

### **Purpose**

This document describes how to monitor Windows machines with Nagios® XI<sup>™</sup> using Windows Management Instrumentation (WMI). WMI allows for agentless monitoring of Windows machines which without having to install or configure agents.

## STOP

## The WMI Wizard has been deprecated. Do not use this document.

## **Please read:**

The migration path that Nagios suggests is to use NCPA. While not a drop-in replacement for remote WMI access it should provide you with the ability to gather the information you require from a Windows machine. This option may work well in your environment--especially regarding security, deployment flexibility, and increased insights. Many of our customers benefit from the flexibility and power of our lightweight Nagios Cross Platform Agent (NCPA) that can also be configured to allow passive checks to be submitted to Nagios XI from various versions of Windows, Linux, and more.

With NCPA you can monitor Windows counters, running and stopped processes as well as services! The agent even has a very robust API and optional ability to run remote plugins to gather server-side performance data.

More info about NCPA can be found at:

https://www.nagios.org/ncpa/

Watch this video for NCPA Windows Monitoring (Nagios Cross Platform Agent)

You can distribute the NCPA client using Nagios XI Deploy Agent or your organization's desired software distribution tools.

Or, if an agent is just not an option, SNMP would also be an agentless monitoring option. However, do be aware that Microsoft may also be deprecating SNMP as well. Here is a video that addresses SNMP:

https://nagios.force.com/support/s/article/Monitoring-Windows-With-SNMP-ebda6f97

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

<u>N</u>agios

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 1 / 17 Updated – April, 2023

Another agentless option is using OpenSSH. Microsoft has embraced OpenSSH, but it is a bit more granular, as it is secure by default. Our SSH Proxy Wizard will allow you to retrieve metrics. However, there needs to be some prep work and testing, within your organization, and will most likely require plug ins from the community. This mean we will only be able to assist with the SSH Proxy wizard:

https://assets.nagios.com/downloads/nagiosxi/docs/Monitoring\_Hosts\_Using\_SSH.pdf

Once you have set up a working monitoring node, with SNMP or OpenSSH, you can then use the Bulk Host Cloning and Import Wizard, to add more hosts:

https://assets.nagios.com/downloads/nagiosxi/docs/How-To-Use-The-Nagios-XI-Bulk-Host-Cloning-And-Import-

### <u>Wizard.pdf</u>

## **Target Audience**

This document is intended for use by Nagios XI Administrators who want to monitor Windows servers and workstations without having to install an agent.

## **Windows Machine Requirements**

You will need to ensure you have the following requirements setup before you can use WMI to monitor and windows server or workstation:

- WMI service is running
- WMI user account set up
- Firewall rules set up

Nagios XI Server

This document will walk you through each of these requirements for the window machine you wish to monitor. You will need to log in as a user with administrator privileges.

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Nagios

#### www.nagios.com

# Windows Server Core (No Desktop)

This guide does not provide instructions for configuring Windows Server Core, some of the required GUI utilities are not available in server core. It is technically possible to configure the permissions remotely by using the information in this document, you will need to research on how to actually perform the actions (beyond the scope of this document).

# WMI Service

Before you can monitor Windows machines using WMI, you must ensure that the Windows Management Instrumentation service is running.

In Windows XP / Vista / 7 / 8 / 10 / Server 2003 / Server 2008

- Click Start and choose Run.
- The window to the right will appear and type services.msc in the Open field and then click OK.

You can also type services.msc in the Search field of the Start menu. This applies to all the instructions going forward in this document.

In Windows Server 2012 / Server 2016

- Open the Server Manager
- In the Tools menu select Services



INTL: 1-651-204-9102 1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671

Nagios

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.



Page 3 / 17 Updated – April, 2023

Run	? ×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	services.msc 💌
	OK Cancel <u>B</u> rowse

Verify the service **Windows Management Instrument (WMI)** is in a status of **Started** and has the Startup Type of **Automatic**.

