Exercise – Nagios

Objective

The objective of this exercise is to install **Nagios XI** on **a Red Hat** machine running in aws and have a look at the dashboard options. We are then going to create two servers, one running **Ubuntu** and one **Windows Server 2016** to monitor.

Outline

You will need to start a new **Red Hat** machine in AWS with the following properties:

- Operating System: Red Hat Enterprise
- Size: t2.medium
- Tag: NagiosXI
- Security Group: Open up 80/tcp, 443/tcp and Echo Request/ICMP

The default username for RedHat is "**ec2-user**".

When accessing the **Nagios** dashboard please make sure to use **Firefox** or **Chrome** as there is a bug with some versions of **Internet Explorer** which means that page does not show.

Installing NagiosXI

Connect to your machine via **SSH**. The default username for **Red Hat** is **ec2-user**.

Run the following:

```
#!/bin/bash
sudo yum update -y
sudo yum install -y epel-release wget


sudo yum-config-manager --enable rhui-REGION-rhel-server-extras
rhui-REGION-rhel-server-optional


cd /tmp
wget http://assets.nagios.com/downloads/nagiosxi/xi-
latest.tar.gz
tar xzf xi-latest.tar.gz


cd /tmp/nagiosxi
sudo touch installed.firewall
# comment lin 80 in “0-repos“ file
yes | sudo ./fullinstall
```

The “touch installed.firewall” line creates a new file which tells the installer not to bother with the firewall step in the installation. The version of Red Hat in AWS doesn’t require this step.

You should now be able to point a browser at **[public ip]/nagiosxi** to complete the install (remember to note the password given or that you chose) and see the dashboard. The terminal output will use the internal IP of the machine, so make sure you look up the correct value.

Take the tour around the dashboard and see what is available!

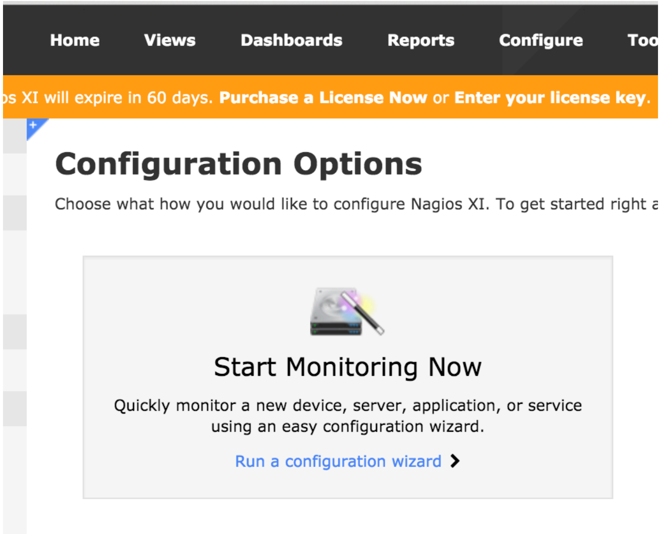
Creating the agents

You will need to then create two additional machines via the AWS console.

- **Linux Machine**
  - Operating system: Ubuntu
  - Size: t2 micro
  - Tag: LinuxHost
  - Security group: Echo Request/ICMP and 5666/tcp from anywhere (although you could specify only from the IP address of the NagiosXI machine in production)
- **Windows Machine**
  - Operating System: Windows Server 2016
  - Size: t2.medium
  - Tag: WindowsHost
  - Security group: Echo Request/ICMP and 12489/tcp from anywhere (although you could specify only from the IP address of the NagiosXI machine)

Monitoring Linux

On your **Nagios master**, click on the "**Configure**" link at the top of the screen, then select "**Start Monitoring Now**".



os XI will expire in 60 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 a

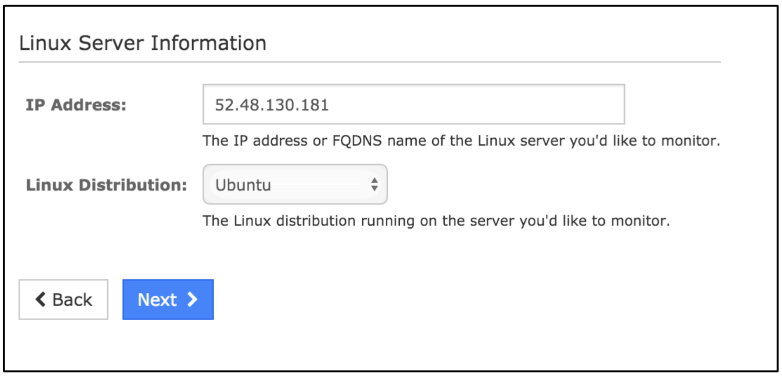
Start Monitoring Now

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

Run a configuration wizard ›

Search for "**Linux Server**" and click on that option.

