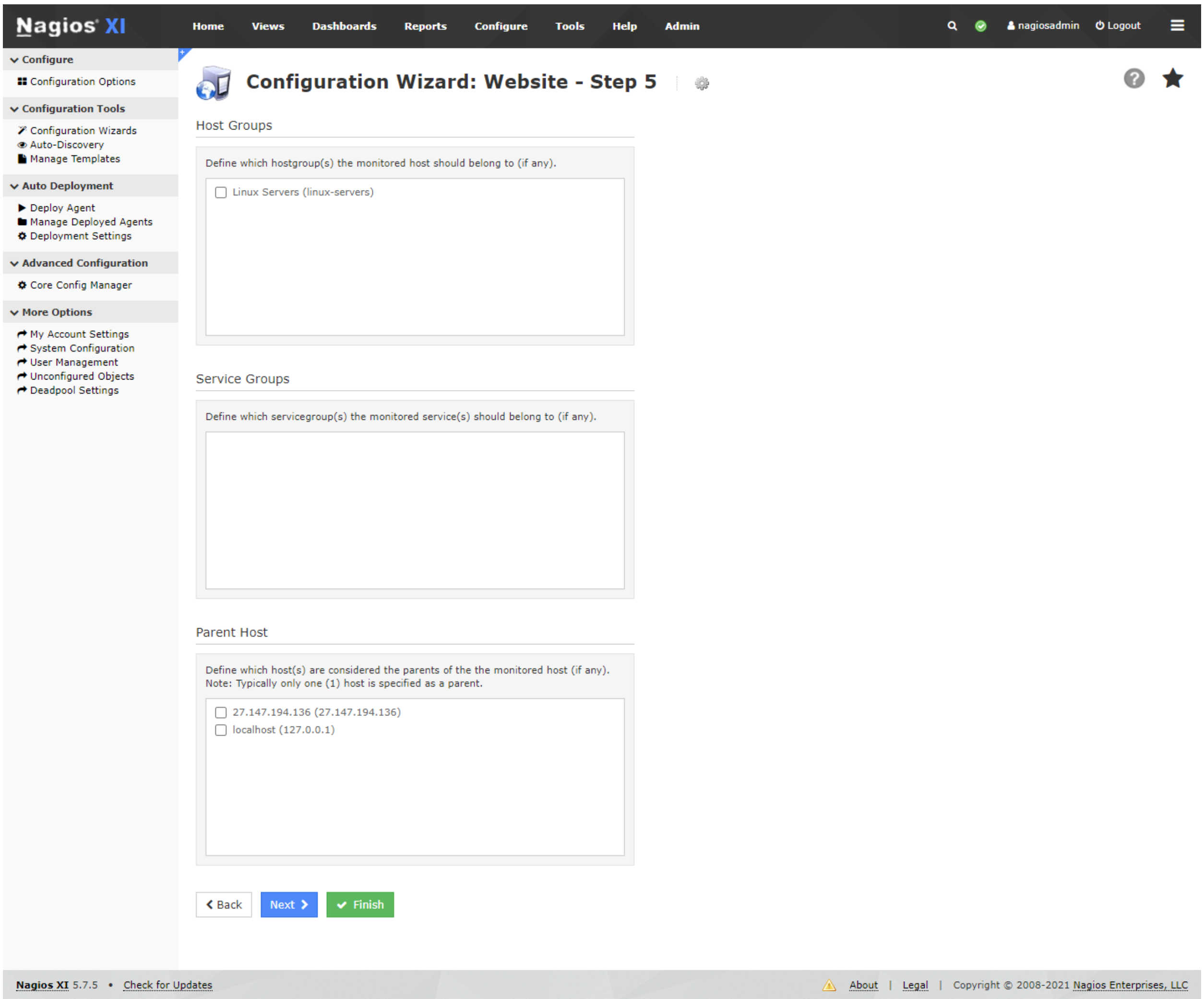
Send a notification every 60 minutes until the problem is resolved.

Send alert notifications to:

☑ Myself (Adjust my settings)
☑ Other individual contacts

☑ Specific contact groups
□ All Contacts (xi_contactgroup_all)
□ Nagios Administrators (admins)

Web site monitor, Step 4,



Configuration Wizard: Website - Step 5

Host Groups

Define which hostgroup(s) the monitored host should belong to (if any).

□ Linux Servers (linux-servers)

Service Groups

Define which servicegroup(s) the monitored service(s) should belong to (if any).

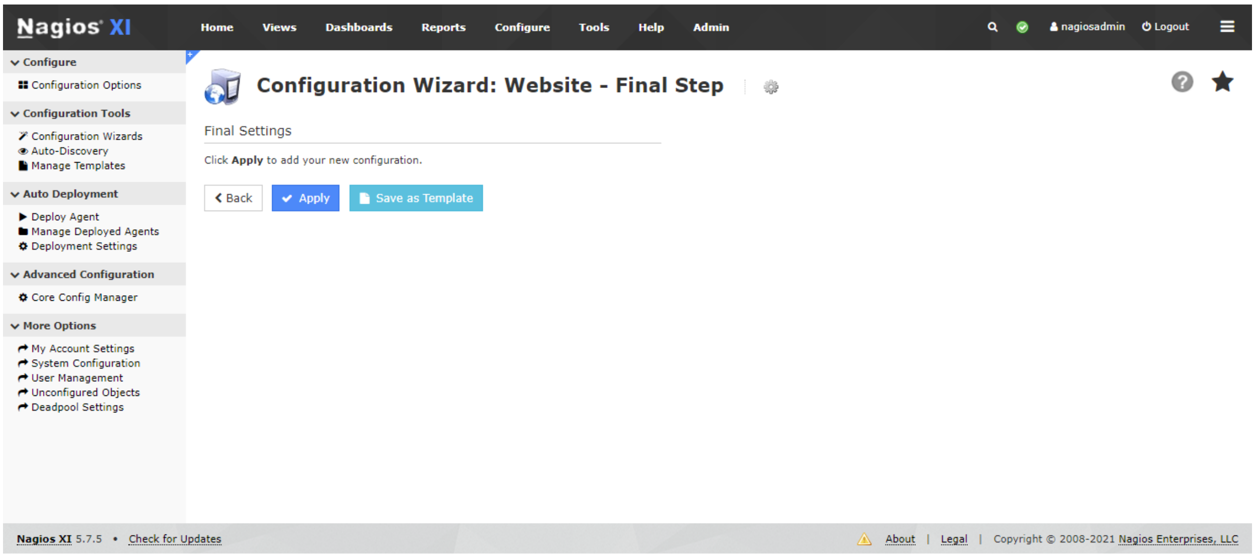
Parent Host

Define which host(s) are considered the parents of the the monitored host (if any).
Note: Typically only one (1) host is specified as a parent.