Description: Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

🍇 Services (Local)

Windows Management Instrumentation

Stop the service Pause the service Restart the service

Name A	Description	Status	Startup Type	Log On As
Secondary Logon	Enables st	Started	Automatic	Local Syste
Security Accounts Manager	The startu	Started	Automatic	Local Syste
Server .	Supports fil	Started	Automatic	Local Syste
🙀 Shell Hardware Detection	Provides n	Started	Automatic	Local Syst
🗞 Smart Card	Manages a		Manual	Local Serv
🗞 Special Administration Console Helper	Allows adm		Manual	Local Syst
System Event Notification	Monitors s	Started	Automatic	Local Syst
🗞 Task Scheduler	Enables a	Started	Automatic	Local Syst
🗞 TCP/IP NetBIOS Helper	Provides s	Started	Automatic	Local Serv
🗞 Telephony	Provides T	Started	Manual	Local Syst
🙀 Telnet	Enables a r		Disabled	Local Serv
🗞 Terminal Services	Allows user	Started	Manual	Local Syst
🙀 Terminal Services Session Directory	Enables a		Disabled	Local Syst
Themes	Provides u		Disabled	Local Syst
🙀 Uninterruptible Power Supply	Manages a		Manual	Local Serv
🙀 Virtual Disk Service	Provides s		Manual	Local Syst
🙀 Volume Shadow Copy	Manages a		Manual	Local Syst
🗞 WebClient	Enables Wi		Disabled	Local Serv
🗞 Windows Audio	Manages a	Started	Automatic	Local Syst
🐝 Windows Firewall/Internet Connection Sharing (ICS)	Provides n	Started	Automatic	Local Syst
🙀 Windows Image Acquisition (WIA)	Provides im		Disabled	Local Serv
🐝 Windows Installer	Adds, modi		Manual	Local Syst
Windows Management Instrumentation	Provides a	Started	Automatic	Local Syst
🙀 Windows Management Instrumentation Driver Extensions	Monitors all	••••••	Manual	Local Syst
🖏 Windows Time	Maintains d	Started	Automatic	Local Serv
🐝 Windows User Mode Driver Framework	Enables Wi		Manual	Local Serv
WinHTTP Web Proxy Auto-Discovery Service	Implement		Manual	Local Serv

# **Configure A WMI User Account On The Windows Machine**

Next, configure a WMI user account on the local machine. This account will be used to monitor the Windows machine from Nagios XI. This document will create a new user account called wmiagent with a password wmiagent as an example.

C:\Users\Administrator>net user wmiagent wmiagent /add The command completed successfully.

C:\Users\Administrator>

From an administrative command prompt execute the following command:

net user wmiagent wmiagent /add

You should get a response of "The command completed successfully".

You should use a stronger password than wmiagent as it will most likely fail the password policy requirements.

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

**Nagios**®

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 4 / 17 Updated – April, 2023

## **Setting WMI Permissions**

WMI requires a valid username and password on the target system. The following steps outline how to add only the permissions needed to the Windows user account. Some of these permissions do not need to be set if your user account is a member of the local administrators group HOWEVER from a security perspective it's best to use an account with only the minimal required permissions.

Note: If you wish to monitor multiple computers across the domain, instead add the user to be a member of the "Distributed Com Users", "Event Log Readers", "Performance Log Users", and "Performance Monitor Users" groups.

# Adding Remote Activation Privilege to Windows DCOM

You need to give your newly created user access to DCOM on the localhost. In order to do this, open **Component Services**.

Click **Start**, choose **Run**. Type **DCOMCnfg.exe** and click **OK**.

In Server 2012 / 2016 this is located at **Server Manager** > **Tools > Component Services**.

Expand **Component Services > Computers** and click on My **Computer**.

Right click on My Computer and select Properties.



1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Nagios

### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 5 / 17 Updated – April, 2023 Nagios XI Moni

Monitoring Windows Using WMI

Click the COM Security tab.

Under Launch and Activation Permissions section click the Edit Limits... button.

Click the Add... button

Type wmiagent in the Enter the object names to select field and click OK.

You may need to use the **Locations** button to set the search scope to be the **local computer object** (instead of the domain).

You will now see wmiagent as a user and it will be selected.

Check the **Remote Launch** and **Remote Activation** check boxes under the **Allow** column.