On the next screen put the **LinuxHost** machine’s IP address and select **Ubuntu** from the distribution menu and then click Next.



Linux Server Information

IP Address: 52.48.130.181

The IP address or FQDNS name of the Linux server you'd like to monitor.

Linux Distribution: Ubuntu

The Linux distribution running on the server you'd like to monitor.

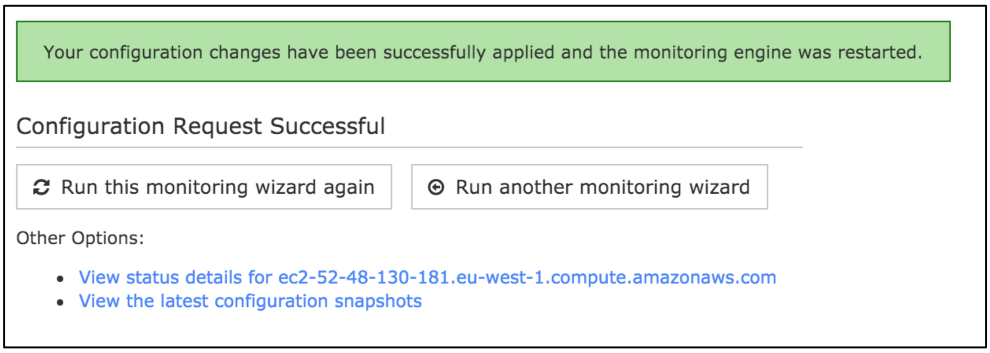
On the next screen are instructions for how to install the agent on the Ubuntu machine. Open the ***Agent Installation Instructions*** link in a new tab and follow the guidelines there. (remember that the default username for connecting to Ubuntu machines is **ubuntu**, not ec2-user).

Connect to your **LinuxHost** machine and install Agent. As well you will need to give the **IP address of the NagiosXI master**:

```
      Allow from:  [public Nagios Master IP address]
```

On the **NagiosXI** dashboard click “**Next**” and then “**Finish**” to start monitoring.

You can see your server directly from the link given on the summary page:



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

Configuration Request Successful

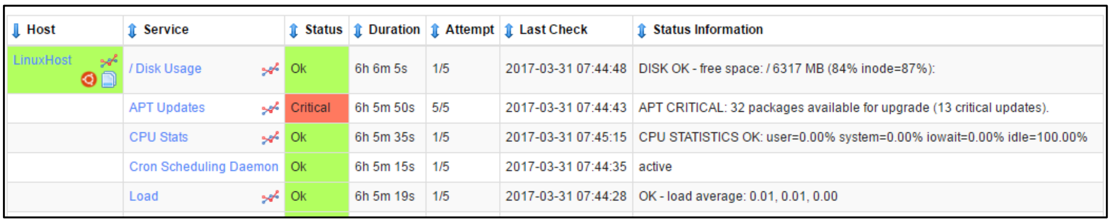
Run this monitoring wizard again
Run another monitoring wizard

Other Options:

- View status details for ec2-52-48-130-181.eu-west-1.compute.amazonaws.com
- View the latest configuration snapshots

To start with the checks may come in critical or unknown. If they continue to stay in a red state, check that you have **port 5666 open on the agent**.

Update and upgrade your **LinuxHost** if you get problem shown below:



Host	Service	Status	Duration	Attempt	Last Check	Status Information
LinuxHost	/ Disk Usage	Ok	6h 6m 5s	1/5	2017-03-31 07:44:48	DISK OK - free space: / 6317 MB (84% inode=87%):
	APT Updates	Critical	6h 5m 50s	5/5	2017-03-31 07:44:43	APT CRITICAL: 32 packages available for upgrade (13 critical updates).
	CPU Stats	Ok	6h 5m 35s	1/5	2017-03-31 07:45:15	CPU STATISTICS OK: user=0.00% system=0.00% iowait=0.00% idle=100.00%
	Cron Scheduling Daemon	Ok	6h 5m 15s	1/5	2017-03-31 07:44:35	active
	Load	Ok	6h 5m 19s	1/5	2017-03-31 07:44:28	OK - load average: 0.01, 0.01, 0.00

Monitoring Windows machines

This starts the same way. Go to the “**Configure Menu**” and click “**Start Monitoring Now**” then search for “**Windows**”.