□ 27.147.194.136 (27.147.194.136)
□ localhost (127.0.0.1)

< Back
Next >
✓ Finish
Nagios XI 5.7.5 • Check for Updates
About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Web site monitor, Step 5,

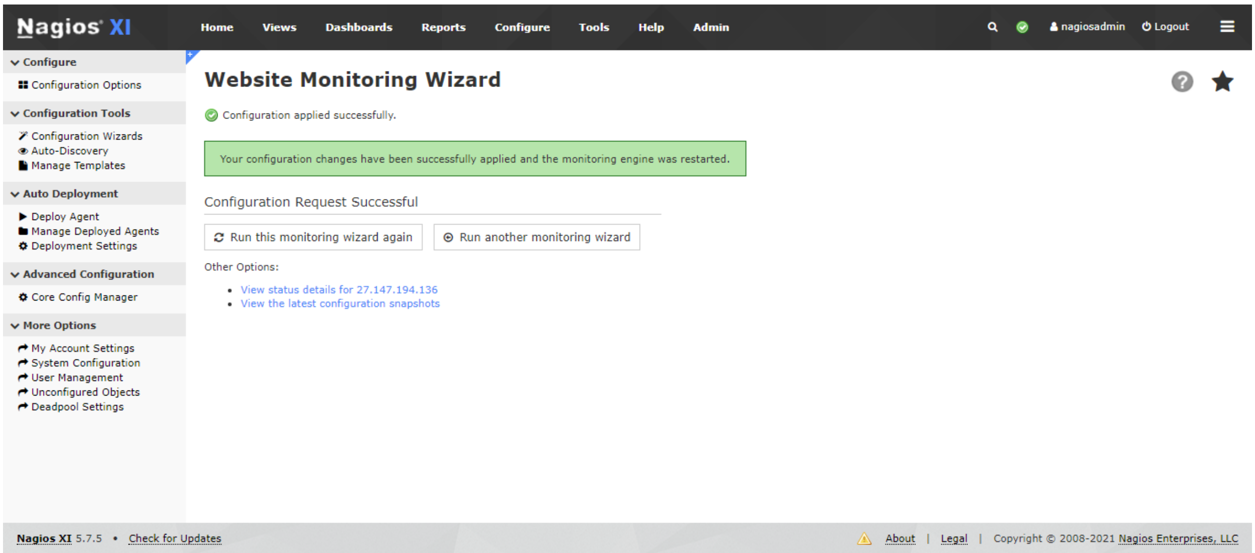


Configuration Wizard: Website - Final Step

Final Settings

Click **Apply** to add your new configuration.

Web site monitor, Step 6,



Website Monitoring Wizard

Configuration applied successfully.

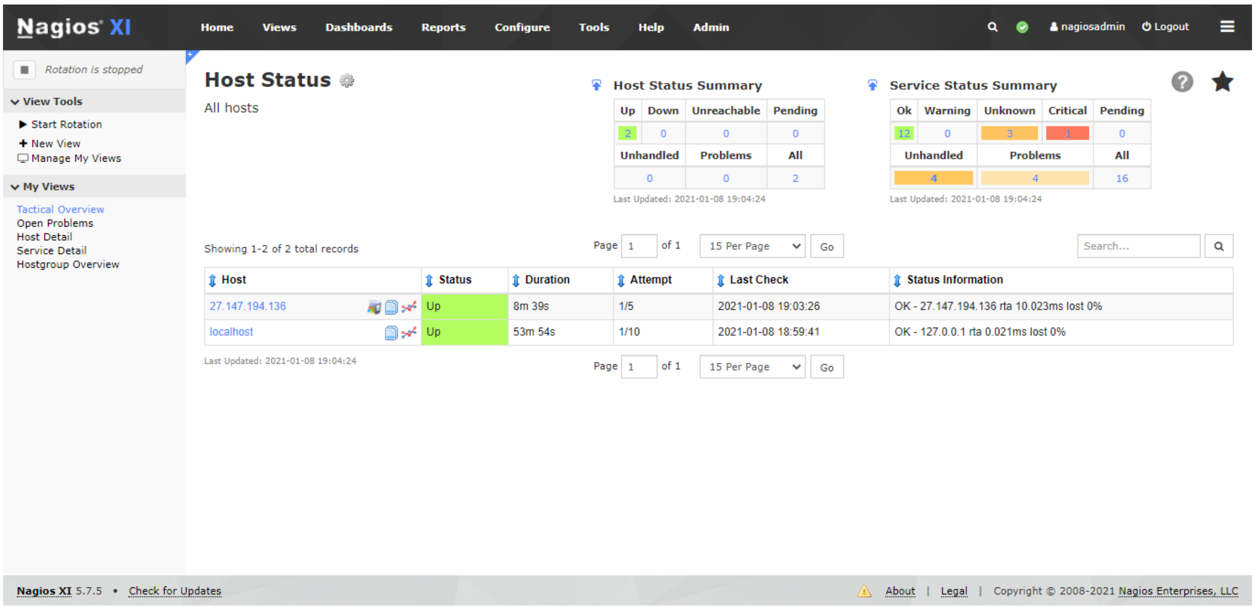
Your configuration changes have been successfully applied and the monitoring engine was restarted.

Configuration Request Successful

Other Options:

- View status details for 27.147.194.136
- View the latest configuration snapshots

Then Views, Host Detail



Host Status

All hosts

Host Status Summary

Up	Down	Unreachable	Pending
2	0	0	0
Unhandled	**Problems**	**All**	
0	0	2	

Last Updated: 2021-01-08 19:04:24

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
12	0	3	1	0
Unhandled	**Problems**	**All**		
4	4	16		

Last Updated: 2021-01-08 19:04:24

Showing 1-2 of 2 total records

Page 1 of 1 15 Per Page Go

Search...

Host	Status	Duration	Attempt	Last Check	Status Information
27.147.194.136	Up	8m 39s	1/5	2021-01-08 19:03:26	OK - 27.147.194.136 rta 10.023ms lost 0%
localhost	Up	53m 54s	1/10	2021-01-08 18:59:41	OK - 127.0.0.1 rta 0.021ms lost 0%