Click **OK** twice. You can now close the Component Services management console.

ly computer Proper	ues					<u></u>
General		Options	1	Default Pr	operties	1
Default Protocols		COM Se	curity		MSDTC	1
Access Permissions You may edit who also set limits on	o is allo applica	owed default acc ations that detem	cess to nine the	application: air own pem	s. You may nissions.	
Caution of applic securely	: Modif cations r.	ying access perr to start, connec	nission: t, funct	s can affect ion and/or	t the ability run	
		Edit Limits		Edit De	efault	
You may edit wh activate objects. determine their o Caution affect th and/or r	o is allo You m wn per Modif ie abilit un sec	wed by default t ay also set limits missions. ying launch and y of applications urely.	on app activat	ch applications the lications the ion permission, connect,	ons or at ions can function	
		Edit Limits		Edit De	efault	
Learn more about <u>set</u>	ting the	ese properties. OK		Cancel	Appl	,

aunch and Activation Permissi	on	? ×
Security Limits		
Group or user names:		
& Administrators (SOLAR0\Adm	ninistrators)	
Reformance Log Users (SOL	LAR0\Performance	e Log Users)
Distributed COM Users (SOL)	AR0\Distributed C	OM Users)
👗 wmiagent (SOLAR0\wmiager	nt)	
	Add	Remove
Permissions for wmiagent	Allow	Deny
Local Launch		
Remote Launch		
Local Activation		
Remote Activation		
Leam about access control and p	emissions	
	OK	
	OK	Cancel

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Nagios

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 6 / 17 Updated – April, 2023

### Nagios XI Monitori

Monitoring Windows Using WMI

## Adding Remote WMI Access

In order for the wmiagent user to return data remotely from WMI, access to the WMI namespace CIMV2 must be granted.

Click Start, choose Run. Type WMImgmt.msc and click OK.

Right click on WMI Control (local) and select Properties.

Click the Security tab of the WMI Control Properties window.

Expand Root and select CIMV2.

Click the Security button.

Click the Add... button

Type wmiagent in the Enter the object names to select field and click OK.

You may need to use the **Locations** button to set the search scope to be the **local computer object** (instead of the domain).

You will now see wmiagent as a user and it will be selected.

Check the **Enable Account** and **Remote Enable** check boxes under the **Allow** column.

Click **OK** twice. You can now close WmiMgmt management console.

ᡖ WmiN	/lgmt - [C	onsole	Root\WMI (	Control (Lo	cal)]
🚟 File	Action	View	Favorites	Window	Help
<	2		?		
Cons	ole Root /MI Contr	ol (Loca	0		Window

WMI Control (Local) Properties	<u>?</u> ×
General Backup/Restore Security Advanced	
	1
Namespace navigation allows you to set namespace specific security.	
⊡	
aspnet	
🗄 🔂 ms_409	
1 power	
E Security	
MicrosoftDfs	
MicrosoftDNS	
	-
Security	
OK Cancel An	olu
	P17-

ecurity for ROOT\CIMV2			
Group or user names:		<b>_</b>	[
x yribbens wmiagent Administrators (SOLAR0\Adm	ninistrators)		
4	Add	Remove	
Permissions for wmiagent	Allow	Deny	
Partial Write	Ë		
Provider Write			l
Enable Account	$\checkmark$		L
Remote Enable			L
Read Security			I.
For special permissions or advance click Advanced.	ed settings,	Advanced	
Learn about access control and p	ermissions		

1295 Bandana Blvd N, St. Paul, MN 55108 <u>sales@nagios.com</u> US: 1-888-624-4671 INTL: 1-651-204-9102

<u>Nagios</u>®

#### www.nagios.com

## **Windows Firewall Settings**

Next, configure the firewall rules specific to the version of windows being monitored.

### Windows Server 2008 / 2012 / 2016 Firewall Rules

To check firewall settings, select **Start** and type **firewall** in the search dialog box and open **Windows Firewall with Advanced Security**.

In Server 2012 / 2016 this is located at **Server Manager > Tools > Windows Firewall with Advanced Security**.

In the left hand pane click **Inbound Rules**. In the right hand pane click **Filter by Group** and then select **Windows Management Instrumentation (WMI)**. You will then be shown the available firewall rules for WMI.