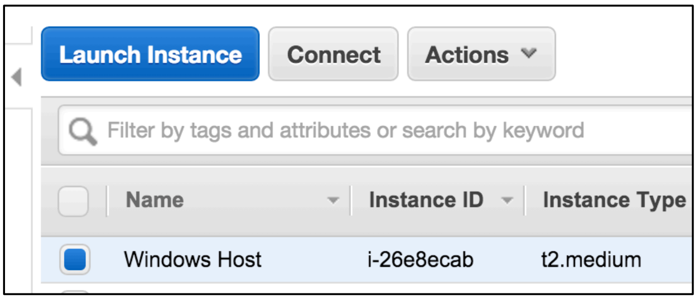
Select “**Windows Server**”

Put in the **IP address** for your **WindowsHost**.

The instructions for this involve installing something on Windows. To do this we will need to connect to the Windows machine.

Connecting to Windows Machines using RDP in AWS

Go to the aws dashboard and select your Windows Host. Click the Connect button at the top.



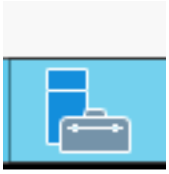
☐	Name	Instance ID	Instance Type
■	Windows Host	i-26e8ecab	t2.medium

Click to download the remote desktop file. You will then need to decrypt the admin password. You do this via the .pem file (NOT the ppk) for the server. Click the “**Get Password**” button and follow the instructions to decrypt the password.

Open the remote desktop file. If you are on a Mac then you will need to install the **Microsoft Remote Desktop** tool. Windows machines should have it already installed.

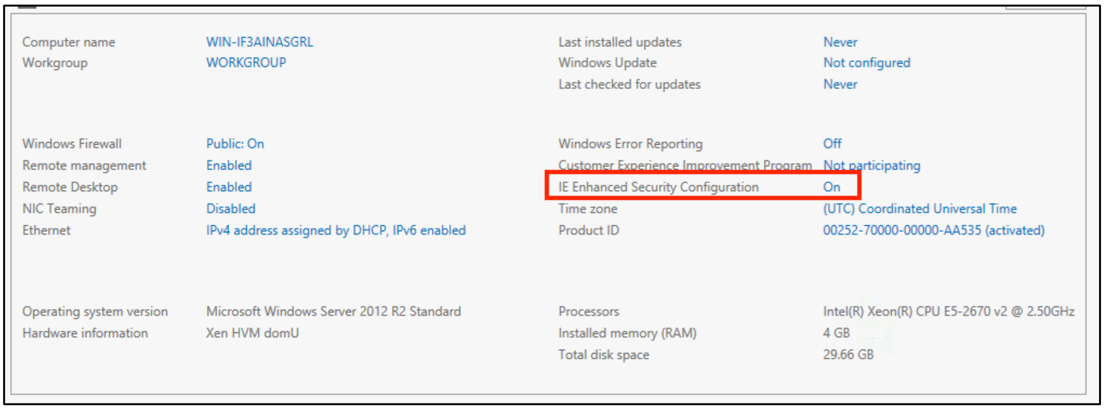
Wait for the machine to log in and you will have your own Windows Server.

On the windows machine click the “**Server Options**”/”**Server Manager**” button