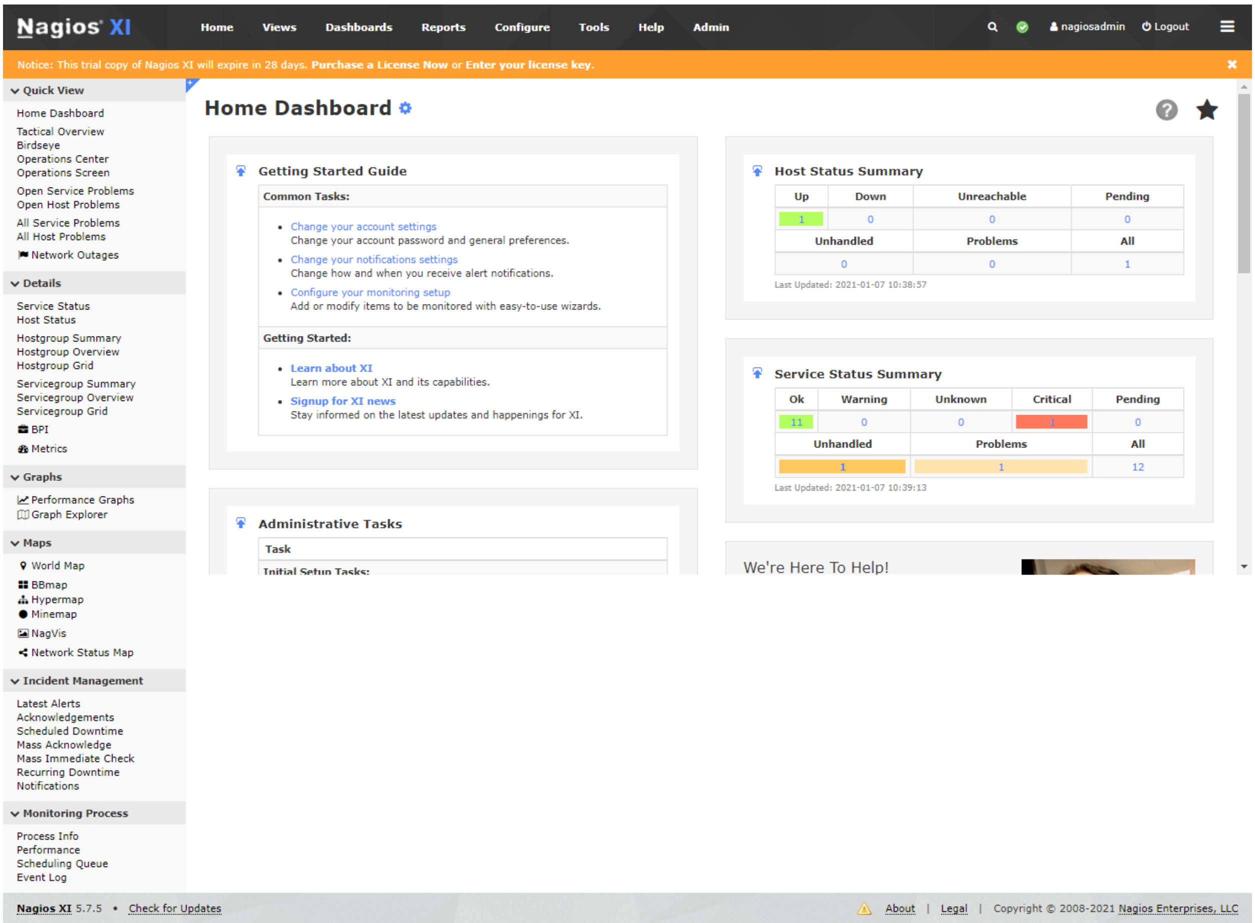
Last Updated: 2021-01-08 19:04:24

Page 1 of 1 15 Per Page Go

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Home,



Notice: This trial copy of Nagios XI will expire in 28 days. **Purchase a License Now** or **Enter your license key.**

Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- **Learn about XI**
  Learn more about XI and its capabilities.
- **Signup for XI news**
  Stay informed on the latest updates and happenings for XI.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0
Unhandled	**Problems**	**All**	
0	0	1	

Last Updated: 2021-01-07 10:38:57

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	0	0	1	0
Unhandled	**Problems**	**All**		
1	1	12		

Last Updated: 2021-01-07 10:39:13

Administrative Tasks

Task

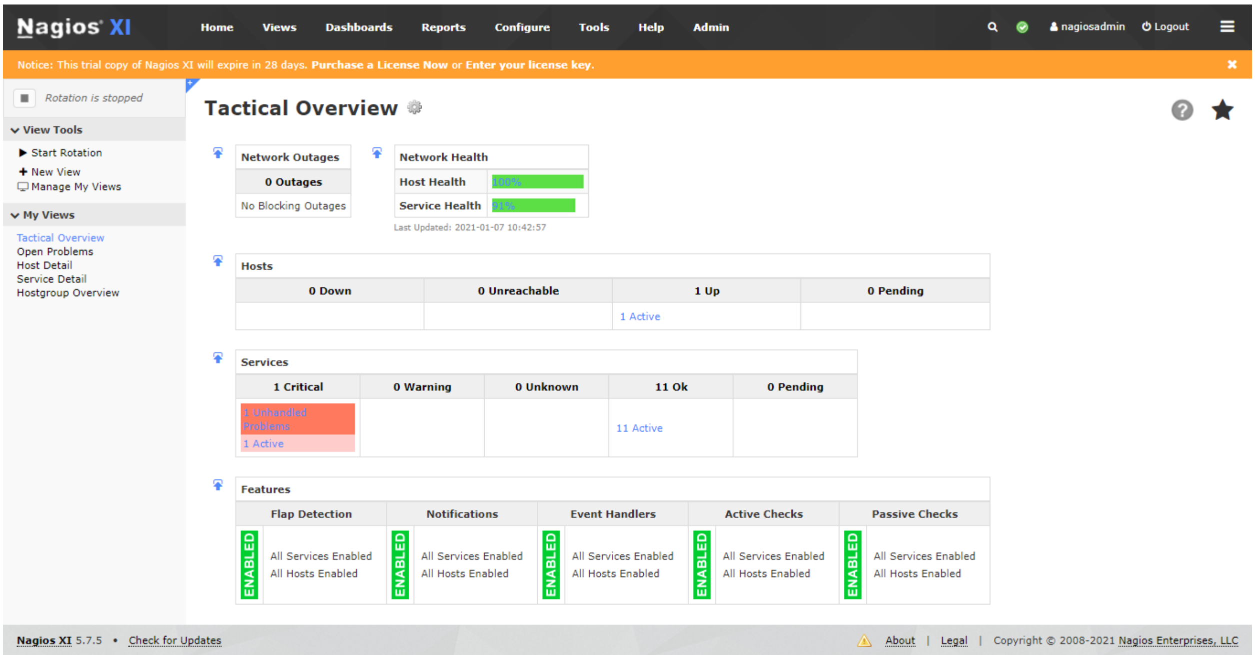
Initial Setup Tasks:

We're Here To Help!

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Views,



Notice: This trial copy of Nagios XI will expire in 28 days. **Purchase a License Now** or **Enter your license key.**