🔗 Windows Firewall with Advance	ed Security						_	Х
File Action View Help								
🗢 🄿 🙇 🖬 🗟 🖬								
🔗 Windows Firewall with Advance	Inbound Rules	Filtered by: Windows Management Instru	umentation (WMI)				Actions	
🔣 Inbound Rules	Name		Group	Profile	Enabled	Æ	Inbound Rules	-
tonnection Security Rules	Windows Ma	anagement Instrumentation (ASync-In)	Windows Management Instr	All	No	Æ	🚉 🛛 New Rule	
> 🖳 Monitoring	😴 Windows Ma	anagement Instrumentation (DCOM-In)	Windows Management Instr	All	Yes	A	🝸 Filter by Profile	•
	🥑 Windows Ma	anagement Instrumentation (WMI-In)	Windows Management Instr	All	Yes	4	🝸 Filter by State	•
							Filter by Group	•
							😽 Clear All Filters	

You need to make sure that the **DCOM-In** and **WMI-In** rules are enabled.

If the WMI rule group does not exist as pictured above, the recommended settings are listed here as outlined by Microsoft. From the command prompt enter (each command is one long command to type):

```
netsh advfirewall firewall add rule dir=in name="DCOM" program=%systemroot
    %\system32\svchost.exe service=rpcss action=allow protocol=TCP localport=135
```

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

<u>N</u>agios

#### www.nagios.com

**Nagios XI** Monitoring Windows Using WMI netsh advfirewall firewall add rule dir=in name ="WMI" program=%systemroot %\system32\svchost.exe service=winmgmt action = allow protocol=TCP localport=any netsh advfirewall firewall add rule dir=in name ="UnsecApp" program=%systemroot %\system32\wbem\unsecapp.exe action=allow netsh advfirewall firewall add rule dir=out name ="WMI OUT" program=%systemroot %\system32\svchost.exe service=winmgmt action=allow protocol=TCP localport=any \_ 🗆 × Administrator: Command Prompt Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. . All rights reserved. C:\Users\Administrator>netsh advfirewall firewall add rule dir=in name="DCOM" p ogram=%systemroot%\system32\svchost.exe service=rpcss action=allow protocol=TCP pr localport=135 0k. C:\Users\Administrator>netsh advfirewall firewall add rule dir=in name ="WMI" pr ogram=%systemroot%\system32\svchost.exe service=winmgmt action = allow protocol= TČP localport=any Ok. C:\Users\Administrator>netsh advfirewall firewall add rule dir=in name ="UnsecAp program=%systemroot%\system32\wbem\unsecapp.exe action=allow Õk. C:\Users\Administrator>netsh advfirewall firewall add rule dir=out name ="WMI\_OU " program=%systemroot%\system32\svchost.exe service=winmgmt action=allow protoc ol=ÎCP localport=any Ok. C:\Users\Administrator}\_

More details about 2008 firewall settings can be found at:

http://msdn.microsoft.com/en-us/library/windows/desktop/aa822854(v=vs.85).aspx

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Nagios

#### www.nagios.com

#### Windows Server 2003 Firewall Rules

The following section describes firewall and DCOM port configuration for a 2003 Windows Server. By default DCOM communicates with the client on a random port, so in order to write firewall rules, specifying a port range is also described.

Click **Start**, choose **Run**, type **DCOMCnfg.exe** and click **OK**.

Run	? ×
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	DCOMCnfg.exe
	OK Cancel <u>B</u> rowse

Expand Component Services, expand Computers, rightclick My Computer, and select Properties.

Click the Default Protocols tab

Click **Properties** button.

My Computer Properties	X
General Options Default Properties Default Protocols MSDTC COM Security	
DCO <u>M</u> Protocols	
Connection-oriented TCP/IP Add Remove Move Up Move Down Properties	
The set of network protocols available to DCOM on this machine. The ordering of the protocols reflects the priority in which they will be used, with the top protocol having first priority.	
OK Cancel Apply	

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

**Nagios**®

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 10 / 17 Updated – April, 2023

### Nagios XI

Monitoring Windows Using WMI

Click the Add button.

Add a port range for COM services. In this example the range is from **5000–5020**. Depending on your environment, you may want to choose a different range.

Click OK when done.

Allow the port range through the windows firewall.

This command will open ports from 5000-5020 to match the COM Internet Services Range.