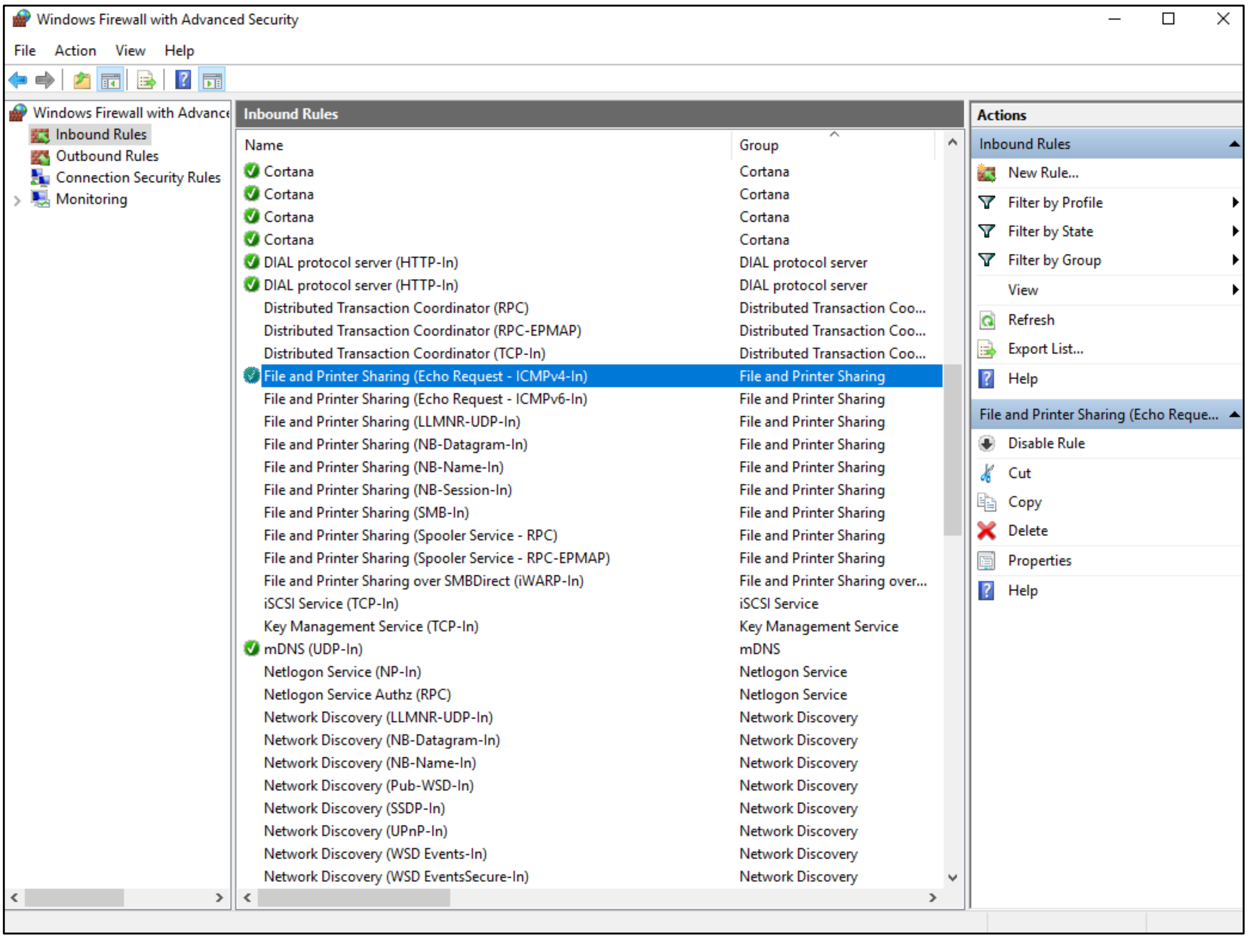
Click the “**Local Server**” box.

Turn “**IE Enhanced Security Configuration**” off by clicking on the word “on”. You want to turn it off for both administrators and users.



Computer name	WIN-IF3AINASGRL	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Public: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-70000-00000-AA535 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors	Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz
Hardware information	Xen HVM domU	Installed memory (RAM)	4 GB
		Total disk space	29.66 GB