Tactical Overview

Network Outages
0 Outages
No Blocking Outages

Network Health	
Host Health	100%
Service Health	91%

Last Updated: 2021-01-07 10:42:57

Hosts

0 Down	0 Unreachable	1 Up	0 Pending
		1 Active	

Services

1 Critical	0 Warning	0 Unknown	11 Ok	0 Pending
1 Unhandled Problems 1 Active			11 Active	

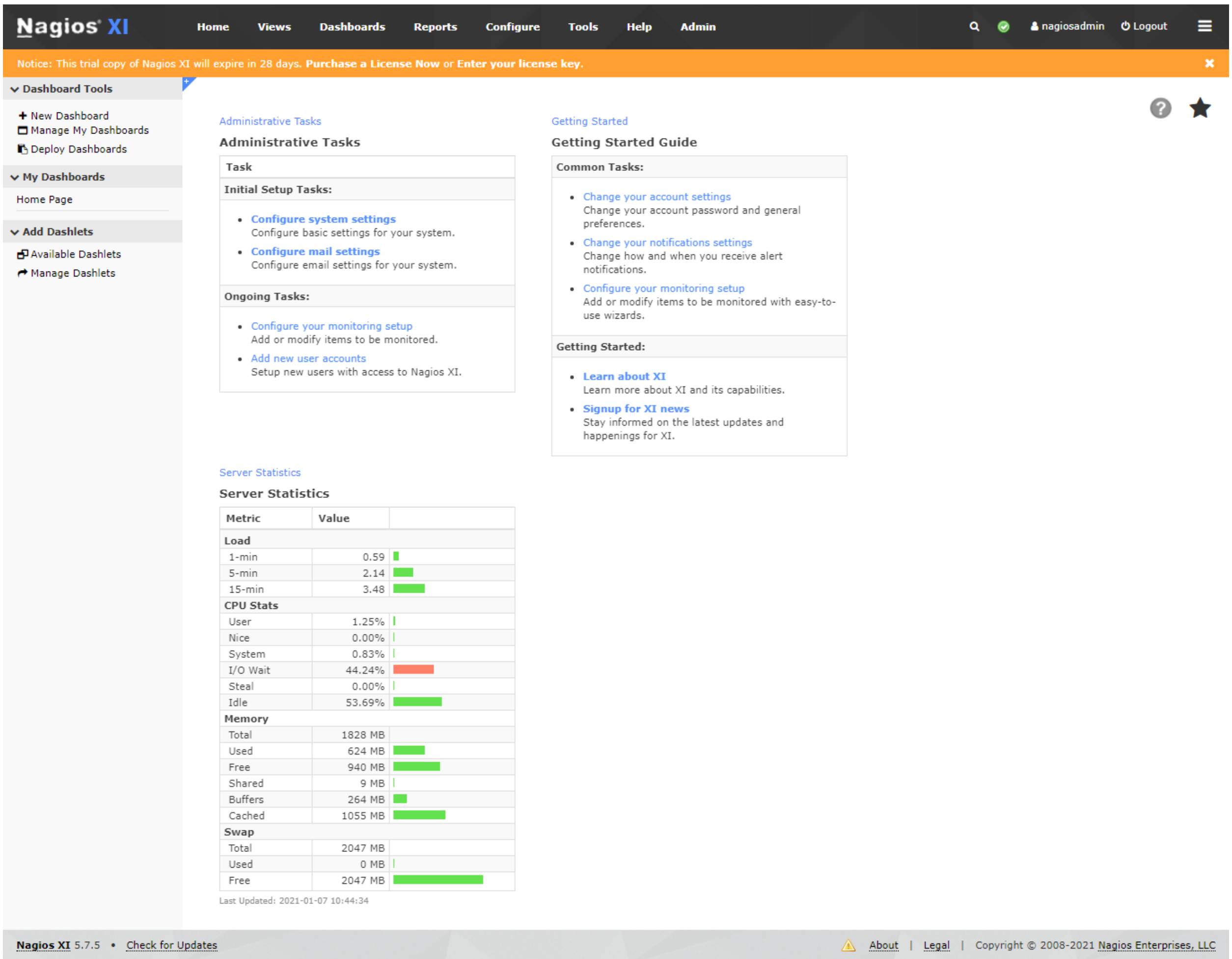
Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
ENABLED All Services Enabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Dashboards,



Notice: This trial copy of Nagios XI will expire in 28 days. **Purchase a License Now** or **Enter your license key.**

Administrative Tasks

Administrative Tasks

Task

Initial Setup Tasks:

- **Configure system settings**
  Configure basic settings for your system.
- **Configure mail settings**
  Configure email settings for your system.

Ongoing Tasks:

- Configure your monitoring setup
  Add or modify items to be monitored.
- Add new user accounts
  Setup new users with access to Nagios XI.

Getting Started

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- **Learn about XI**
  Learn more about XI and its capabilities.
- **Signup for XI news**
  Stay informed on the latest updates and happenings for XI.

Server Statistics

Server Statistics

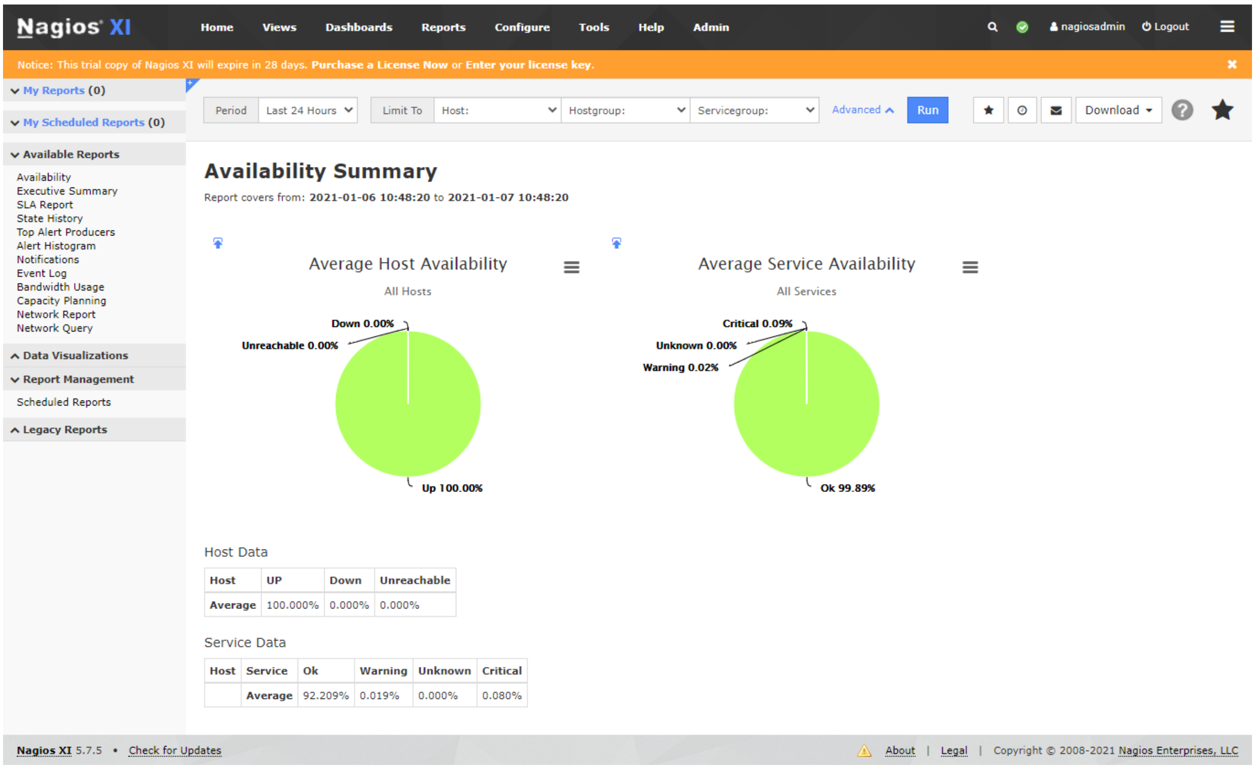
Metric	Value	
Load		
1-min	0.59	🟩
5-min	2.14	🟩
15-min	3.48	🟩
CPU Stats		
User	1.25%	🟩
Nice	0.00%	🟩
System	0.83%	🟩
I/O Wait	44.24%	🟥
Steal	0.00%	🟩
Idle	53.69%	🟩
Memory		
Total	1828 MB	
Used	624 MB	🟩
Free	940 MB	🟩
Shared	9 MB	🟩
Buffers	264 MB	🟩
Cached	1055 MB	🟩
Swap		
Total	2047 MB	
Used	0 MB	🟩
Free	2047 MB	🟩

Last Updated: 2021-01-07 10:44:34

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Reports:



Notice: This trial copy of Nagios XI will expire in 28 days. **Purchase a License Now** or **Enter your license key.**

Period: Last 24 Hours | Limit To Host: | Hostgroup: | Servicegroup:

