

Dom Moore  
Lab Nagios

Information Security Continuous Monitoring (ISCM) systems and processes are implemented by security professionals to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. One such monitoring system is Nagios XI. An enterprise-class application capable of monitoring systems, networks, and infrastructure, Nagios XI can be a critical tool in your efforts to keep a watch over critical systems. Today you will deploy Nagios XI.

## Part 1: Staging Nagios XI Monitoring Service

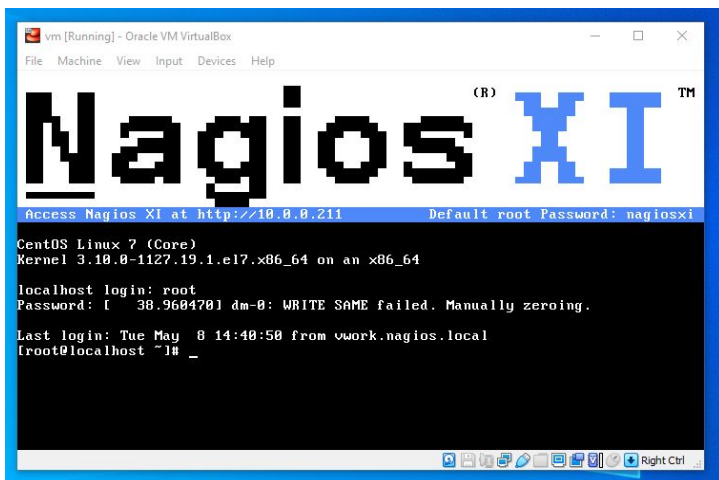
Step 1- Deploy Nagios XI to a VM in your local lab environment

Step 2- From another computer on the LAN, access Nagios XI via browser. Run setup wizard.

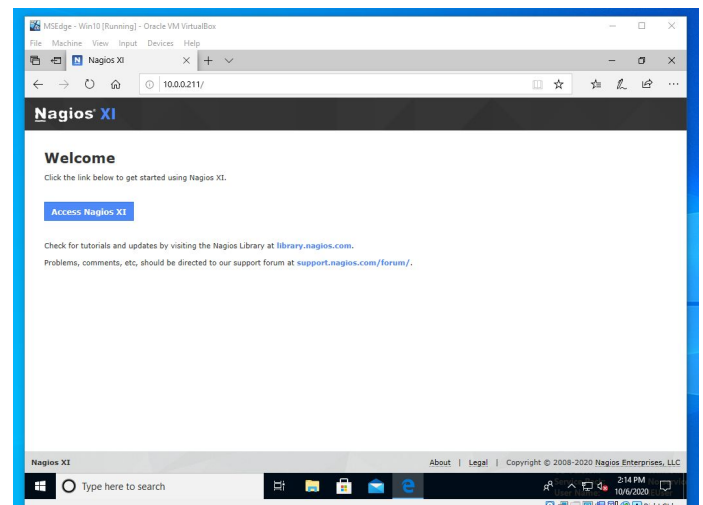
Step 3- Perform an auto-discovery job to scan all hosts on your network.

Step 4- Have Nagios monitor your Windows 7 VM and all other hosts it detects to your pool of monitored resources.

### Nagios Deployed/ Install



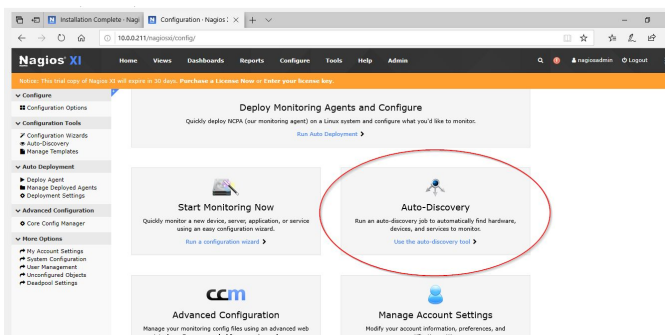
### Access Wizard from browser



## Problem Area

The next steps of the process I ran into some roadblocks, when working in the wizard for discovery of devices on my network, it did not show any devices within the network range list, to troubleshoot I checked I navigated to the terminal of my host computer and windows VM and input the ipv4 and later the subnet address into the discovery wizard and it continued to return 0 devices found, I wasn't sure what the error was. I then began to try other IP ranges and eventually entered 10.0. and it returned 5 devices but none of the devices returned were in my network. I also tested network connectivity by attempting to ping the devices, when doing so I was able to ping into the Nagios terminal from host pc but I could not ping from Nagios terminal to the host pc nor the windows VM.