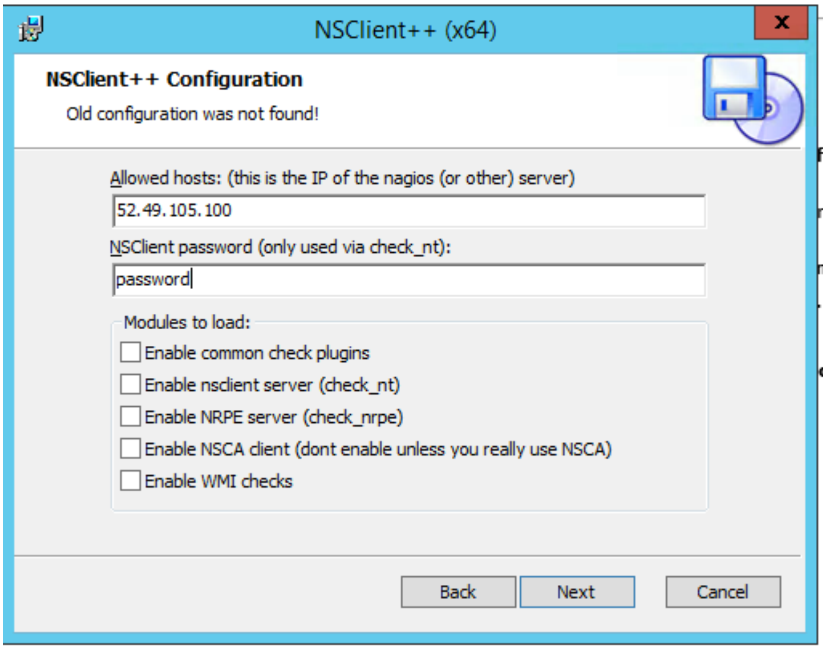
Turn on "**File and Printer Sharing (Echo request – ICMPv4-In)**" in **Windows Firewall with Advanced Security**.



Name	Group
✓ Cortana	Cortana
✓ Cortana	Cortana
✓ Cortana	Cortana
✓ Cortana	Cortana
✓ DIAL protocol server (HTTP-In)	DIAL protocol server
✓ DIAL protocol server (HTTP-In)	DIAL protocol server
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing
File and Printer Sharing (NB-Name-In)	File and Printer Sharing
File and Printer Sharing (NB-Session-In)	File and Printer Sharing
File and Printer Sharing (SMB-In)	File and Printer Sharing
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...
iSCSI Service (TCP-In)	iSCSI Service
Key Management Service (TCP-In)	Key Management Service
✓ mDNS (UDP-In)	mDNS
Netlogon Service (NP-In)	Netlogon Service
Netlogon Service Authz (RPC)	Netlogon Service
Network Discovery (LLMNR-UDP-In)	Network Discovery
Network Discovery (NB-Datagram-In)	Network Discovery
Network Discovery (NB-Name-In)	Network Discovery
Network Discovery (Pub-WSD-In)	Network Discovery
Network Discovery (SSDP-In)	Network Discovery
Network Discovery (UPnP-In)	Network Discovery
Network Discovery (WSD Events-In)	Network Discovery
Network Discovery (WSD EventsSecure-In)	Network Discovery

Now we can download the Nagios plugin installer. Go to the start menu and start up Internet Explorer. The link we need was on the NagiosXI dashboard, so go back to that and right click "**Download vx.x.x (64 bit)**" and select "**Copy Link Address**"

Go back to the windows server and paste in the address to download the install file. Run the installer giving it the IP address of your NagiosXI machine and a password.



NSClient++ Configuration

Old configuration was not found!

Allowed hosts: (this is the IP of the nagios (or other) server)

52.49.105.100

NSClient password (only used via check_nt):

password

Modules to load:

☐ Enable common check plugins
☐ Enable nsclient server (check_nt)
☐ Enable NRPE server (check_nrpe)
☐ Enable NSCA client (dont enable unless you really use NSCA)
☐ Enable WMI checks

Click “**Start service**” at the end of the installation.

Configuring NSClient++ 0.4.x

The configuration file in NSClient++ 0.4.x is called **nsclient.ini** and is located here: `C:\Program Files\NSClient++\`**nsclient.ini**

This document is going to show you examples of the different options available in NSClient++. The NSClient++ installer creates the **nsclient.ini** file with the minimal settings that allow NSClient++ to work *(defined by your choices during the installation)*. To use the options described in this document you will need to populate the **nsclient.ini** file with the additional options.

Open a Command Prompt as an Administrator and run the following commands:

```
cd "C:\Program Files\NSClient++"
.\nscp settings --generate --add-defaults -load-all
```

This should not produce any output, however don't be alarmed if you see some “Failed to register plugin” errors.