Availability Summary

Report covers from: **2021-01-06 10:48:20** to **2021-01-07 10:48:20**

Host Data

Host	UP	Down	Unreachable
Average	100.000%	0.000%	0.000%

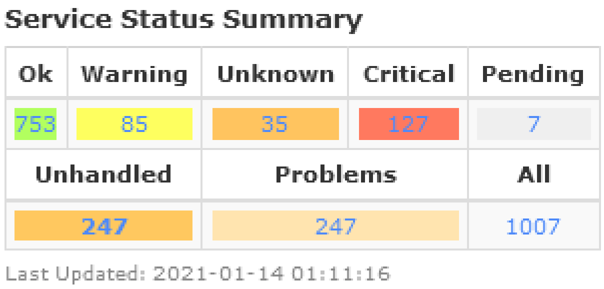
Service Data

Host	Service	Ok	Warning	Unknown	Critical
	Average	92.209%	0.019%	0.000%	0.080%

Nagios XI 5.7.5 • Check for Updates

About | Legal | Copyright © 2008-2021 Nagios Enterprises, LLC

Service Status Summary

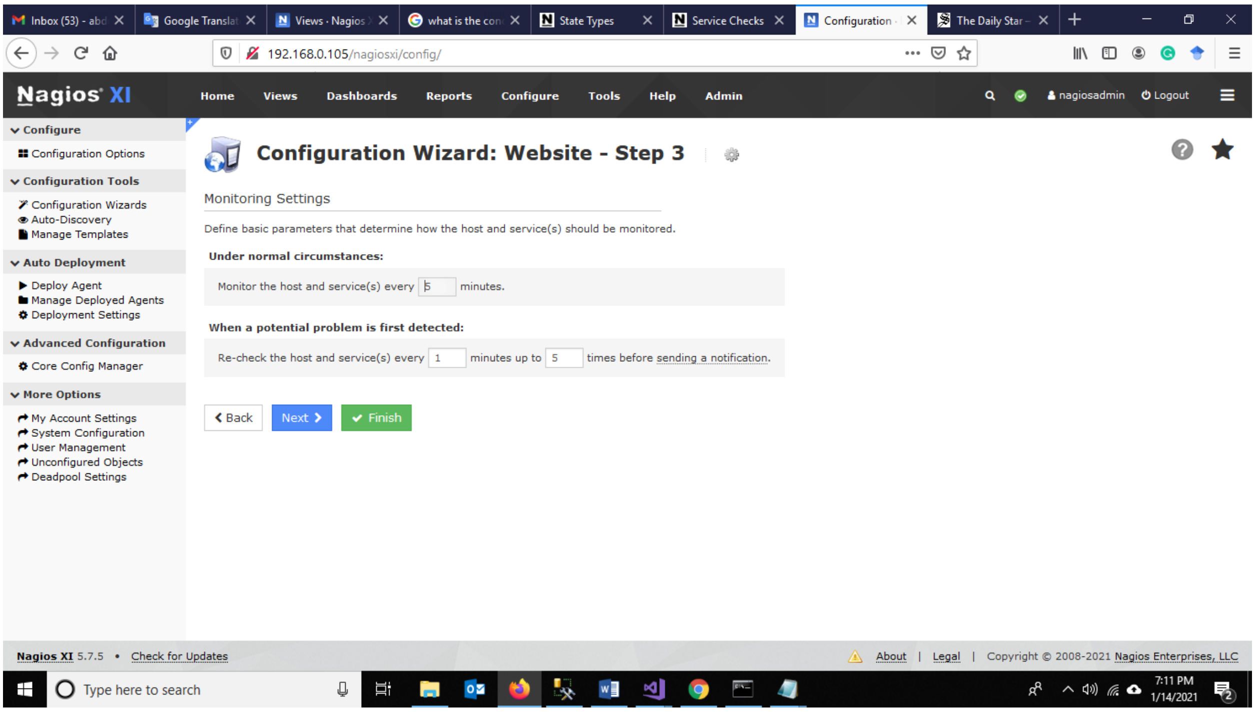


Service Status Summary

Ok	Warning	Unknown	Critical	Pending
753	85	35	127	7

Unhandled	Problems	All
247	247	1007

Last Updated: 2021-01-14 01:11:16



Configuration Wizard: Website - Step 3

Monitoring Settings

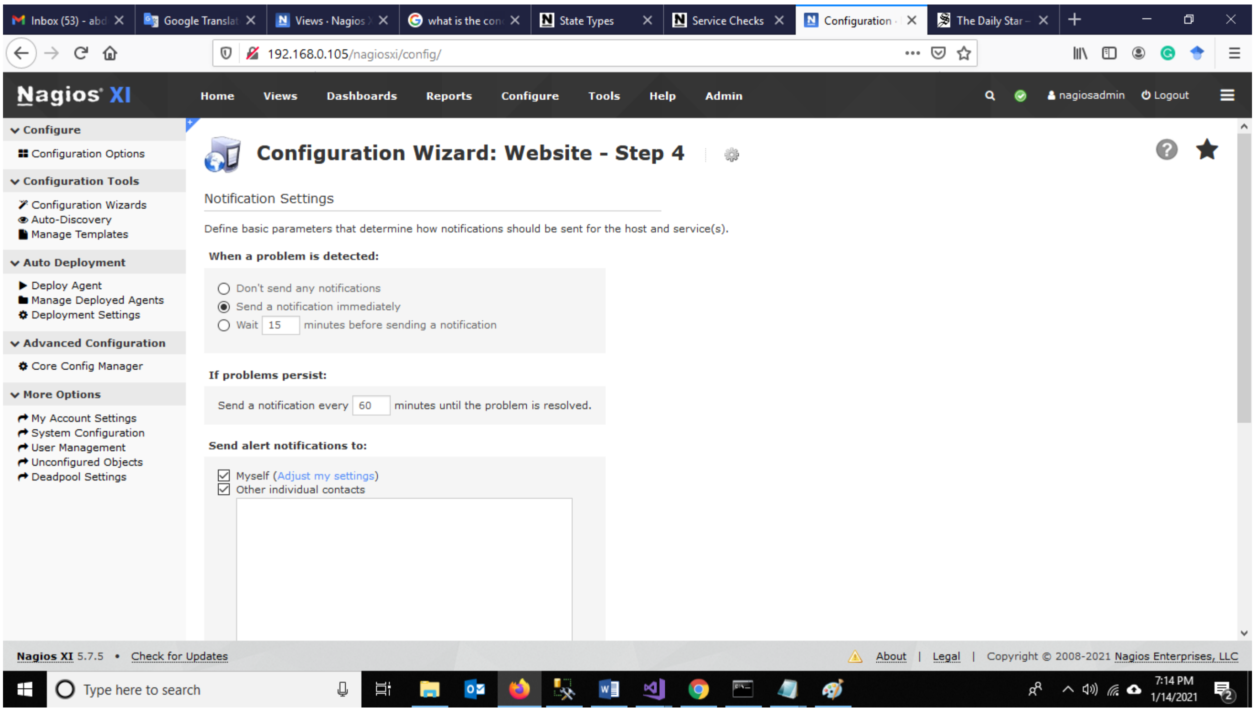
Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:

Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.



Configuration Wizard: Website - Step 4

Notification Settings

Define basic parameters that determine how notifications should be sent for the host and service(s).

When a problem is detected:

○ Don't send any notifications
● Send a notification immediately
○ Wait 15 minutes before sending a notification

If problems persist:

Send a notification every 60 minutes until the problem is resolved.

Send alert notifications to:

☑ Myself (Adjust my settings)
☑ Other individual contacts

State Types

https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/statetypes.html

https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/servicechecks.html

Pros and Cons

Pros

- Nagios is open source software. It's free to use and edit.
- It has an open configuration which is easy to add a custom scripts to extend the services available.
- There're many devices which the Nagios system can monitor. The requirement is an SNMP protocol on that device.
- Alert, notification or comment the status of the system. It has varieties of alert tools.
- It has many plugins and add-ons which are free to download and develop.