From the command prompt enter:

FOR /L %I IN (5000,1,5020) DO netsh firewall add portopening TCP %I "COM"%I

Lastly, open DCOM port 135.

Nagios

From the command prompt type:

netsh firewall add portopening TCP 135 "DCOM"



1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Properties for COM Internet Services X Use the port ranges controls to add or remove port ranges from গ্ৰন্থল the port categories for use with packet filtering or firewall software Port Ranges 5000-5020 <u>R</u>emove Remove All Add. Port range assignment Internet range O Intranet range Default dynamic port allocation Internet range O Intranet range

Cancel



OК

www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 11 / 17 Updated – April, 2023

### **Nagios XI**

Monitoring Windows Using WMI

#### Windows XP Firewall Rules

If you are running a firewall on the Windows machine, you must ensure that the Nagios server can contact the WMI service.

To do this, you must open TCP Port 135 on the Windows firewall.

Navigate to Start > All Programs > Accessories > System Tools > Security Center.

From the Windows Security Center click on the link to Manage Setting for: Windows Firewalls.

Switch to the **Exception** tab and click the **Add Port** button.

Enter WMI for the **Name** and Port number 135, then click **OK**.

### **Running The Windows WMI Wizard**

Nagios

Now that WMI has been configured on your windows machine you can now run the Windows WMI wizard from your Nagios XI server. To begin using the Windows WMI wizard navigate via the top menu bar to Configure > Run a configuring wizard and select the Windows WMI wizard. In the following screenshot you can see how the search field allows you to quickly find a wizard.

<u>N</u> agios' XI	Home Vie	ews Dashbo	ards Repo	ts Confi	gure T	ools	Help	Admin		٩	0	占 nagiosadmin	🖒 Logout	≡
✓ Configure	1		Conservation of the											
Configuration Options	Config	uration V	Vizards	- Selec	t a Wi	zard	÷							?
✓ Configuration Tools	Start monitori	ing your infrastruc	ture in minutes.	Configuration	wizards guid	ie you thro	ough the p	process of	setting up	your devices, se	rvers, a	pplications, servic	es, and more	in
Configuration Wizards Auto-Discovery Manage Templates	Show:	wm	A		*	8	9		N			Get Mr	re Wizards P	2
✓ Advanced Configuration	Show.					0	· ·		<u></u>					
Core Config Manager														
✓ More Options	N 1	Vindows WMI												
<ul> <li>My Account Settings</li> <li>→ System Configuration</li> <li>→ User Management</li> </ul>	M L	lonitor a Microsoft(	B Windows work	station or serv	er using WI	4I.								

INTL: 1-651-204-9102 1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671

#### Add a Port X Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use Name: WMI Port number: 135 ICP O UDP What are the risks of opening a port? Change scope.. OK Cancel

#### www.nagios.com

Page 12 / 17 Updated - April, 2023

On **Step 1** the wizard will prompt you for the **IP Address** of the Windows machine, along with the **Domain** (if applicable), **Username** and **Password** to access the machine.

Alternatively you can use an **Auth File** that includes the username and password. Please refer to the <u>Authentication File</u> section in this document for more information.

Click Next to proceed to Step 2.

When you proceed to <b>Step 2</b> , the wizard will
perform a WMI query against the Windows
machine to get a list of the available disks,
services and processes.

If Nagios XI is not able to communicate via WMI, an error will be displayed (see the <u>Troubleshooting</u> section on resolving these errors).

Make sure the Host Name field is correctly populated.

Select the server metrics you wish to monitor and

	Configuration	Wizard: \	Nindows	WMI	- Step	1		÷
--	---------------	-----------	---------	-----	--------	---	--	---

IP Address:	
	The IP address of the Windows machine you'd like to monitor.
	Please see the requirements for the Windows machine setup in this document
uth Info	
Domain:	
	The domain the windows machine is associated with.
	Leave blank if the machine to be monitored is not associated with a domain.
Username:	
	The username used to connect to the Windows machine.
Password:	
	The password used to authenticate to the Windows machine.
Or	
Auth File:	
	File to use with username and password for authentication.
Plugin Deta	ils
The check_wmi	plus.pl plugin truncates plugin output to a maximum of 8192 bytes. Use this field to
ncrease the plu	gin output length in bytes. Leave Blank to use the default.