At this point if you open **nsclient.ini** in a text editor you will see all the available options for the modules you have enabled. **NOTE**: You will need to **restart** the NSClient++ **service** whenever you make changes (see the steps before troubleshooting section).

https://assets.nagios.com/downloads/nagiosxi/docs/Configuring-The-Windows-Agent-NSClient++-for-Nagios-XI.pdf

We now need to edit some of the configuration files. Open **c:\program files\nsclient++\nsclient.ini**

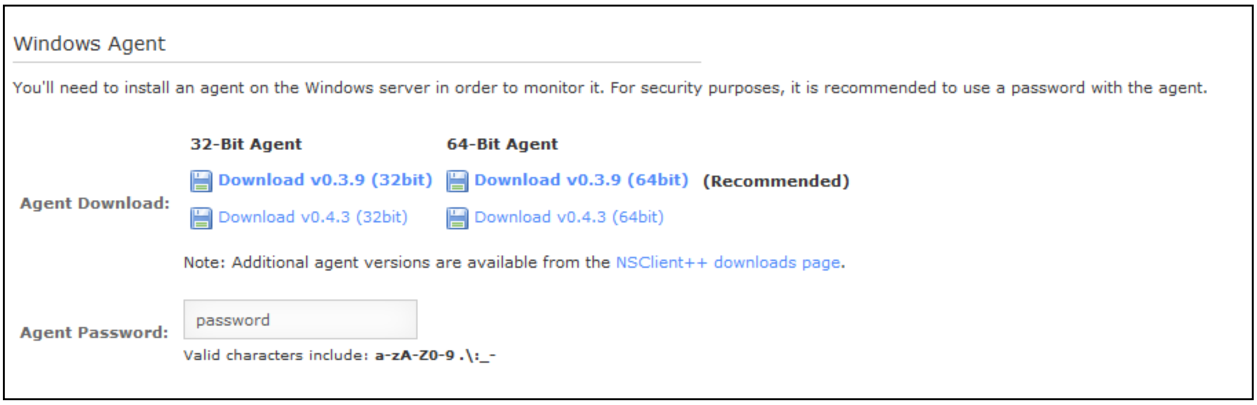
`Old Style`	`New Style`
Uncomment the following lines (by removing the ; symbol) the lines starting with:	Equal to 1 all services (change from 0 to 1): In the [/modules] section
`[modules]`	`[/modules]`

`FileLogger.dll`
`CheckSystem.dll`
`CheckDisk.dll`
`NSClientListener.dll`
`NRPEListener.dll`
`SysTray.dll`
`CheckEventLog.dll`
`CheckHelpers.dll`
`CheckWMI.dll`
`CheckNSCP.dll`
	`NRPEServer = 1`
	`NSCAClient = 1`
	`NRPEClient = 1`
	`CheckWMI = 1`
	`CheckSystem = 1`
	`CheckExternalScripts = 1`
	`CheckHelpers = 1`
	`CheckEventLog = 1`
	`CheckNSCP = 1`
	`CheckDisk = 1`
	`CheckTaskSched = 1`
	`NSClientServer = 1`
	`NRDPClient = 1`

`[NSClient]`	`; PORT NUMBER - Port to use for check_nt.`
`port=12489`	`port = 12489`
`and`	`; TIMEOUT - Timeout when reading/writing packets to/from sockets.`
`socket_timeout=30`	`timeout = 30`
`[NRPE]`	`; PORT NUMBER - Port to use for NRPE.`
`port=5666`	`port = 5666`

Save the file. Then go to the start menu and type "**services**" to bring up the service panel. Find the **NSClien**t in the list and double click it. Under the "**Log On**" tab check the "**Allow service to interact with desktop**" box, then go back to the ***General tab***. Click **Apply** and then close that window, then stop the service and start it again by right clicking the **NSClient++** service. This will reload the **config** file we edited.

Finally, go back to **NagiosXI**. Fill in the password on the **NagiosXI** configuration page and click **next** followed by finish to setup monitoring for the windows machine.



Windows Agent

You'll need to install an agent on the Windows server in order to monitor it. For security purposes, it is recommended to use a password with the agent.

	32-Bit Agent	64-Bit Agent	
Agent Download:	Download v0.3.9 (32bit)	Download v0.3.9 (64bit)	(Recommended)
	Download v0.4.3 (32bit)	Download v0.4.3 (64bit)	

Note: Additional agent versions are available from the NSClient++ downloads page.

Agent Password: password

Valid characters include: a-zA-Z0-9 .\:_-

It may take a while for Nagios to gather all the data about your windows machine (“Timeout after 10 seconds” is a common error”) but it should sort itself out over time.