  (https://www.nagios.com/news/2020/08/benefits-of-network-monitoring/)

Cons

- Many features are not available on a free version of Nagios. Features such as wizards or interactive dashboard are available on Nagios XI, which is very expensive.
- There're many configuration files which are very hard to configure.
- Nagios core has a confusing interface.
- Nagios can't monitor network throughput (bandwidth uses or available).
- Nagios can't manage the network, just monitor the network.
- Nagios makes no distinction among different types of devices like servers, routers, or switches.
- Nagios treats every device generically as a host.

Notes:

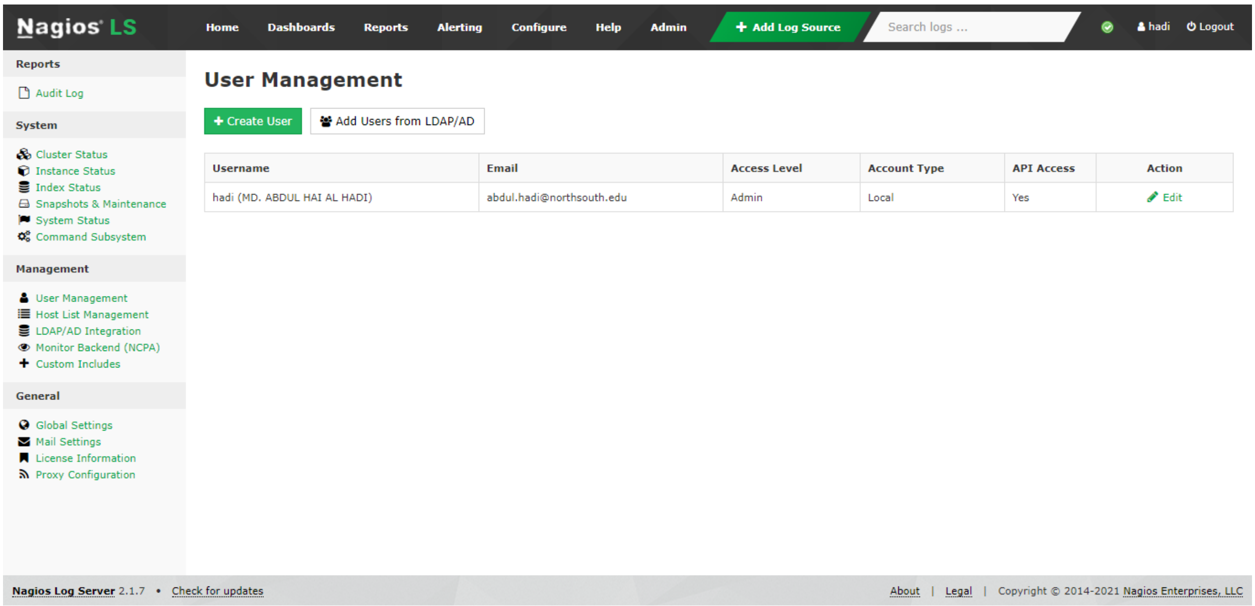
1. **The main tasks of Nagios are to monitor status of network devices and their services and to notify system administrators of network problems.**
2. Nagios perform status check and notify a problem through the use of external "plugins", which are compiled executables or scripts (Perl, shell, etc.)
3. The core of Nagios engine is a scheduler daemon that regularly executes plugins to probe specified network devices and their services

How we use and understand Nagios Log Server?

Nagios Log Server facilitates the ability to search all entries of logs in a quick and easy way. Beyond that, it has allowed us to configure alerts for notification when there are potential threats (may they be security threats or only application-side problems), and to filter the data for audits and compliance.

Admin:

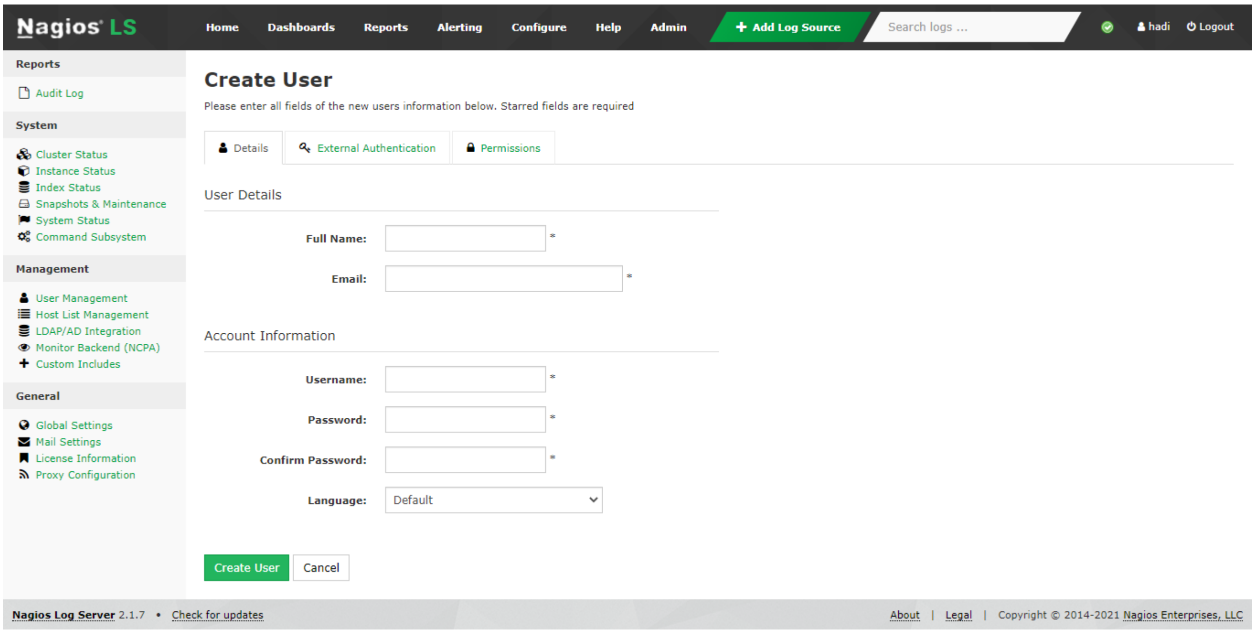
User management,



User Management

Username	Email	Access Level	Account Type	API Access	Action
hadi (MD. ABDUL HAI AL HADI)	abdul.hadi@northsouth.edu	Admin	Local	Yes	Edit

Create User



Create User

Please enter all fields of the new users information below. Starred fields are required