IP Address:       10.25.14.3         Host Name:       10.25.14.3         The name you'd like to have associated with this Windows machine.         Server Metrics         Specify which services you'd like to monitor for the Windows machine.	
Host Name: 10.25.14.3 The name you'd like to have associated with this Windows machine. Server Metrics Specify which services you'd like to monitor for the Windows machine.	
The name you'd like to have associated with this Windows machine. Server Metrics Specify which services you'd like to monitor for the Windows machine.	
Server Metrics Specify which services you'd like to monitor for the Windows machine.	
Server Metrics Specify which services you'd like to monitor for the Windows machine.	
Specify which services you'd like to monitor for the Windows machine.	
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 u	ptime.
CPU	
Monitors the CPU (processor usage) on the machine.	
A 80 % A 90 %	
Memory Usage	
Memory Usage Monitors the memory usage on the machine.	
Memory Usage Monitors the memory usage on the machine.	
Memory Usage Monitors the memory usage on the machine. 80 % () 90 %	
Memory Usage Monitors the memory usage on the machine.	
Memory Usage Monitors the memory usage on the machine. 80 % 90 %	
Memory Usage Monitors the memory usage on the machine. 80 % 90 % Page File Usage Monitors the page file usage on the machine	

1295 Bandana Blvd N, St. Paul, MN 55108 <u>sales@nagios.com</u> US: 1-888-624-4671 INTL: 1-651-204-9102

**Nagios**<sup>®</sup>

#### www.nagios.com

### Nagios XI Monitor

Monitoring Windows Using WMI

adjust the thresholds as required.

For Disk Usage, the automatically detected disk drives will be populated in the **Scanned Disk List** and they will already be selected in the drop down lists.

×	<b>Disk Usage</b> Monitors disk usa	ge on the n	nachi	ine.		
	WMI plugin de	tected disk	s on '	win7-02.box	293.lo	cal
	Drive: C: •	<u>à</u> 80	%	95	%	Scanned Disk List (Status - Drive: Statistics)
	Drive: E: 💌	<u>80</u>	%	95	%	OK - C: Total=39.90GB, Used=12.89GB (32.3%), Free=27.01GB (67.7%) OK - E: Total=40.00GB, Used=0.09GB (0.2%), Free=39.91GB (99.8%)
	Drive:	۸۵ 📐	%	95	%	
	Drive:	<u>à</u> 80	%	95	%	
	Drive:	۸۵ 📐	%	95	%	
	Add Row   Delete	Row				

For Services, the automatically detected services will be populated in the **Scanned** 

You can add a service to be monitored by double clicking it in the **Scanned Service List**.

For Event Logs you can select the specific log on the windows machine and define warning and critical thresholds based on the amount of Warning or Error logs found in the past x hours.

Services
----------

Specify any services that should be monitored to ensure they're in a running state.



	Windows Service	Display Name	Scanned Service List (Service Name (Display Name) Status)
×	Spooler	Print Spooler	Application Management (AppMgmt) is Stopped BitLocker Drive Encryption Service (BDESVC) is Stopped
			DCOM Server Process Launcher (DcomLaunch) is Running DHCP Client (Dhcp) is Running DNS Client (Dnscache) is Running
			EFS (EFS) is Stopped Windows Event Log (eventlog) is Running
			Add Selected   Select All

Add Row | Delete Row

#### Event Logs

Specify what type(s) of event log data you'd like to monitor.

	Event Log	Display Name	Severity	Hours	Warning Count	Critical Count			
×	System	System Log Critical Errors	Errors	1	5	10			
×	Application	Application Log Warnings	Warnings 💌	1	3	6			
			Warnings 💌						
			Warnings 💌						
			Warnings 💌						
Add Row   Delete Row									
<pre> Back Next &gt;</pre>									