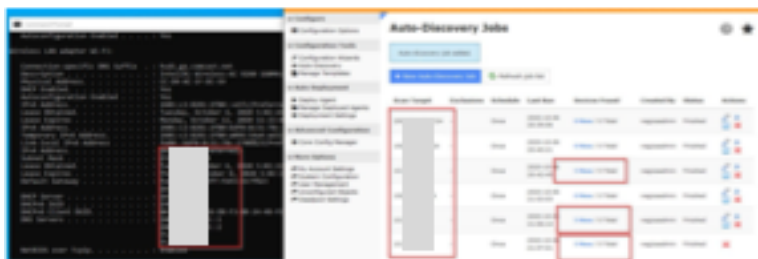
## Auto Discovery wizard



## Default Network for Discovery

A screenshot of the 'New Auto-Discovery Job' form. The 'Scan Target' field is set to '192.168.1.0/24'. The 'Exclude IPs' field is empty. The 'Schedule' is set to 'Frequency: One Time'. The 'Submit' button is highlighted in blue.

## Display of Discovery results 0



## Devices found are not on my LAN

A screenshot of the 'Hosts and Services' table. The table lists discovered hosts and their services. The 'Hosts' column is highlighted with a red box, showing a value of 0.

Address	Type	OS	Status	Host Name	Services	Service Name	Service Port	Protocol
10.0.0.1	Linux Server	Linux 3.11 - 3.14	New	gateway	<input type="checkbox"/> TCP Port 53 - domain	domain	53	TCP
					<input checked="" type="checkbox"/> HTTP	http	80	TCP
					<input checked="" type="checkbox"/> HTTPS	https	443	TCP
					<input type="checkbox"/> TCP Port 49152		49152	TCP
10.0.0.12	Unknown	Apple iOS 5.0.1	New	10.0.0.12	<input type="checkbox"/> TCP Port 3306 - mysql	mysql	3306	TCP
10.0.0.69	Linux Server	Linux 3.7 - 3.15	New	localhost.localdomain	<input checked="" type="checkbox"/> SSH	ssh	22	TCP
					<input checked="" type="checkbox"/> HTTP	http	80	TCP
					<input checked="" type="checkbox"/> HTTPS	https	443	TCP
					<input type="checkbox"/> TCP Port 3306 - mysql	mysql	3306	TCP
10.0.0.209	Unknown	Android 4.1	New	10.0.0.209	<input type="checkbox"/> TCP Port 8009		8009	TCP
10.0.0.254	Unknown		New	10.0.0.254				

## Solution

After continuous troubleshooting with the help of a Team member, we began to think about why we could ping into the Nagios terminal but not from the Nagios terminal to other devices on the network because they all had IP addresses within the same network and subnet. The question led us to start to look at the adapter setting of all the machines and devices and we noticed that not the virtual machines but the virtual box was on a default APIPA ip address and that may be the root cause of the network issues, therefore I manually changed the address within the setting of the virtual box navigate to host network and update the adapter IP address manually, after making this adjustment I was able to ping all devices in going and outgoing to the Nagios terminal and host, windows pc.

## Virtual box Adapter config

Adapter		DHCP Server
<input type="radio"/> Configure Adapter Automatically		
<input checked="" type="radio"/> Configure Adapter Manually		
IPv4 Address:		
IPv4 Network Mask:	255.255.255.0	
IPv6 Address:	fe80::f564:7104:549d:64c6	
IPv6 Prefix Length:	64	

Steps continue:

## Monitoring of Devices

					<input type="checkbox"/>	TCP Port 3306 - mysql	mysql	3306	TCP
<input checked="" type="checkbox"/>	10.0.0.69	Linux Server	Linux 3.7 - 3.15	Old	localhost.localdomain				
					<input checked="" type="checkbox"/>	SSH	ssh	22	TCP
					<input checked="" type="checkbox"/>	HTTP	http	80	TCP
					<input checked="" type="checkbox"/>	HTTPS	https	443	TCP
					<input type="checkbox"/>	TCP Port 3306 - mysql	mysql	3306	TCP
<input checked="" type="checkbox"/>	10.0.0.154	Windows Workstation	Microsoft Windows Vista SP2	New	10.0.0.154				
					<input checked="" type="checkbox"/>	SSH	ssh	22	TCP
					<input type="checkbox"/>	TCP Port 135 - epmap	epmap	135	TCP

## Part 2: Status Change Notifications

Step 1- Power on the Windows 7 VM. Include a screenshot of Service Status for Windows 7 VM showing NetBIOS, Ping, SSH in OK (green) status.

Step 2- Shut down the Windows 7 VM. Include a screenshot of Service Status for Windows 7 VM showing NetBIOS, Ping, SSH in Critical (orange) status.

Step 3- Configure email notifications from Nagios to your email account.

Step 4- Configure SMS text notifications from Nagios to your cell phone.

Step 5- On your Windows 7 VM, block ICMP packets in Windows Firewall. How does this affect Nagios?