User Details

Full Name: *

Email: *

Account Information

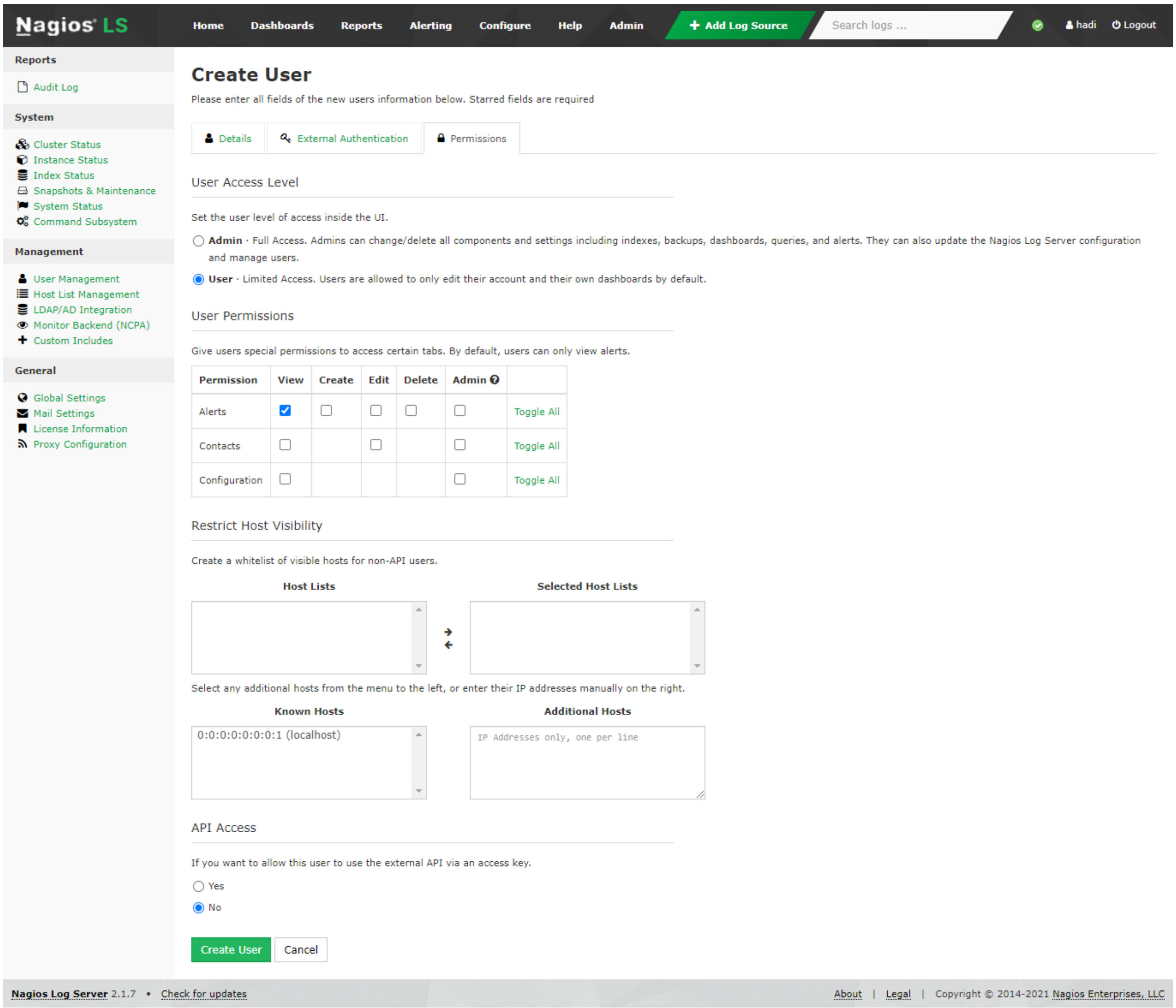
Username: *

Password: *

Confirm Password: *

Language: Default

User Permissions



Create User

Please enter all fields of the new users information below. Starred fields are required

User Access Level

Set the user level of access inside the UI.

○ **Admin** · Full Access. Admins can change/delete all components and settings including indexes, backups, dashboards, queries, and alerts. They can also update the Nagios Log Server configuration and manage users.

● **User** · Limited Access. Users are allowed to only edit their account and their own dashboards by default.

User Permissions

Give users special permissions to access certain tabs. By default, users can only view alerts.

Permission	View	Create	Edit	Delete	Admin	
Alerts	☑	□	□	□	□	Toggle All
Contacts	□		□		□	Toggle All
Configuration	□				□	Toggle All

Restrict Host Visibility

Create a whitelist of visible hosts for non-API users.

Host Lists

Selected Host Lists

Select any additional hosts from the menu to the left, or enter their IP addresses manually on the right.

Known Hosts

0:0:0:0:0:0:0:1 (localhost)

Additional Hosts

IP Addresses only, one per line

API Access

If you want to allow this user to use the external API via an access key.