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

# **Nagios**®

#### www.nagios.com

Once you've finished selecting all the items you wish to monitor 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	1 Attempt	Last Check	\$\$ Status Information
10.25.14.3 🖋	Application Log Warnings	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - 0 event(s) of Severity Level: "Error, Warning", were recorded in the last 1 hours from the Application Event Log.
	CPU Usage	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK (Sample Period 18 sec) - Average CPU Utilisation Need at least 2 WMI samples%
	Drive C: Disk Usage 🦷 😽	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - C: Total=39.90GB, Used=12.89GB (32.3%), Free=27.01GB (67.7%)
	Drive E: Disk Usage 🦂	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - E: Total=40.00GB, Used=0.09GB (0.2%), Free=39.91GB (99.8%)
	Memory Usage 😽	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - Physical Memory: Total: 1,023.492MB - Used: 578.648MB (57%) - Free: 444.844MB (43%)
	Page File Usage	Ok	1m 1s	1/5	2016-12-12 14:37:17	Overall Status - OK. Individual Page Files Detail: OK - C:\pagefile.sys Total: 1GB - Used: 113MB (11%) - Free: 911MB (89%), Peak Used: 143MB (14%) - Peak Free: 881MB (86%)
	Ping 💅	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - 10.25.14.3: rta 3.952ms, lost 0%
	Print Spooler 🥪	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - Found 1 Services(s), 1 OK and 0 with problems (0 excluded). 'Print Spooler' (Spooler) is Running.
	snmp.exe 🧩	Critical	1m 1s	2/5	2016-12-12 14:37:17	CRITICAL - [Triggered by _ItemCount<1] - Found 0 Instance(s) of "snmp.exe" running (0 excluded).
	System Log Critical Errors	Ok	1m 1s	1/5	2016-12-12 14:37:17	OK - 0 event(s) of Severity Level: "Error", were recorded in the last 1 hours from the System Event Log.

This completes configuring Nagios XI to monitor a Windows machine using WMI.

## **Authentication File**

Nagios

On Step 1 of the configuration wizard you can provide the location of a file that contains the authentication username and password. This provides the following advantages:

- Credentials are stored in one location, if you need to update the credentials you only need to update the file and all services that use the file are immediately affected
- Admins using Core Configuration Manager won't see these credentials, they will only see the reference

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

#### www.nagios.com

Page 15 / 17 Updated – April, 2023 Nagios XI Mo

Monitoring Windows Using WMI

to the file

To create a file you will need to establish a terminal session to your Nagios XI server. This example will create a file called wmi\_auth.txt that will be stored in /usr/local/nagios/etc/. Create the file by opening vi using this command:

vi /usr/local/nagios/etc/wmi\_auth.txt

When using the vi editor, to make changes press *i* on the keyboard first to enter insert mode. Press *Esc* to exit insert mode.

Add two lines that contain your username and password, for example:

username=wmiagent password=wmiagent

When you have finished, save the changes in vi by typing:

:wq

and press Enter.

You can now close your terminal session and proceed to the following page to see how to use the authentication file in the configuration wizard.

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Nagios

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 16 / 17 Updated – April, 2023

### Nagios XI

Monitoring Windows Using WMI

Here you can see on Step 1 of the configuration wizard how the Auth File has been defined.

It is important that the Username and Password fields above are empty to ensure the wizard correctly works.

Click Next and complete the wizard as explained in this documentation.

|--|

< Back

Next >

### Configuration Wizard: Windows WMI - Step 1 👘 🕸

Windows Machine Information

IP Address:	10.25.14.3
	The IP address of the Windows machine you'd like to monitor.
Auth Info	
Username:	
	The username used to connect to the Windows machine.
Password:	
-	The password used to authenticate to the Windows machine.
Or	
Auth File:	/usr/local/nagios/etc/wmi_auth.txt
	file to use with username and password for authentication.
Plugin Detai	ls
The check_wmi_ increase the plug	plus.pl plugin truncates plugin output to a maximum of 8192 bytes. Use this field to jin output length in bytes. Leave Blank to use the default.
Truncate Out	put Length: 8192 bytes

## **Troubleshooting**

Please refer to the following KB article for troubleshooting problems with WMI:

### https://support.nagios.com/kb/article.php?id=579

# **Finishing Up**

This completes the documentation on how to monitor Windows using WMI in Nagios XI.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

### https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

### https://support.nagios.com/kb

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

<u>Nagios</u>®

#### www.nagios.com

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Page 17 / 17 Updated – April, 2023