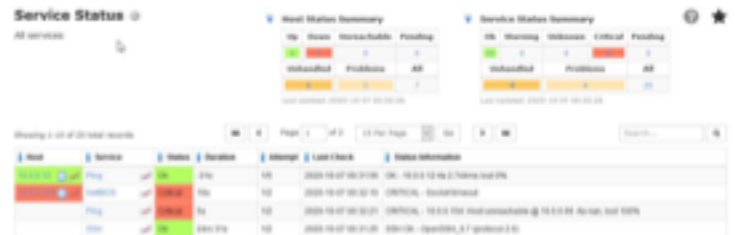
Step 6- On your Windows 7 VM, block SSH traffic in Windows Firewall. How does this affect Nagios?

### Windows NetBios OK



This screenshot shows the Nagios Service Status page for a host named 'alltel'. The 'Host' column shows 'alltel' with a green status icon. The 'Service' column shows 'NetBIOS' with a green status icon. The 'Status' column shows 'OK'. The 'Last Check' column shows '2009-10-07 10:02:01'. The 'Status Information' column shows 'NetBIOS is OK'.

### Windows NetBios Down



This screenshot shows the Nagios Service Status page for a host named 'alltel'. The 'Host' column shows 'alltel' with a red status icon. The 'Service' column shows 'NetBIOS' with a red status icon. The 'Status' column shows 'Down'. The 'Last Check' column shows '2009-10-07 10:02:01'. The 'Status Information' column shows 'NetBIOS is Down'.

### Email Notification

Outbound Mail Settings

Send From:

Send Method: ☐ Sendmail ☒ SMTP

Loggings: ☒ Enable logging of mail sent with the internal mail component (PHPMailer) /usr/local/nagiosxi/tmp/phpmailer.log

SMTP Settings

Host:

Port:

Username:

Password:

Security: ☐ None ☒ TLS ☐ SSL

[Send a Test Email](#)

[Update Settings](#) [Cancel](#)

### SMS Notification

Mobile Carriers

Manage the mobile carrier settings that can be used for email-to-text mobile notifications. Note: The `%number%` macro in the address format will be replaced with the user's phone number.

#	Unique Id	Description	Email-To-Text Address Format	Delete
1	alltel	Alltel	%number%@message.alltel.com	<input type="checkbox"/>
2	att	AT&T	%number%@txt.att.net	<input type="checkbox"/>
3	cingular	Cingular	%number%@cingularme.com	<input type="checkbox"/>
4	metropcs	Metro PCS	%number%@mymetropcs.com	<input type="checkbox"/>
5	nextel	Nextel	%number%@messaging.nextel.com	<input type="checkbox"/>
6	powertel	Powertel	%number%@ptel.net	<input type="checkbox"/>

## Part 3: Reporting

Access the [Nagios XI Demo Environment](#)

Step 1- Examine the Graph feature in Nagios.

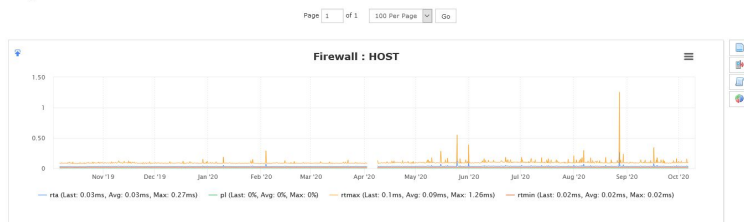
- What does Performance Graphs depict? Explain.
  - This Graph depicts some of the core checks and results of the systems that are being monitored; it provides visuals and keys that define various levels of activity for the firewall, service log network, router, and many more. You can check the history and recent notifications to be updated on key changes
- What does Graph Explorer depict? Explain.
  - This feature provides a visual indication of programs that, system health, performance health of the devices, and systems within the device, this includes traffic that has passed through the device from outside the network.
  - This feature provides indication statuses on the health and status by a status indicator if a percentage of critical, ok, and warning stages.

Step 2- Examine the Maps > BBmap menu and explain what is depicted here.

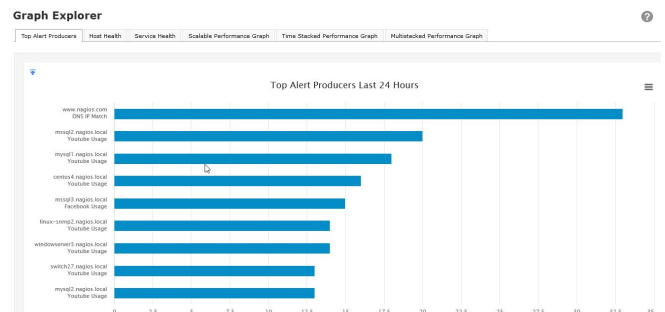
Bbmap is another visual feature that breaks systems and programs that are running or that have interacted with a system that is being monitored and provides individual indications on the status of that particular system or application. This feature allows you to narrow status checks to a singular item and can gather a more detailed look by selecting the system to want to dive into.