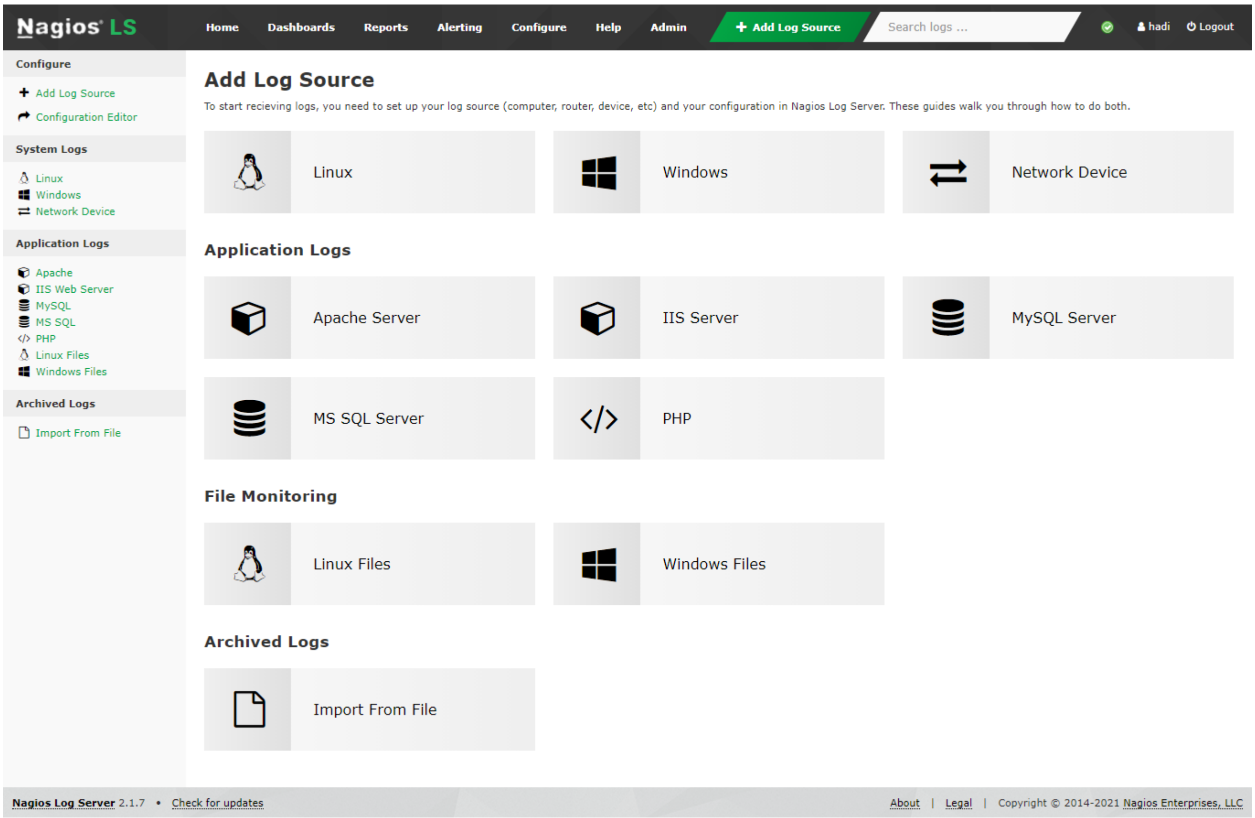
○ Yes

● No

Nagios Log Server 2.1.7 • Check for updates

About | Legal | Copyright © 2014-2021 Nagios Enterprises, LLC

Configuring devices and applications

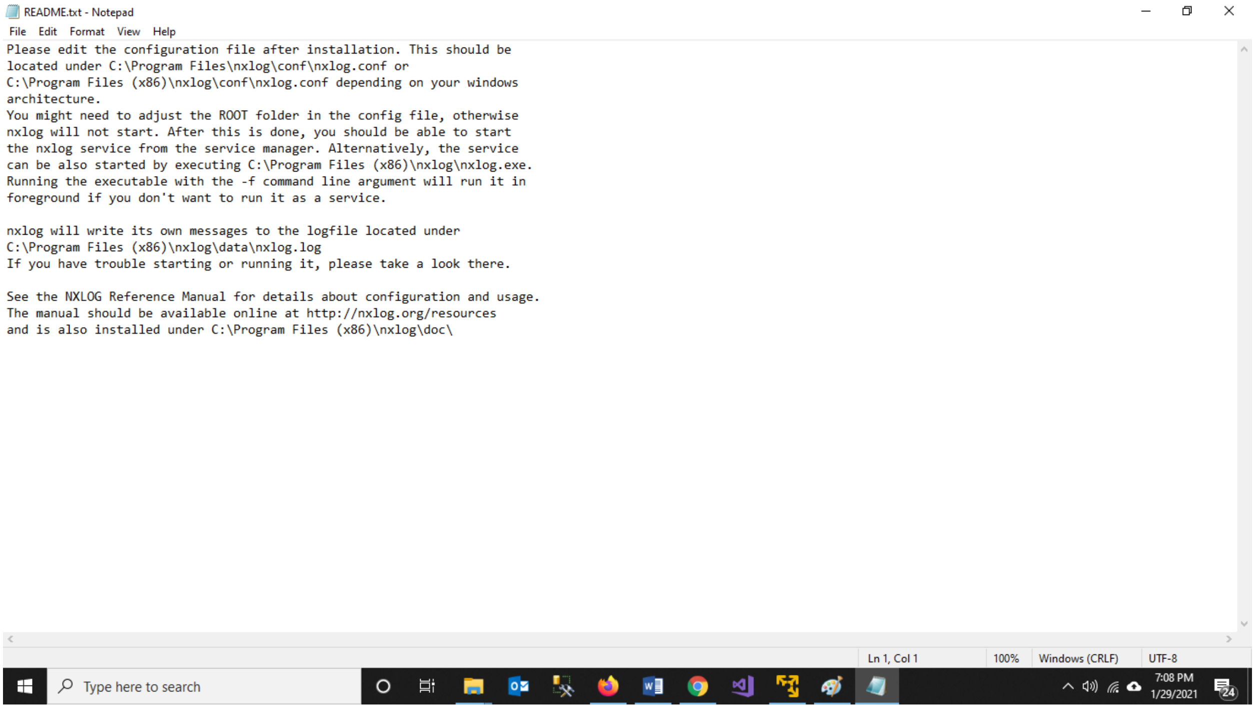


To start recieving logs, you need to set up your log source (computer, router, device, etc) and your configuration in Nagios Log Server. These guides walk you through how to do both.

Windows:

Download agent

Get started by downloading NXLog CE and install it on the Windows desktop or server you want to receive logs from.



```
Please edit the configuration file after installation. This should be
located under C:\Program Files\nxlog\conf\nxlog.conf or
C:\Program Files (x86)\nxlog\conf\nxlog.conf depending on your windows
architecture.
You might need to adjust the ROOT folder in the config file, otherwise
nxlog will not start. After this is done, you should be able to start
the nxlog service from the service manager. Alternatively, the service
can be also started by executing C:\Program Files (x86)\nxlog\nxlog.exe.
Running the executable with the -f command line argument will run it in
foreground if you don't want to run it as a service.

nxlog will write its own messages to the logfile located under
C:\Program Files (x86)\nxlog\data\nxlog.log
If you have trouble starting or running it, please take a look there.

See the NXLOG Reference Manual for details about configuration and usage.
The manual should be available online at http://nxlog.org/resources
and is also installed under C:\Program Files (x86)\nxlog\doc\
```

Notes:

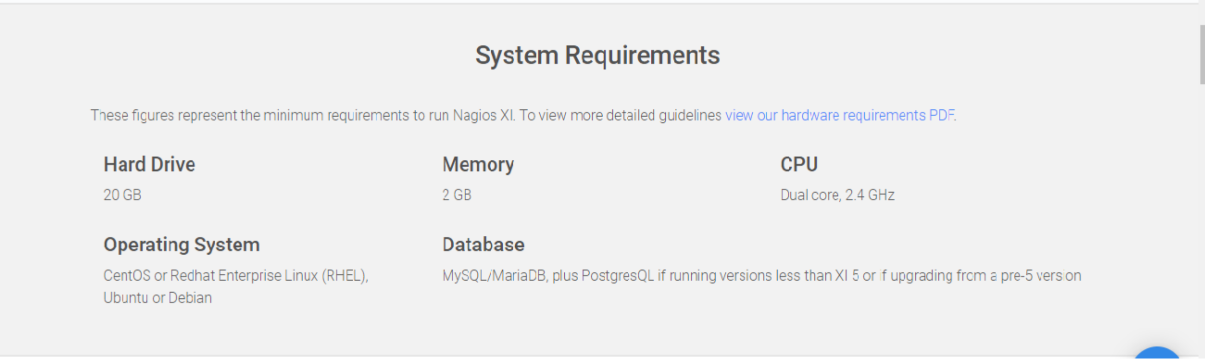
1. Nagios Log Server provides centralized log management, monitoring and analysis software.

Best Network Monitoring Software

The best Network Monitoring Software vendors are Zabbix, PRTG Network Monitor, SolarWinds NPM, LogicMonitor, and NETSCOUT nGeniusONE. Zabbix is the top solution according to IT Central Station reviews and rankings. One reviewer writes: "A free enterprise monitoring solution ", and another reviewer writes: "Reasonable network monitoring which works okay if you don't mind the glitches". The 2nd best product is PRTG Network Monitor. A user writes: "The product makes it easier for us to find and identify problems", and another reviewer writes: "We can see as soon as there is a problem and track it down pretty quickly".

Summary

- Continuous monitoring is a process to detect, report, respond all the attacks which occur in its infrastructure.
- Nagios is free to use open source software tool for continuous monitoring
- Nagios offers effective monitoring of entire infrastructure and business processes.
- Ethan Galstad uses the ideas and architecture of his earlier work to begin building a new application Nagios which runs under Linux OS.
- Nagios is relatively scalable, Manageable, and Secure.
- Three important components of Nagios architecture are
  1) Web Interface (GUI)
  2) Nagios Server
  3) Plugin
- Nagios allows application monitoring from a single console with transaction-level insights
- This tool not allows us to manage the network but only allows to monitor the network.



System Requirements

These figures represent the minimum requirements to run Nagios XI. To view more detailed guidelines view our hardware requirements PDF.

Hard Drive	Memory	CPU
20 GB	2 GB	Dual core, 2.4 GHz

Operating System

CentOS or Redhat Enterprise Linux (RHEL), Ubuntu or Debian

Database

MySQL/MariaDB, plus PostgresQL if running versions less than XI 5 or if upgrading from a pre-5 version