### Performance Graph

Performance Graphs  
Host Performance Graphs - 1 Year View  
Showing 1-52 of 52 total records



### Graph Explorer



BBmap

BBMap

Status Grid



Event Log

Report covers from: 2020-10-06 21:28:47 to 2020-10-07 21:28:47  
Showing 1-10 of 427 total records

Type	Date / Time	Information
	2020-10-07 21:25:10	SERVICE ALERT: gateway:HTTPS;OK;SOFT;3;HTTP OK: HTTP/1.1 200 OK - 17046 bytes in 9.899 second response time
	2020-10-07 21:24:01	SERVICE ALERT: gateway:HTTPS;CRITICAL;SOFT;2;CRITICAL - Socket timeout
	2020-10-07 21:22:56	SERVICE ALERT: gateway:HTTPS;CRITICAL;SOFT;1;CRITICAL - Socket timeout
	2020-10-07 21:21:47	SERVICE ALERT: gateway:HTTPS;OK;SOFT;2;HTTP OK: HTTP/1.1 200 OK - 17046 bytes in 8.096 second response time
	2020-10-07 21:20:44	SERVICE ALERT: gateway:HTTPS;CRITICAL;SOFT;1;CRITICAL - Socket timeout
	2020-10-07 21:16:35	SERVICE ALERT: gateway:HTTPS;OK;SOFT;2;HTTP OK: HTTP/1.1 200 OK - 17046 bytes in 7.722 second response time
	2020-10-07 21:15:32	SERVICE ALERT: gateway:HTTPS;CRITICAL;SOFT;1;CRITICAL - Socket timeout
	2020-10-07 21:13:31	SERVICE ALERT: 10.0.0.154;SSH;OK;SOFT;2;SSH OK - OpenSSH_6.7 (protocol 2.0)
	2020-10-07 21:12:32	SERVICE ALERT: 10.0.0.154;SSH;CRITICAL;SOFT;1;connect to address 10.0.0.154 and port 22: Connection refused
	2020-10-07 21:08:33	SERVICE ALERT: gateway:HTTPS;OK;SOFT;2;HTTP OK: HTTP/1.1 200 OK - 17046 bytes in 4.900 second response time

Executive Summary

This is an High-level view of systems performance and health level and indicated by monitoring of hardware and applications that were discovered by the Nagios system.

Executive Summary

Report covers from: 2020-10-06 21:31:48 to 2020-10-07 21:31:48

Availability

Average Host Availability

All Hosts

Unreachable 0.00%

Down 12.00%

Up 88.01%

Average Service Availability

All Services

Critical 13.68%

Warning 0.00%

Unknown 0.00%

Ok 86.32%

Top Alert Producers

Total Alerts	Host	Service	Latest Alert
9	gateway	HTTP	2020-10-07 11:17:45
7	10.0.0.154		2020-10-07 20:59:20
7	10.0.0.154	Ping	2020-10-07 20:59:48
7	10.0.0.154	NetBIOS	2020-10-07 20:59:46
6	10.0.0.154	SSH	2020-10-07 20:59:43
6	gateway	HTTPS	2020-10-07 01:25:06

Alert Histogram

Alerts by Hour of the Day

Latest Alerts

Source	Latest Alert	Alerts
No recent alerts.		

Last Updated: 2020-10-07 21:31:48

## Part 4: Exploit Detection

Step 1- Open a Meterpreter shell from Kali Linux VM to Windows 7 VM.

Step 2- Review Nagios logs during the timeframe of your exploit.

Step 3- Discuss in your submission

- Is there evidence of an attack in Nagios logs?
  - There was no evidence that an attack was taking place on the victim computer, when checking event logs it presented an ok status and provided no indication that an attack had taken place.
- Why/why not?
  - One of the reasons I believe that it was not detected is that once the file was already downloaded to the victim PC so no big change occurred to cause an alert and once the file was executed it did not recognize the attacker computer because of escalation, also because it is a trial version, if you added some of the more specific security features that come along with the service and turn on the firewall you would likely get alerts when unknown actions took place on victim pc.
- What kind of system might compliment Nagios to achieve the desired outcome? Research at least three additional network monitoring solutions and discuss what they do
  - Some monitoring tools that may compliment Nagios are SolarWinds System Management Bundle - this tool can be used for enterprise-level monitoring its doesn't come with as many add on as Nagios which would make it easier to learn and apply to a specified need also has a user-friendly interface and works well with virtualized machines. Another is Zabbix - the benefits of this service is that it is also enterprise-level IT monitoring that is open source and could be a good cost-effective option for orgs with budgets which is all orgs, another thing is that it does not work on windows so could benefit newer companies that are not as traditional



